Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 2, 2026

CYBER TERRORISM AND THE FUTURE OF PAKISTAN'S NATIONAL SECURITY

Haider Abbas[1]
[1]*Civil Servant in the Government of Pakistan*
[1]*haiderabbasgg@gmail.com*

DOI: https://doi.org/10.5281/zenodo.18454386

Keywords:
Cyber-Terrorism, Critical Infrastructure, National Security, Pakistan, Public-Private Partnerships, Resilience, Defense Policy, Artificial Intelligence, Quantum Computing

Article History
Received on 10 Jan, 2026
Accepted on 22 Jan, 2026
Published on 02 Feb, 2026

Corresponding Author:

Abstract

The new digital age is vastly restructuring the national security, giving the states the first priority to face threats with less similarity to the conventional conflict. Politically inspired attacks on information infrastructure are the focus of specific limitations of cyber terrorism, which are thoroughly explored in this paper. We discover that, the existing defense construct- intends to address state-base military threats are fatally inappropriate to this new field. The root cause of this weakness is a mere thought-provoking disjuncture between the administrations, which bear a duty of providing national security to the world, and the privately owned and operated massive mainstream of critical infrastructure. By using a qualitative content analysis of major world cyber events evidence, the current paper reaches the conclusion that there should be a radical transition to a resilience-based approach, which is based on the strong Public-Private Partnerships (PPPs). We argue that cyber-terrorism needs to be brought into the national security focus of Pakistan, and other states of this kind. The paper ends by outlining a real policy roadmap to the Pakistani government, which includes the requirement of PPPs, a National Cyber Resilience Centre, and systemic legal and education reforms, and responding to newer issues such as AI-generated attacks and quantum computing vulnerabilities that will become the staple of cyber hostilities in the next ten years.

1. Introduction

The world is experiencing a paradigm shift in human history due to the vast digitalization of daily life. The former means of communication has become, in reality, the very foundation of our modern society of the financial markets, the medical system, and even the national defense systems.[1] Such disproportionate hyper-connectivity has increased speed of innovation and efficiency- however it has also caused severe and far-reaching points of vulnerability- making the cyberspace a major playground of the 21 st century. To national security institutions long accustomed to the territorial constraint of their efforts in terms of conventional military threat- this change requires a principal reconsideration of strategy. In the modern-day global connectivity of the world, the attacks can be cross border in nature because they happen immediately, this is; they do not adhere to the normal defense strategy but instead intercept the digital system and sensitive information that enable a country to function itself.[2]

Such a digital transformation has created what according to the security scholars is the gray zone of conflict- an operational terrain that is neither peace nor an open war but in which both state and non-state actors engage in sustained operations without any limitations to crossing the thresholding of traditional military operations.[3] One of the grey zone that have been particularly problematic is the cyber-terrorism which has been using the anonymity, rapidity and international coverage of digital networks to accomplish strategic objectives without necessarily facing the conventional military retaliations. In this regard, the same networked digital platform that has enhanced the effective functioning of the modern societies has also brought them in contact with the novel platform of vulnerability. There is a growing alarm among experts that there is a wider move toward the weaponization of all things whereby civilian systems can be used in different ways to cause havoc to all societies that depend on them.[4]

The paper will make a stern argument that our policy with regard to national level defense must be undergone major overhaul-in order to continue being successful, it must be wholly aligned with the multifaceted challenges of cyber-terrorism using a model, which would best ensure the proper resilience and practical, operational favouring the establishment of Public-Private Partnerships (PPPs). Why is this so vital? Due to the cyber limitations and conflict, the classic power structure in countries is shrunk. In the meantime, a nation-state cyber warfare headlines the news, the steady and potentially devastating limitation of threat to cyber-terrorism is languishing in a policy vacuum--usually as a criminal impediment, not an action.[5] The historic distinction between high politics (national security) and low politics (crime) has been completely broken during the digital age, and it has left some critical gaps in our defensive posture.

