Journal of Media Horizons
ISSN: 2710-4060 2710-4052 Volume 6, Issue 3, 2025

CYBER-ENABLED TRANSFORMATION OF NATIONAL SECURITY PARADIGMS

Rimsha Malik

Associate Research Officer at Center for International Strategic Studies Ajk

rimsham156@gmail.com

DOI: https://doi.org/10.5281/zenodo.16742213

Keywords
National Security Pakistan Cyberspace Digital Deterrence Strategic Stability

Article History
Received on 05 May 2025
Accepted on 19 July 2025
Published on 05 August 2025

Corresponding Author: *
Rimsha Malik

Abstract
In what ways is cyberspace changing national security paradigms for governments negotiating changing strategic environments and technical advancements? The conceptual shift of security in the digital age is examined in this study, with special attention to Pakistan, a nation that is becoming more linked to the global information environment. The study, which is based on the framework of digital deterrence, looks at how information warfare, data flows, and cyber power are changing the fundamentals of statecraft, strategic stability, and sovereignty. Cyberspace is not a peripheral issue but rather a key area of national power where influence is established by controlling networks, narratives, and digital infrastructures rather than by annexing new territory. The experience of Pakistan provides important insights into how developing nations adjust to these shifts, striking a balance between autonomy, resilience, and deterrence in a setting characterized by both opportunity and risk. The study advances a better understanding of how the emergence of cyberspace is redefining the logic of national security in the twenty-first century.

INTRODUCTION

The emergence of the internet and other information technologies has fundamentally changed the basis of global security. The internet used to be a marvel of connectivity that made it simple to share knowledge and ideas. But today, it is a complex strategic field with power struggles, weak points, and emerging threats that transcend the conventional boundaries of war and diplomacy. Cyberspace is more than just a playground for technology in today's linked world; it is also a covert but continuous geopolitical battleground.

The internet was first developed in the field of academics and research with the goal of fostering collaboration rather than competition. However, the system's shortcomings were exposed when it was made public. The Morris Worm of 1988 was one of the first indications of the potential for broad disruption of digital systems, and it foreshadowed the current era of cyber conflict (Libicki, 2009). Cyber operations have evolved from experimental forms to increasingly sophisticated statecraft instruments. Since nation-states now frequently use cyber espionage and sabotage as part of their intelligence operations, it is become harder to distinguish between cybercrime and warfare. The Stuxnet worm, which was believed to be an operation by the United States and Israel targeting Iran's nuclear facilities, Russian cyber operations in Ukraine, and the 2016 U.S. elections, have all made cyberspace a crucial component of contemporary strategic thinking (Lindsay, 2013).

Examples of non-state actors who have utilised digital tools to influence and disrupt processes are hacktivist organisations and cybercrime syndicates, which function internationally with little to no

accountability. Because cyberspace is interconnected, the effects of cyber catastrophes could have an impact on global financial systems, governance structures, and public trust. The largest challenge, though, is attribution, which makes it harder to carry out retaliation and deterrent efforts since it is impossible to pinpoint the exact location of attacks.

Given this rapidly evolving environment, traditional national security paradigms that rely on the physical defence of territory are being reconsidered. In addition to practical flexibility, today's strategic environment requires a conceptual shift in hazard assessment, mitigation, and deterrent. This paper looks at cybercrime using a functional model of digital deterrence that includes denial and punishment mechanisms as well as control systems based on reputational norms. This section provides the foundation for assessing how cyberspace affects Pakistan's national security strategy while the rest of the world attempts to figure out how to govern in the face of pervasive digital disorder.

The ability to inflict punitive damage or deny benefits to the adversary is essential to digital deterrence, as is the capacity to mould perceptions, alter reputations, and establish credible postures of cyber resistance. Signals and perception, not just capabilities, are becoming more and more important in cyber deterrence. States like Pakistan, which struggle to manage technical dependency, strategic exposure, and institutional weaknesses as geopolitical competitions shift into the digital sphere, must reevaluate their national security strategies.

The study shifts its attention to Pakistan in this evolving security environment, looking at how the nation is adjusting to the needs of digital security and reacting to the worldwide evolution of cyberthreats. It examines Pakistan's vulnerability to cyberthreats, the demands of regional rivalry, and its continuous efforts to build up its national resilience against quickly changing digital obstacles.

Traditional National Security Paradigms

Military forces, domain boundary defence, and strategic geographical positioning formed the basis of traditional national security systems. The conventional framework, according to Walt (1991), is a system that is focused on state-on-state threats from conventional military attacks or nuclear deterrent concepts that date back to the Cold War. Under this concept, the foundation of national defence programs was the defence of national boundaries, sovereignty, and strategic interests in the kinetic dimensions (land, sea, air, and subsequently, nuclear domains). Since military might is often associated with national security, organisations aimed at preventing, defending against, and punishing threats have been established.