The cyber-terrorism attributes a number of uniqueness to its users such as the credible deniability, rather lower operational cost, global and capability to disrupt on a huge scale without travelling a single physical boundary.[6] The psychological and economic impact of an attack that put a country entire power grid or hospital systems out of commission may be as great as the

impact of the traditional explosive devices. In case a cyber-attack would cause a nationwide power outage that would last some time, the impact of such an event would rapidly spread through its most vital areas, including water supply, sanitation, healthcare, and logistics. Not only would the resulting agitation cause a humanitarian crisis, but it would also bring about a serious loss of authority and credibility of the state. Nevertheless, in Pakistan, as in most other countries, the response has been kept, principally in the area of law enforcement and intelligence services, which is not a strategic response to the issue.[7]

Central to this problem is there is an apparent discrepancy between the old security policy and the conditions of the modern threat landscape. Concepts like deterrence that have been practiced long before are no longer effective as they once were since concepts of reliable attribution and the concentration of critical expertise in state institutions are no longer as effective as they used to be. And in reply, the paper moves to a Whole-of-Nation, approach to cyber defense that does not focus on the search to get absolute protection and move towards more resilience the capability to predict, threats, absorb shocks and recover effectively to an attack. This thesis is that this resilience can be constructed only by agile, legally sound, and mandated Public Private Partnerships (PPP). It has been analyzed that first of all indicates the weaknesses of traditional security models, followed by how effective alliances can be designed, evaluates the emerging technological issues, and finally offers a series of useful recommendations in the form of policy suggestions that would be specific to the security environment of Pakistan.

2. Literature Review and Theoretical Framework

2.1 Defining the Threat: Cyber-Terrorism and Critical Infrastructure

To put this analysis in context, it is important to define the concept of cyber-terrorism, in this paper the term will imply a deliberate application of cyber capabilities, with political or ideological motives, to attack information systems in a manner that can result in violence, extreme economic or strong psychological pressure that may cause mass fear in the society.[8] This definition was deliberate to disregard the activity of the typical cybercrime and smaller-scale digital offenses, but rather the actions aimed at producing the terroristic impact. The technical approach taken to instill cyber-terrorism is not what distinguishes it as other malicious cyber activities, but with the sole purpose of gaining financial gain.

The conceptual boundaries of cyber-terrorism are controversial in the academic literature and does not provide a definitive opinion on where the boundaries of cyber-terrorism are intended to be made. Although in literature there are authors who claim an expensive interpretation, which includes a broad spectrum of politically motivated hacking activity (e.g., Myriam Dunn Cavelty), others are much more restrictive (e.g., Thomas Rid, who states that there is a necessity to draw a line between digital activism, cyber espionage, and an activity that actually represents terrorism in the cyber realm).[9] This paper fits into this latter strategy. It focuses on cyber operations aimed at instilling fear by causing massive disruption or destruction of critical systems, as opposed to

manipulation or intelligence-gathering operations on a wider basis. This discrepancy is not just a matter of abstract conception; it has an immediate inference into the law and policy. Tactics that will be used to combat the low-level hacking or an average cybercrime will not help against ideologically driven individuals who have a mission of destabilizing the society at the expense of personal gain.

Critical infrastructures (CI) are the main targets that have often been linked to these attacks; It is a complex and network of a system whose failure would result in severe implications on the security of the country at the national level, the economy and the people.[10] Examples of sectors that are in this category are electricity grids, financial markets, and water treatment facilities. The weakness of these resources is not the topic solely of obsolete technology and weak cyber protection but one of a more profound structural issue. In most developed economies, 85 to 90 per cent of key infrastructure is owned and run by the privates.[11] Consequently, a core conflict arises- governments are eventually responsible to provide security in the country. In many cases, they do not have direct jurisdiction over the same systems which such security is based on- a situation which may be interpreted as a sovereignty paradox.

This organization generates a distinct and very succinct conflict- as far as the national level security is a mandate of the state enshrined in the constitution- but the capacity to control the most sensitive resources is widely vested in the hands of the private players. The information, network access, technical expertise, and physical infrastructure used by these actors possess the relevant data, would be targeted in a major cyber-attack..[12] Since, as Ben Buchanan in The Hacker and the State notes, this is in fact the role occupied by corporations, although they were never designed, or rewarded, to game in that way. Corporate interests, competitions, profit and the privacy of customer information, often do not sit well with the demands of government as far as sharing of information, supervision and control over its operations. The space between these conflicting urgencies is not neutral- It is in it, with its lack of trust and conflicts of interest, that cyber-terrorist actors find the greatest opportunity to pursue vulnerability. [13]

2.2. Theoretical Underpinnings

In order to get a deeper insight into this issue we have focused on three theoretical lenses that offer a combined insight on the matter at hand and form a complete framework of the analysis:

Securitization Theory: This was developed by the Copenhagen School- the theory is how some of the problems get to be conceptualized as existential threats as a justification of exceptional actions which are not subjected to ordinary politics.[14] Based on the given view, cyber-terrorism is no longer something that requires a regular policy approach, the extent to which it can disrupt and the character of the treat suggest that it has slipped substantially into the category of issues that warrant emergency level responses. Securitization of cyber-terrorism is the prerequisite to marshal the political will and resources needed to effect the radical policy shifts that are being postulated in this paper. Once securitized, the issue needs to be addressed by exceptional means and no longer

subjected to the normal bureaucratic procedures, which is the very thing that the cyber-terrorism threat needs to be approached with, as it could inflict a devastating damage.

Resilience-Centered Security Framework: This framework has a drastic shift in security conceptualization, as opposed to the unrealistic pursuit of comprehensive protection; it focuses on the ability of the systems to resist disruption and adapt to intensive conditions and keep on functioning.[15] The focus on resilience must not be seen as an adoption of defeat, but rather as an example of a realistic approach toward the constraints of prevention in complicated digital environments. In a broader sense, this means adding redundancy, fail safe procedure and other defined recovery process with the acceptance that some intrusion is inevitable. In this regard, regarding the cybersecurity, the resilience-based model is largely relevant as it incorporates the probability of the unavoidable breach, and is focused on the conservation of the crucial operations and the mitigation of damage. By doing this, it takes the emphasis off anticipation as such towards a more complex and resilient model of security, one that could be defined by military planners, as a defense in depth, with a number of safeguards and back up capabilities that reduce the likelihood that any one point of weakness could lead to systemic breakdowns.

Cyber Power Framework: This is a theory that was formed by other scholars like Joseph Nye that make us view the cyberspace as an extension of power that is practiced in similar domains as the traditional domains, which are, land, sea and air.[16] This model shows that cyber-terrorism manifests not so much as unselective digital vandalism, but as the projecting of power. This model illuminates this approach to explain the strategic reasoning of using cyber proxies by countries - such model provides a relatively inexpensive means to achieve political goals with some level of deniability. In situations like North Korea, this theory applies because it invests in cyber capabilities, which support an asymmetric instrument that fills the shortcomings of conventional military capabilities. Likewise, the cyber-security theory illuminates the strong force of non-state actors, who can now apply pressure and restructure the results in a manner previously solely dominated by the states, thus redesigning the pattern of international security environment.

Lastly, combined, these theoretical perceptions provide a diagnostic toolkit that is comprehensible. The theory of securitization is the reason behind cyber-terrorism being maintained as an issue that cannot be addressed with the same degree of political attention. A resilience-based approach also assists in outlining the planned purpose, which seeks to focus on persistence and recuperation instead of perfect foretelling. The Cyber-power theory, in its turn, positions the state and non-state actors in the vast strategic landscape, in which cyber security are occurring. This combination enables a further stratification of empathetic of cyber-terrorism and its implications and eliminates the constrained technical solutions to the issue, and focuses on the overall political and strategic elements that define both the threat and the response measures that exist.

3. Methodology

To the strength of the said arguments that are empirically based, this study is based on qualitative analysis of significant cyber incidents, relying mostly on the Center of Strategic and International Studies (CSIS), yet with Significant Cyber Incidents as the primary source of timeline. This timeline is an extensively-documented list of high-impact incidents and is especially informative to educative to track the recurring patterns, operation procedure and general geopolitical incentives around such events. Moreover, a qualitative content analysis is used to analyze textual data, facilitates a systematic process of interaction with fact and figure with the help of coding and narrative analysis.[17] This approach is stronger when it comes to the aspect of modeling the intricacy of cyber-terrorism- which cannot be effectively described using the prism of quantitative indicators only.