This paradigm persisted far into the late 20th century, driven by realism and the belief that power maximisation and self-help techniques are necessary in anarchic international systems (Mearsheimer, 2019). Security policies throughout this age concentrated on state actors, conventional warfare, and the balance of power in countries like South Asia, where long-standing rivalries like that of India and Pakistan have solidified the idea of deterrence via conventional and nuclear capabilities (Tellis, 2023).

The shortcomings of this antiquated paradigm became apparent as digital technology became more and more integrated with government, defence, and infrastructure systems. Today, national security encompasses more than just obvious and palpable dangers. The development of cyberspace as a vital domain has made it impossible for earlier models to adequately capture the complexity of today's threats. According to Smeets and Tanchum (2024), an excessive dependence on physical deterrence ignores the distributed, unclear, and inexpensive character of cyber activities, which can get past conventional defences.

The inadequacies of the conventional paradigm are brought to light by dealing with non-state actors, transnational threats, and hybrid warfare—aggressions that cut over national borders and do not follow the normative guidelines of state conflict. The national vulnerabilities revealed by the explosion of digital infrastructures, particularly vital systems like banking networks, telecommunications, and electrical grids, cannot be addressed by traditional militarism alone (Carr, 2023).

Furthermore, modern threats might occasionally take the shape of sub-threshold actions like cyber espionage, intellectual property theft, and disinformation operations, which erode state stability over time without evoking traditional reactions (Kello, 2020). The effectiveness of conventional deterrent techniques has been weakened by this discrepancy as

well as the difficulties with attribution in cyberspace. The dynamic character of threats suggests a widening gap between old security concepts and modern realities shaped by cyber dependency.

For countries like Pakistan, who operate in a volatile regional environment and face new non-traditional threats, the continued use of traditional strategic thinking restricts the creation of more flexible, preventative, and deterrent-informed responses. According to Riaz and Khan (2024), the Pakistani national security apparatus still gives kinetic threats excessive attention, even in the face of an increase in cyberattacks on the country's banking, defence, and energy sectors.

Additionally, a slow reaction to cyber-centric attacks is a result of traditional security groups' institutional rigidity. Since the state is ill-prepared to handle persistent, widespread, and hard-to-attribute threats, national security strategy must be reformed to include the digital sphere as a major theatre of war and deterrence. The global shift towards integrated cyber-defense systems is exemplified by the policy of countries like the US, Estonia, and Israel, highlighting the agreement that conventional security measures must change to stay relevant (Libicki, 2023).

In essence, as cyber dangers continue to evolve, the conventional approach to national security is beginning to fail. despite the fact that it is essential. It is necessary to reevaluate security architecture in light of the transition from traditional to cyber-oriented concepts of national defence, especially for regimes like Pakistan's that are both strategically susceptible and structurally incapable of developing cyber deterrence systems.

Rise of Cyberspace as a Strategic Domain

One of the reasons cyberspace has emerged as a key area is the late 20th century globalisation of digital networks and the internet. As the internet gained popularity in the 1990s, it began to facilitate new kinds of communication and engagement, despite its humble beginnings as a tool to boost connectivity and trade. As cyberattacks increased in frequency and sophistication in the early 2000s, it became clear that cyberspace could turn into a battlefield and significantly affect national security (Libicki, 2007). This shift was brought about by the increasing recognition that cyber capabilities might be applied to offensive and defensive military operations in addition to economic and informational ones.

Cyberspace is defined by the convergence of strategic and technical issues (Libicki 2007). Controlling the flow of information or destroying digital infrastructure can alter the balance of power, whether in a war or a peace. The transformation of cyberspace from a mere tool to a vital battlefield has had profound effects on military operations, political influence, and economic stability. Kaplan (2016) goes into further detail on this subject by highlighting how countries' military tactics and strategy evolved as they realised that cyberspace could be used as both an offensive and defensive instrument.

The emergence of cyberspace as a strategic arena portends a shift away from traditional conflict strategies. Kinetic forces, which have long dominated traditional military doctrine, include ground forces, airstrikes, and naval operations. However, as noted by Tikk and Kaska (2010), cyberwarfare operates under a completely different paradigm. Deterrent strategies are complicated by the difficulties of determining the consequences of cyberattacks that are undertaken remotely and do not physically breach boundaries. Data breaches, malware injection, and DDoS attacks are examples of cyberattacks that have increased in frequency and have disastrous consequences for both nation-states and non-state actors.

Cyberwarfare can target critical infrastructures, including government networks, financial systems, and power grids, endangering a country's economy and security (Tikk and Kaska, 2010). These powers conflict with conventional security measures like border patrols and other forms of strategic force. As countries reevaluate their security policies in reaction to cyber infrastructure vulnerabilities, digital deterrence has become a fundamental element of defensive doctrines (Kaplan, 2016).

New national security plans with an emphasis on deterrence have been developed as a result of the recent official acknowledgement of cyberspace as a strategic sector. In order to apply traditional ideas of punishment and denial to the virtual world, this thesis suggests a theoretical framework known as "digital deterrence." Undefined digital borders and largely unnamed stateless entities who carry out cyberattacks make it extremely difficult to identify the culprits of these attacks (Libicki 2007).