3.1 Data Collection and Research Design

The key objective of the analysis was to construct a consistent narrative analysis out of formally documented cases- enabling the paper to investigate the practical implementation of cyber-attacks in practice as opposed to theory. Here, the CSIS timeline present all inclusive and credible and systematically assembled records of cyber events that have definite strategic implications and with high strength of a national security implication.[18] Not only is the efficacy of its reporting the strength of the CSIS, but also its timeframe, as it allows tracing the cyber incidents since 2006 can allow an analysis of the changing trends and strategies, targets, which could serve as an important frame of reference in terms of determining how the cyber vulnerability evolved over the years.

Moreover, our research will not be based on a single piece of evidence rather the CSIS data have been cross-examined with a broad array of other sources such as peer-reviewed scholarly sources, governmental official publications published by national cybersecurity agencies, widely published media articles, and technical analysis reports published by major cybersecurity companies. This triangulation process was to reduce the adverse effects of depending on the possible bias of single source and to overcome the weaknesses that are inseparable with single source. Lastly, these resources provide an insight into a more multi-layered interpretation of every cyber-event. Practically, the CSIS will often provide a cursory summary of an incident, whereas technical reports which have been released by companies like Mandiant or CrowdStrike can give insight into the methodology, techniques and framework used to conducting the analysis. The government publications often provide an extra dimension of provenance, which, however, allows positioning an individual attack in the broader context of strategy and politics.

3.2. Data Selection Criteria

the analysis has not tried to reflect every recorded incidence of cyber related aspects- in order to maintain a clandidine focused focus on matters that can be relevant to the national security, the cases have been chosen based on a set of pre-established criteria.

- Only the incidents that were related to cybersecurity and in which the target was a government institution, a defense related organization and damage to infrastructure or economic activity with the losses of more than one million dollars were considered. This was set in place to make sure that the analysis focused on those events that had a broader national security consequence- not just individual cases of victimization or limited crime but large-scale.

We placed more emphasis on the incidents that have a good attribution to a state or a well-organized group- formed with reasonable confidence. The issue of attribution on cyberspace is complex in nature, and the study does not make it conclusive. Still, cases that were evaluated with moderate to high confidence by well-known government agencies or reputed cybersecurity companies were selected first- because the information would be more precise on the motive, capabilities and strategic actions of the involved cyber actors.

- We have given precedence to the techniques of attacks- including phishing campaigns, ransomware implementation or supply-chain breach in the sample. These demands facilitated a systematic study of the way various actors change their approaches over time among incidents.

This change made sure that the analysis paid attention to events that have physical implications to defense and security related policy- but not viewing cybersecurity incidents as a technical episode. Lastly, it also allowed one to compare tactics and its result in a unique political and operational environment in a uniform process. The selection process focused on incidents that represented a meaningful innovation in the method of attack, left a lasting impact on the world or had specific signals in the overall context of geopolitics.

3.3 Data Analysis Process and Limitations

We conducted our analysis in multi-stage and applying the common strategies to qualitative content analysis in national security literature. At the preliminary phase, we coded the incidents based on their initial targets, objectives and the participants and the technique used by them- this categorization enhanced systematic framework of comparison among the different incidents. Recurring themes in the data were then coded, especially considering variations in attack vector and how they were correlatable with overall geopolitical trends over time. Also, as a result of this narrative coding process, we identified certain patterns with regard to the preferences of targets, the degree of technical sophistication and how cyber activities are congruent with the time frame of more widespread geopolitical stresses.

In the last stage of the analysis, the patterns that have been identified were researched within the context of their wider political and technological contexts to evaluate underlying motivation and policy consequences. The prioritization of incidents on the context of a particular situation is crucial to substantial derivatives to, by example, a cyber operation against Ukrainian infrastructure during a military conflict with Russia indicates a distinct set of policy orientation as opposed to a relative attack organized on the systems of a state not engaged in a military conflict.

The use of our methodological framework is limited to some extent, first of all, the attributions in the cyber domain is not clear or explored but is usually involved in political and ideological issues. Moreover, the publicly accessible documents about the events are always incomplete since numerous events remain unreported because of privacy issues or because of active government repression. Although a qualitative design can be interpreted in detail and be contextualized in depth- however it cannot provide statistical assurance. We have recognized all these limitations- but the common themes that have been found throughout well-documented cases are very valuable in policy analysis. This study is not aimed at quantifying measure regarding cyber risk- but illuminating the strategic space within which cyber operations are practiced and pointing out the weaknesses of the current security policy. A close examination of major incidences even in the absence of a comprehensive data can provide insights, which are credible and influential to policy makers.

4. Analysis and Findings

The summary of the cybersecurity events during the last ten years suggests that there are recurring patterns that raise the question of how effective the traditional defensive models are- and suggests the difficulty is not the emergence of a new technical means, but is the urgency of a type of conflict that follows a different logic. The answer to it, in its turn, will involve the reevaluation of long-standing beliefs regarding the security, sovereignty, and even the essence of defense.

4.1. The Reason Conventional Teaching is Failing

The formulated national security approaches have been grouped into three main areas that cut across the core of the conventional national levels security models. Among the most important and important issues to be considered the logic of military deterrence, which traditionally has been based on the believable threat of retaliation. However, in cyberspace, as it were, this concept is hard to maintain, attribution is often postponed, contradicted and can be subjected to conscious manipulation. On the same note, advanced actors actively exploit proxies, multiple operations and misleading signals - confusing the task of determining accountability and interrupting the political decision-making authority. The 2014 intrusion involving Sony Pictures—marked by competing and disputed attribution claims—illustrates how these dynamics can undermine a state capacity to respond authoritatively. Where duty members are unable to be familiar with sufficient self-confidence, the inhibitory impact of retaliation is greatly worsened.[19] Some experts have characterized this impediment as a deterrence paradox the characteristics that render cyber operations desirable by the adversary ambiguity and deniability which damages the feasibility of conventional deterrence policy. Instead, nations are left in the position of possessing effective reactive possibilities but not knowing how to control them with confidence, when and with whom to employ them.

Second, the idea of protecting the sovereign territory is virtually useless in this case. The digital attacks have an easy way circumventing borders so that the security of the nation should extend to

the system of the whole corporate system where its most important resources are located. The battlefield has become omnipresent, as does a control system of a power station in Karachi or a banking transaction server in Lahore, the majority of which are privately owned and out of the personal control of national defense. This refers to a critical limitation to the Westphalian perception of sovereignty that has strengthened international relations over durations of time. As an attackers can disrupt the critical infrastructure of a country using a server in a third country and sitting in a fourth country, our traditional ideas of maintaining territorial defense are no longer very suitable.

Another pressing dilemma is the disparity in working surroundings whereby the traditional defense agencies, endowed in longer procurement processes, and evaluated decision-making authorities, have difficulty in keeping pace with the threat groups who may develop and arrange fresh adventures within hours in a country. The 2017 WannaCry outbreak proves this issue, the virus exploited a known vulnerability that most of the administrations, including the governmental ones, have not fixed yet mainly because of bureaucratic delays and complex upgrade process.[20] On the same note, non-state cyber actors, in their turn, have the ability to operate with such a liberation, such agility, which these bureaucratic assemblies are not adequately prepared to rival. This tempo difference enables the attackers to adjust and become innovative more quickly than the defenders, and poses a lasting operation advantage.

4.2 The Critical Infrastructure Bullseye and The PPP Imperative

The conclusions made are that critical infrastructure is not only a target, but a key location in modern cyber operations. Such patterns of attacks appear considerate- targeting these systems gives an opportunity to make a large-scale disruption as well as enhancing the psychological impact beyond the actual location of attack. The evidence is intriguing and has a vivid development to an infrastructure failure that leads to cascading effects on the services offered to the population, societal stability, and economic activity. This change of targeting can imply a strategic reasoning which is aimed at maximization, not at incidental damage.