According to Perlroth (2021) and Kaplan (2016), there are issues that arise from dubious cyber defence strategies. According to Kaplan (2016), digital deterrence differs from traditional deterrence based on force and vengeance since it provides cyber retaliation, such as the destruction of adversary cyber capabilities and cyber counterattacks. Perlroth (2021) has identified the issue of inadequate source recognition, which presents challenges for the technique. When attackers use anonymous networks or proxies, it becomes more difficult to identify them through their crimes.

Given the growing cyber danger, Pakistan should reconsider its national security strategy to make cyberspace a major part of it. Conventional military deterrent systems, which have their roots in kinetic combat, must be modified to meet the new realities of cyberwarfare. While denial by denial concentrates on minimising vulnerabilities, this strategy emphasises the danger of retaliation, much like deterrent by punishment. Nevertheless, Tikk and Kaska (2010) contend that this approach can accomplish the overall objectives of digital deterrence.

Our perspective on national security has completely changed as a result of cyberspace's rise to prominence as a critical area. Because cyber capabilities are dynamic and must adjust to new threats, national security strategies must place a high priority on cyberspace and make sure deterrence systems are sufficiently technologically advanced. In order to integrate a digital deterrent into its national defence plan, Pakistan must reconsider conventional ideas of security.

The Impact of Social Media

Social media platforms are a significant component of cyberspace's strategic significance because they provide significant potential in three areas: influence warfare, psychological operations, and perception management. States are using social media sites like Facebook, Instagram, and Twitter in real time to discredit adversaries, sway public opinion, and project narratives. Social media's weaponization has made it harder to distinguish between violent and nonviolent conflicts, regional and global threats, and true and fake news (Perlroth, 2021).

Digital deterrence is significantly impacted by the ease and speed with which false material can circulate on social media. People are increasingly exploiting social media influence operations to erode community cohesion and public confidence in institutions. Election procedures, intercommunal disputes, or diplomatic narratives are the focal points of these non-violent challenges to state sovereignty. The South Asian cyberwarfare between India and Pakistan is a prime example of this way of thinking, as Pakistan coordinates its disinformation efforts around significant events and uses communal narratives (Hook & Verdeja, 2022).

The emergence of social media has caused a significant change in Pakistan's political and social environments as well as the dynamics of national security. With more than 40 million active users and rapidly growing digital connections, social media platforms have become an indispensable part of peoples' everyday lives. 87 million internet users and 85 million 3G/4G customers enable this expansion (Rizvi, 2021; Wilson et al., 2014). Facebook, which has over nine million active users in Pakistan, is one example of a platform that shows how much of the country's diverse population uses the internet. This digital transformation has increased people's access to information and means of expression, but it has also increased the vulnerability of national security frameworks.

Propaganda, deception, and cybercrime flourish in the digital public sphere, which has expanded in scope and impact due to the widespread availability of inexpensive internet access. Often, Pakistani police forces lack the technology capabilities necessary to effectively identify or neutralise such threats. As a result, social media has turned into a two-edged sword: a forum for democratic expression and a tool for criminals to sway public opinion, organise uprisings, and undermine the government. The rapidly growing usage of social media, particularly among youth, has become the focus of security agencies due to concerns about opinion formation and ideological radicalization (Woolley, 2022).

In more than 70 countries, including Pakistan, social media has been employed as a weapon by both state and non-state actors for disinformation campaigns, psychological operations, and recruitment. One historical illustration of how online communities may ignite enormous social movements and overthrow governments is the Arab Spring, which is sometimes

referred to as the "Facebook Revolution" due to its extensive usage of social media. Social media gave those affected by repressive regimes a forum for self-expression, but it also exposed the shortcomings of traditional forms of governmental control in the contemporary digital era. Pakistan and other growing nations are currently dealing with the issue of information warfare, which has extended beyond conventional battlefields and into people's daily digital interactions (Gire, 2014).

Given this, the media's dual function as a propagandist and a judge of truth presents a major risk to national security. As it attempts to reconcile the conflicting demands of stability and sovereignty, Pakistan has long struggled with the theoretical conflict between state control and free speech. Classic theories of media, like the Authoritarian, Libertarian, and Social Responsibility models, can help us understand how the media affects governmental power. With conflicting interests from the government, corporations, and civil society all attempting to influence the public discourse in the nation, Pakistan's media landscape is complicated.

Data Leaks and Oversharing

Social media's inherent nature makes it simple for users to divulge excessive personal and professional information without considering the possible consequences. This frequent oversharing, which has happened even from official accounts, has resulted in several data leaks. Without considering the possible security dangers, users in Pakistan, particularly those in the younger generations, frequently share information about their travels, jobs, and even private company details. Malicious actors commonly utilise this data to initiate spear-phishing attacks or gain illegal access to computer networks (Kaspersky, 2022).

A troubling occurrence occurred in 2020 when a government official unintentionally revealed a confidential project timetable on LinkedIn. An international threat intelligence team located the post and used it to initiate focused assaults on the organization's systems. Similar to this, there have been instances where military personnel have shared geotagged photos, project references, or their deployment locations on social media sites like Facebook and Instagram. These posts are not private but could be strategically useful.

Approximately 18% of corporate breaches in Pakistan between 2021 and 2022 were linked to negligent social media data leak, according to the National Cyber Security Council (NCSC, 2022). These examples highlight how important it is for institutions to have digital security awareness programs. Pakistan's defence and bureaucratic systems are vulnerable to seemingly innocuous activities on social media unless there are stringent rules and user education.

Malicious Shortened Links

Bit.ly and TinyURL, two services that shorten URLs, have increased the effectiveness of online communication. However, because of their opacity, hackers have found them interesting. Attackers occasionally use dramatic headlines or emotionally charged bait content to entice users to social media sites, where they use shortened links to insert malicious payloads. Clicking on these links may result in the installation of malicious software, phishing websites, or hijacked browser sessions (Cao, 2016).

The risks of utilising short URLs are still not widely known in Pakistan. According to PTA's 2023 Annual Cybersecurity Report, URL shortening techniques were utilised in more than 42 percent of phishing attacks in the preceding year. Social media profiles that seem to be from well-known businesses, like local news stations or governmental organisations, have a higher chance of gaining users' confidence and encouraging interaction. For instance, during the COVID-19 epidemic, several malicious links that looked like health alerts propagated via shortened URLs on Twitter and WhatsApp, infecting devices at home and at work (PTA, 2023).

Government digital response teams like CERT-PK have made strides in blacklisting dangerous domains. The quick and constantly evolving nature of URL generation makes real-time blocking very challenging, and Pakistan's cybersecurity infrastructure severely lacks investment in or use of AI-driven monitoring solutions.

Fake Accounts and Online Manipulation

Fake accounts on social media have been an issue for a while, but the methods in which they endanger national security are always evolving. These accounts are frequently used for social engineering, espionage, dissemination of misleading information, and theft of

personal data. The problem is especially bad in Pakistan because of the nation's unpredictable political and social environment, which makes manipulation simple.

Disinformation was spread by Indian media to incite hostilities with Pakistan. When propaganda starts to trump critical thinking, questioning skills, and emotional appeals, it is most persuasive. According to a survey published by a think tank magazine, the majority of key Indian television news channels recorded fake news levels above 90%, indicating that a startling proportion of the monitored war news information was untrue.

For example, out of 10,700 war-related news that Times Now broadcast, 99.15% were discovered to be false, leaving only three accurate reports. In a similar vein, Aaj Tak reported 97.44% incorrect content, while Republic Bharat and NDTV India had 98.96% and 98.29% fake news, respectively. Even networks like CNBC Awaaz and Bharat24, which are thought to be a little more impartial, had fake news rates of 88.21% and 89.17%, respectively. (THINKTANK JOURNAL, 2025)

Both academics and policymakers concur that domestic social media platforms, national cyber legislation, and robust public awareness campaigns are the best ways to solve these issues. A well-thought-out national strategy is required to safeguard digital freedoms and ensure security; social media bans in general are unworkable and anti-democratic. Purchasing technology is only one part of the puzzle; another is educating the public about digital responsibility. To maintain public confidence and the integrity of the country in this age of hybrid threats, reliable information ecosystems, professional media conduct, and open state-media relations are crucial.

Technological Advancements and the Evolving Threat Landscape

Our digital environment is made brighter by technology as a result of the world's digital transformation. A vast network of interconnected items has been produced by the advancement of artificial intelligence and the growing number of internet-connected devices. Wearable technology, smart appliances, industrial systems, and critical infrastructure are all part of this web. Despite the immense growth potential, these advancements have resulted in a complicated and constantly evolving cybersecurity landscape. The term cybersecurity refers to safeguarding our data, systems, and networks from online threats that could cause harm (Zaid & Garai, 2024).

Given the frequency of assaults and the speed at which related technologies are developing, modern cybersecurity is a critical issue. It is essential for their continued safety because of how reliant individuals and businesses are on digital technologies. Cybersecurity protocols are essential for government agencies, healthcare organisations, financial institutions, smart cities, power systems, educational institutions, and the military. Cybersecurity is under risk from a wide range of terrorists, state actors, cybercriminals, and even insiders (Admass et al., 2024).

The digital landscape is continuously changing due to new technology, thus cybersecurity needs to be given more attention. Businesses need to take safeguards to protect their customers' digital assets, intellectual property, and personal information because cybercrime is becoming more common. When businesses rely on digital technology, they run the risk of endangering operations, customer trust, and company confidence. These days, cyberattacks are more frequent, sophisticated, and severe than ever before. In light of this, it is crucial to consider how to preserve digital assets while also guaranteeing the privacy, accessibility, and calibre of data (Mandal et al., 2023).