- In 2015 and 2016 such attacks as the one on the Power grid in Ukraine which was suspected to be carried out by Russian state-related actors linked to Sandworm group signified a shift in the utilization of cyber operations. Such particular events demonstrate that the use of cyber activity might produce direct tangible effects: hundreds of thousands of civilians are deprived of power when it is winter. It also reflected a high degree of technical sophistication in the operations especially the ability of the attacker to transition between corporate information technology settings and industrial control systems that were used to operate physical infrastructure.[21] These attacks were not aimed at causing undercover operations or data theft like the previous cyber disruptions, but to cause physical disruption to normal lifestyles. Thus, they blurred the line between computerized operations and the conventional warfare.

- In 2021, with the Colonial Pipeline ransomware attack, it was seen how the troubles of a single private firm can easily escalate to a national security incident of its own, causing shortages and panic buying of fuel and a federal emergency declaration. The company was forced to pay a multi-million-dollar ransom, which underscores the financial motives behind such attacks and at the same time provided devastating economic security implications on a national level.[22] This case is an ideal example of the sovereignty inconsistency, because the decision of a private company to pay the ransom (to the cybersecurity matter) had direct and practical consequences on the national security, but the government could do very little to influence the decision of that specific case.
- The Solar-Winds breach showed an even greater weakness, hackers had access to thousands of supports, operated by organizations, including major US governmental agencies, by breaching one, large, trusted software provider. [23] This event demonstrates that, our national security is as weak as our poorest digital connection to the global supply chain. It showed that intruders could go massively large by capitalizing on the trust that is vested upon us by our daily digital life. In that regard, the SolarWinds incident is a paradigm shift of the way attacks are conducted; rather than focusing on attacking, attackers attack the trust connections, which make our digital infrastructure stronger.

The result of this trend is a distinct entrapment of where the national cyber defense is where it is needed most, private-sector now lies in the heart of it, but not intentionally but by default. Meanwhile, there is still a continuing cultural and institutions conflict, that is, companies can be afraid of information sharing due to reputation issues, potential liability and competitive loss, and governments might face the problem of not being open to the sharing of intelligence or operational information. What has come out is a structural disjoint in coordination and trust- in this vacuum of misaligned incentive and lack of information sharing that attackers can best exploit and adapt to.

Such an ambition towards what can be referred to as a whole-of-nation approach is therefore the key to the real resilience. Relying on informal or even voluntary support is not sufficient considering the magnitude and pace of modern cyber related threats. Rather, both the public and the private partnerships should be made official in terms of legal descriptions that are capable of ensuring long-term affiliation. These efforts must enable collective, real time threat evaluation and operational reaction, as opposed to restricting collaborative collaboration to what is required and notified afterwards of a subsequent incident. Properly formed, these partnerships may facilitate advance planning and shared responsibility with the participation of the actors on the private-sector level becoming active participants of national cyber defense, instead of simply being vulnerable points [24] for this model to be an efficient—information sharing alone is not adequate. Effective work between the state and the business means clearly defined roles: legal

protection of mutual data, and consistent joint training, so that trust and familiarity with the work are built before the crisis manifests itself.

4.3 The Evolving Playbook and Geopolitical Game

The cybersecurity threats are dynamic in nature and not fixed-end because the adversaries have continuously changed their approaches, which depress the defensive models. Another prominent trend has been the increase in the significance of Advanced Persistent Threats (APTs) sustained and well-coordinated campaigns by legitimate actors. It is a patient, covert operation, where ticking time bomb can be left in networks over long durations, even months, and even years. Latent risks are hidden in such persistence and can only manifest themselves when needed. Conventionally, this kind of activity does not fit well with perimeter oriented defense strategy because APT operations are oriented towards a long term access and strategic placement than disruption. In this respect, their techniques were more related to the intelligence collection activities rather than the conventional cyber-attacks.

The development of Ransomware-as-a-Service (Raas) schemes has been an indicator of an extensive professionalization of ransomware operation the scheme demonstrates a technically skilled developer design and maintenance of ransomware tools that are subsequently sold or leased to non-technically competent affiliates. The result of this is a more organized criminal ecosystem that lowers the technical barriers to entry and maximizes the scope of ransomware attack both in the public and private sectors. The result of this commercialization is a significant change in the cyber threat landscapes - what used to take more technical experience is now available to a far broader set of parties - greatly increasing the pool of potential attackers and the overall volume of the threat.