Due to the rapid advancement of technology, a digital dilemma emerges. While technological advancements present new opportunities for cybersecurity defences, they also reveal vulnerabilities that malicious actors may take advantage of. Innovations, creativity, and scientific progress have long been attributed to the development of the economy and society. Outstanding technological advancements, especially in the recent several centuries, have caused a significant transformation in the digital environment. However, there is a cost associated with improvement. People are becoming more and more reliant on technology, which raises the risk of abuse and exploitation (Rolenc, 2020).

As more sophisticated technology is developed, cybersecurity poses challenges. Because simplified systems are notoriously hard to modify, more

conventional security measures have to be developed. This vulnerability is caused by outdated security protocols, inexperience with software, and a general lack of technological knowledge. Because cyberattacks are constantly evolving, having a multi-layered security approach is essential to successfully surviving them. A robust defence requires regular security system evaluation and monitoring (Kalra et al., 2020).

Underdeveloped nations are facing challenges as a result of an increasing number of cyberattacks (Otieno, 2020). These countries struggle to strike a balance between the advantages and disadvantages of technology. Data breaches and network attacks are more common in developing nations than in industrialised ones. Even while cyberattacks increasingly harm both individuals and businesses, there have been instances where significant national infrastructure has been interrupted, leading to unpredictability and a detrimental impact on services. Furthermore, private government data could be obtained by non-state actors conducting cyber espionage, endangering national security and perhaps having disastrous consequences. In order to combat this threat, all stakeholders—regardless of their level of experience—must prioritise cybersecurity and broaden their understanding of emerging technologies. To strengthen their cyber defences and take advantage of technological breakthroughs, nations must work together.

Artificial intelligence (AI) is a crucial technology because of its unparalleled ability to strengthen cybersecurity systems. Artificial intelligence (AI) has the potential to improve cybersecurity by reducing threats, strengthening defences, and enhancing threat detection. AI can analyse historical data and spot current trends to assist companies in implementing preventative defences. These technologies will assist in identifying possible threats and putting defences in place to stop widespread cyberattacks. AI enables this strategy, which can improve cybersecurity (Camacho, 2024).

Furthermore, while AI is transforming national security capabilities and plans globally, the South will be most affected. Every country is pursuing AI-driven projects to strengthen its internal security, including surveillance, autonomous technology, and cybersecurity, among many others. States now have more strategic flexibility than ever before thanks to the spread of AI and advancements in data processing, which enables them to better safeguard their independence, sovereignty, and peace. This is due to AI's capacity to improve data analysis, cyber resilience, intelligence surveillance, and well-informed decision-making by proactively identifying dangers (Srivastava, 2023).

Interdependence and Systemic Vulnerabilities

The idea of sovereignty becomes entangled in code, connections, and circuits rather than geography alone during a time when conflict is defined by virtual borders rather than actual frontiers. Strangely, the very technology that promised emancipation from the limitations of the old world has made state dependency, vulnerability, and exposure worse. The state finds itself in a precarious position as national infrastructures become more interwoven in the web of global interdependence. It is nearly invisible since it is both empowered and threatened by connectedness (Eric Brahm, 2016).

This signifies a change in metaphysics rather than merely a change in instruments. Instead of a stronghold surrounded by walls and moats, the state now resides in porous architecture, where defences are dynamic and attacks are sensed rather than seen. Hackers can interfere with a minor network function, which causes important processes to stop until the network is completely shut down. The philosophical conundrum starts here: How can a sovereign entity defend itself when its power is determined by algorithms rather than soldiers, given that its essence is distributed rather than singular? In this world, fighting occurs in secret, in the dark, and frequently goes unnoticed. Contrary to the traditional grammar of deterrence, silence may be a strategy in this society where resilience is a survival language.

Deterrence can therefore be viewed as an ontology of readiness rather than a philosophy of retaliation. The promise of continuity—that systems will remain, that trust will not be betrayed, and that disruption will not destroy the social and political bargain that the state is based on—rather than the threat of counterattack is the signal of strength. Being stable does not mean being secure from damage; rather, it means having the capacity to absorb and adapt to disruptions.

These problems with interdependence are structural, systemic, and inherent to the existing power structure; they are not an exception to anything. Refusing them is a recipe for trouble. To demonstrate strategic acumen, one must first acknowledge it. Ironically, a state's susceptibility to asymmetric attacks rises with its level of integration into the global digital matrix (Libicki, 2021). The current state of affairs in Pakistan is appalling. Pakistan's cyber defence capabilities have increased as a result of the rapid growth of information and communication technology (ICT), which is beneficial for a nation that is still having difficulty modernising its institutions.

This expansion is increasingly dependent on biometric technology (like Nadra) and digital infrastructure in the military and energy sectors (Aziz, 2022). Critical systems are vulnerable to hostile manipulation as a result of the multiplying effect of disconnect between cybersecurity readiness and digital usage. This expansion is increasingly dependent on biometric technology (like Nadra) and digital infrastructure in the military and energy sectors (Aziz, 2022). Critical systems are vulnerable to hostile manipulation as a result of the multiplying effect of the disconnect between cybersecurity readiness and digital usage.

The web of interdependence that encompasses monetary systems also includes global monitoring and communication systems. Pakistan's underwater fiber-optic cables, which span strategically significant marine regions, make it susceptible to foreign influence and surveillance (Healey, 2023). In hostile geopolitical situations, such as those involving India, the dependence on infrastructure creates what Nye (2021) refers to as "strategic choke points," which can be used to obtain an advantage without ever going over the traditional line of confrontation.

States that are prone to conflict have been the subject of research on this topic. The first successful cyberattack on such infrastructure was in Ukraine in 2015, when Russian-backed hackers tried to take down the country's electrical grid. It demonstrated that the kinetic potential of cyber attacks is increased and strategic shortcomings are exacerbated by the connectivity of digital networks and civilian infrastructure (Zhora, 2022). Ukraine was susceptible to similar operations as Pakistan because to its political instability and deteriorating infrastructure; this episode serves as an example of the perils of cyber-enabled hybrid warfare.

These drawbacks demonstrate the necessity of a philosophical shift when seen from the standpoint of Digital Deterrence Theory. Traditional deterrent strategies that rely on punitive powers are ineffective in cyberspace due to the fuzziness of online attribution and the increased likelihood of deterrence through denial rather than punishment (Hunker & Waller, 2021). With a focus on strengthening cyber defensive systems, lowering vulnerability, and enhancing institutional readiness, it seems that Pakistan is moving its approach towards resilience-based deterrence.

More sophisticated forms of warfare, such as information warfare, are now possible due to the way everything is connected online. Due to Indian influence activities, the EU DisinfoLab (2020) discovered more than 750 fake news websites that propagate narratives against Pakistan. Through the nation's digital openness, these initiatives influence global opinion and harm Pakistan's diplomatic standing without launching a single traditional cyberattack.

Therefore, reliance on digital technology in architecture has certain potential advantages but also some disadvantages. Pakistan's independence is constantly in risk from cyber incursion and influence rather than traditional invasion, and these vulnerabilities are made worse by the absence of international enforcement mechanisms (Kaplan, 2021).

Technical solutions are not enough to counter these threats. It urges greater funding for cyber education, encourages regional cyber diplomacy, and emphasises the necessity of incorporating cybersecurity into national security plans. Until a comprehensive system of governance is put in place, Pakistan must strengthen its digital capabilities to withstand cyber manipulation, dishonesty, and systematic disruption—the characteristics of contemporary strategic competition.

Strategic Implications for State Sovereignty and Stability

There would be significant repercussions for fundamental issues like state sovereignty and global systemic stability if cyberspace were to become a

contentious strategic region. Important state functions, such as financial systems, civic governance, and defence logistics, depend on digital infrastructure at a time when the conventional Westphalian concept of sovereignty is becoming more hazy and leaking. Historically, claims to sovereignty have been based on the creation of monopolies inside well defined borders and the use of force to uphold them. In the digital age, this monopoly is weakened by invisible, non-kinetic, external intrusions that are occasionally poorly ascribed and undermine state control over its informational environment and security system. According to Richard A. Clarke and Robert K. Knake (2020), authors of "The Fifth Domain," cyber operations have made it possible to "attack governments without invasion." This shift in focus from geography to infrastructure has given rise to a new paradigm of vulnerability. National security, the legitimacy of the state, and its presumed capabilities are all at risk from any adversary, whether state-based or non-state-based, that can exploit digital linkages. The paradox of cyber visibility is clarified by applying digital deterrence theory in this context: countries must demonstrate their dissuasion capabilities, but doing so may expose their weaknesses.

Although traditional deterrence theories, like nuclear posture, can benefit from strategic ambiguity, the idea is difficult in cyberspace due to shifting power dynamics and a lack of norms (Nye, 2017). Pakistan's administration is particularly susceptible because of its underdeveloped infrastructure and religious turmoil, which have depleted its resources. Its control over the electronic realm is constantly threatened by foreign propaganda, espionage, and subversive digital intrusions, frequently with the pretence of plausible deniability. This is taking place in spite of its ostensibly intact sovereignty.

Cyberspace is the conceptual counterpart of a Hobbesian wasteland, where a digital "state of nature" emerges in the absence of generally accepted and upheld regulations. The only people who can maintain stability here will be those who possess superhuman levels of institutional strength and technological proficiency. Suter (2021) argues that states in the modern era need to reconsider sovereignty from multiple perspectives, including narrative sovereignty, digital sovereignty, infrastructural sovereignty, and physical control.

Examples further illustrate the strategic implications. Key digital strategies employed during the 2019 Balakot event, a kinetic response to the Pulwama attack, included information warfare, social media manipulation, and cyberattacks on Pakistani institutions (Klimburg, 2021). Similar to this, Pakistan is dealing with a type of narrative warfare that is threatening both its international standing and its national stability as a result of the ongoing accusations and digital attacks made against the nation in numerous international forums, which are frequently supported by coordinated, false online activity.

Furthermore, social media's rapid growth has turned it into both a communication tool and a cause of strategic ambiguity. Without regulatory oversight, these websites are being used as weapons to deepen religious, political, and ethnic divides, undermining trust in national institutions and escalating internal strife. Platforms like Facebook and Twitter are "attention merchants," as Tufekci (2018) persuasively argues, and their algorithmic incentives occasionally favour lies over truth and agitation over reason.

Therefore, the digital world may be both a platform for progress and power and a tool for instability and tyranny. Information and communication technologies (ICTs) are dual in nature, thus nations should ideally put preventive measures in place to lower cyber risk and boost cyber productivity. Cybersecurity is a collection of procedures that may include both administrative and technical controls and are intended to safeguard establishments that depend on information and communication technology. These latter are viewed as both technical tools and social institutions, much like how ICTs are used to accomplish sociopolitical goals.

Because of this, they are important socioeconomic determinants of cyber power, or national power. "Application of cyberspace to generate benefits and shape occurrences in other kinetic domains and across the five modes of operation" is the formal definition of cyber power. Therefore, better law and order systems, faster economic growth, more effective military dominance, and a well-run administration all depend on the efficient and effective use of ICTs.

While there are several positive outcomes from this attack, such as Pakistan's rapidly growing Internet access and ICT infrastructure, there are also many significant cybersecurity dangers. Hacking, cyber-

terrorism, organised cybercrime, and cyberwar are a few instances of these threats. This is particularly relevant in light of the general discomfort that permeates Pakistan and the surrounding regions. Cyber espionage frequently targets Pakistan, and Indian hackers frequently target Pakistan's banking sector. Given the growing role of the internet in conflicts, Pakistan is at risk from terrorist groups, and India may retaliate by attacking Pakistan with cyberattacks.

Pakistan in the Context of Global Cybersecurity Shifts

In this digital revolution, Pakistan is situated at a pivotal juncture. Despite structural weaknesses and hostile technology advancements, the nation has shown an increasing understanding of cyberspace as an integrated area of national security. By engaging in diplomatic discussions, improving internal coordination, and making investments in technical self-reliance, Pakistan is gradually taking on a responsible role in the global cyber ecosystem rather than remaining a passive actor. These actions reflect a developing cyber perspective sensitive to the intricacies of digital interconnectivity.

Crucially, cyberspace has evolved into a key arena of impact rather than merely serving as an accessory to physical force. In this dynamic space, stories are created, alliances are put to the test, and sovereignty is negotiated. In this matrix, Pakistan's developing cybersecurity strategy shows how strategic awareness and technological ambition come together. In addition to safeguarding domestic infrastructure, it aims to influence international cyber standards by means of regional cooperation and unambiguous regulations.

Cyber threats are by their very nature asymmetric, frequently undetectable, psychologically damaging, and untraceable. These traits call for strategic planning for nations with a history of security challenges, such as Pakistan. Developing skills for attribution, credible signalling, and cyber diplomacy is the difficult part. With the introduction of cyber awareness campaigns, the expansion of CERT activities, and the use of narrative counter-responses to indicate deterrence, Pakistan has made admirable progress in this area. These show a deliberate move towards responsible, reasonable, and trustworthy cyber behaviour.

Pakistan's digital footprint has grown significantly, especially in areas like national identity systems, banking, energy, and aviation. The government has started to reinforce institutional mandates and legislative tools in recognition of the stakes. A significant document, the National Cyber Security Policy 2021, demonstrates a sincere effort to eliminate systemic flaws and brings Pakistan into line with global best practices. The nation has demonstrated policy-level maturity by institutionalising cybersecurity as a part of national defence, not just administrative regulation, even though implementation is still ongoing.

Furthermore, Pakistan is actively promoting international cyber stability through multilateral forums such as OIC meetings and UN discussions. (Khan, 2022)

Conclusion

The field of cybersecurity is always changing due to the quick development of technology and the shifting balance of power in the world. Cyberspace is now a strategic domain in and of itself as a result of the redefining of national security paradigms brought about by the digitization of communication, infrastructure, and government. This change offers Pakistan both possibilities and difficulties. Pakistan is actively negotiating this transition as a digitally evolving state, strengthening its cyber readiness, readjusting its strategic posture, and building institutional resilience in response to changes around the world.

Information warfare and narrative manipulation are two areas that are receiving more attention and concern. Coordinated disinformation efforts have targeted Pakistan, especially during politically delicate times. The goal of these programs is to erode social cohesiveness and institutional trust. In response, Pakistan is establishing counter-narrative projects based on factual transparency and public participation in addition to bolstering mechanisms for monitoring digital media. In the face of hybrid challenges, these measures seek to preserve digital harmony and epistemic integrity rather than suppress dissent.

In terms of regional dynamics, the nation's moderation and moral stance stand out. For example,

instead of escalating reprisal, diplomatic engagement has been used to address cross-border cyber breaches, such as unauthorised access attempts on vital databases or infrastructure networks. Instead than focussing on cyber aggression, this strategy emphasises a more comprehensive theory of responsible deterrence based on sovereignty, resilience, and strategic signalling.

Nowadays, perception and soft power have just as big of an impact on the global cybersecurity scene as technical skill. In the digital age, deterrence is more about relationships, clarity, and credibility than it is about retaliation. Recognising this change, Pakistan is pursuing a philosophy that blends strong internal resilience with normative leadership.

Cybersecurity issues today include social engineering, psychological operations, and information asymmetries in addition to espionage and technological disruption. In this regard, Pakistan must both establish institutional protections and have a philosophical position on what behaviour in cyberspace is unacceptable. This work is made more difficult by the lack of a legally binding international cyber treaty, but Pakistan is still in favour of a rules-based digital order that promotes collective security and sovereignty.

Both vision and alertness are necessary for the future. Pakistan has to keep up its momentum by investing in human resources, establishing cross-sectoral coherence in policy execution, and institutionalising cyber governance. More significantly, cybersecurity needs to be viewed as a foundational element of national identity, sovereignty, and strategic autonomy rather than merely a bureaucratic task. Pakistan is actively helping to reshape these norms as the world moves closer to a "Westphalian moment" in cyberspace, when influence spheres, cyber sovereignty, and digital boundaries are being rewritten. Although it is still in the early stages of development, its cyber policy architecture demonstrates a balanced approach, emphasising regional collaboration, strategic signalling, moral moderation, and a dedication to global cyber peace.

References

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Comparative Strategy, 12(2), 141–165. https://doi.org/10.1080/01495939308402915

Baylis, J., Wirtz, J. J., & Gray, C. S. (2018). Strategy in the contemporary world: An introduction to strategic studies (6th ed.). Oxford University Press.

Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Clarke, R. A., & Knake, R. K. (2012). Cyber war: The next threat to national security and what to do about it. Ecco.

Deibert, R. J. (2013). Black code: Inside the battle for cyberspace. Signal Books.

Dunn Cavelty, M. (2008). Cyber-security and threat politics: US efforts to secure the information age. Routledge.

Eric Brahm. (2016, June 29). Sovereignty. Beyond Intractability. https://www.beyondintractability.org/essay/sovereignty

Gire, S. (2014). THE ROLE OF SOCIAL MEDIA IN THE ARAB SPRING | pangaea journal. Sites.stedwards.edu. https://sites.stedwards.edu/pangaea/the-role-of-social-media-in-the-arab-spring/

Healey, J. (Ed.). (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Hook, K., & Verdeja, E. (2022, July 7). Social Media Misinformation and the Prevention of Political Instability and Mass Atrocities. Stimson Center. https://www.stimson.org/2022/social-media-misinformation-and-the-prevention-of-political-instability-and-mass-atrocities/

Khan, S. (2022). Cyber Security Challenges in Pakistan: An Assessment. 1(1), 78–89. https://www.researchgate.net/publication/360256123_Cyber_Security_Challenges_in_Pakistan_An_Assessment

Kaplan, F. (2016). Dark territory: The secret history of cyber war. Simon & Schuster.

Klimburg, A. (2017). The darkening web: The war for cyberspace. Penguin Press.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Nye, J. S. (2010). Cyber power. Harvard Kennedy School Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/cyber-power

Nye, J. S. (2011). Power and national security in cyberspace. In S. Bosco (Ed.), Deterrence in the twenty-first century: Proceedings (pp. 5–15). NATO.

Perlroth, N. (2021). This is how they tell me the world ends: The cyberweapons arms race. Bloomsbury Publishing.

PTA, C. V. D. (2023). PTA CYBER SECURITY Annual Report 2023. https://www.pta.gov.pk/assets/media/2024-11-06-Cyber-Secuirty-Annual-Report-2023.pdf

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Tikk, E., & Kaska, K. (2010). International cyber incidents: Legal considerations. NATO Cooperative Cyber Defence Centre of Excellence.

THINK TANK JOURNAL. (2025, May 14). Indian media used 90% fake news to flare up Indo-Pak nuclear war: Report. ThinkTank.pk. https://thinktank.pk/2025/05/14/indian-media-used-90-fake-news-to-flare-up-indo-pak-nuclear-war/

United Nations. (2021). Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (A/76/135). https://www.un.org/ga/search/view_doc.asp?symbol=A/76/135

Woolley, S. (2022, July). Digital Propaganda: The Power of Influencers. Journal of Democracy. https://www.journalofdemocracy.org/articles/digital-propaganda-the-power-of-influencers/

Zaid, T., & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. Blockchain in Healthcare Today, 7(1). https://doi.org/10.30953/bhty.v7.302.