Most vocal, cyberspace has turned into a geopolitical weapon, the timing of major incidences is often congruent with the time when the political or kinetic pressure is heightened. An effective example of a hybrid warfare is Russian cyber campaigns on Ukrainian energy, financial, and government infrastructure, which is easily combined with cyber and kinetic operations to intimidate an enemy.[25] North Korea's brazen theft of cryptocurrencies is a clear case of cybercrime being employed for a state persistence and sanctions evasion.[26] Such are not crimes of unreachability, but instead they are a tool of national security policy, which serves to state that cyber-power has become an important device of rule. We also have the birth of what some scholars call liminal warfare - the processes that are deemed to remain below the point of armed conflict yet achievements of strategic intention through the mounting of pressure and standardization of intrusion.

5. Threat Landscape Future: Future Challenges.

When looking into the future, it is possible to expect the appearance of even more technological expansions that will complicate the cyber-terrorism landscape. These technological developments are creating new attack sources and new entry points- most of which are beyond the assumptions

that the existing security models are founded upon. Consequently, the current strategies might not be adequate to counter the manifestations of risk that start emerging.

Artificial Intelligence (AI): Developments in artificial intelligence are reinventing cybersecurity in both directions. On the defensive side- AI tools will be able to further improve the effectiveness and speed of threat detection and enable a faster response. Simultaneously, these technologies are also becoming incorporated in offensive activity. They are being actively exploited to enhance social engineering, create content in bulk that is misleading, automate the exposure discovery process, and assist malware that will adjust its behaviour in response to detection. The first instances can be observed in AI-enhanced phishing campaigns where the messages are created to continue addressing individual targets with a high level of realism. In the future, it is even conceivable that more sophisticated systems will be able to independently organize multi-stage actions, choose targets and exploit vulnerabilities with only slight human control.

Quantum Computing: Cryptographically suitable quantum computers are still in development, but they are observed to represent a threat to the existing encryption standards. Encryption, on which much of our digital security, including secure communications and financial transactions, is based, could be violated by quantum computers, and this is not only a threat to future communications, but also to already gathered encrypted data, which a future attacker may be storing to be decrypted later. The shift to quantum-resistant cryptography was viewed as one of the greatest cybersecurity challenges of the next decade.

Internet of Things (IoT) Proliferation: The unstable increase of the number of connected devices significantly increases the surface attacks. A large number of IoT inputs possess insignificant security topography and are unable to be readily repaired or updated. Such powerless devices could be recruited into botnets to be used to issue reckless attacks or to be the gateway to more sophisticated systems. This weakness is propagated by the physical systems because, as more and more critical infrastructure systems are changed to include IoT devices to monitor and control them, real-world systems suffer the impact of the vulnerability.

Space-Based Assets: With the increase in reliance on satellite networks to communicate, navigate, and observe the earth, the space-based infrastructure is now a major target of society. On the same note, attacks on satellite networks would affect all other communication, financial transactions, and emergency services in the military. The space mobilization and the emergence of anti-satellite competences indicate that space is going to be an increasingly disputed sphere in cyber war.

These new realities underscore the fact that the threats environment will only keep evolving - need to respond with adaptive and strong national security policies as opposed to the single-threat single-policy response.

6. An In-depth SWOT Analysis: The Pakistani Situation

These threats are multiple and real-time possibilities to Pakistan, which is not abstract. A SWOT analysis, organized in a systematic way, gives us an understanding of our weaknesses as well as our future prospects of upward growth and increased strength besides having a clear picture of our status, and what we have to do.

Strengths

- **Increasing Institutional Awareness:** The development of the institutions such as the National Centre of Cyber Security (NCCS) and the announces of the National Cyber Security Policy (NCSP), (2021) indicates the solid awareness of the issue at the policy level. These developments support a central backup of remodel a more energetic cyber defense climate-goals which cybersecurity has become a subject of cabinet-tier debate provide a significant advancement even ten years afterward.
- **Large Tech-Savvy Youth Population:** The population of Pakistan is composed of a large number of young people that are already well-informed about the digital technologies making them a big pool of potential related cybersecurity talent. The specified interventions possibly include training programs and the suitable incentive procedure to help the specified part of the population in a manner that, may have a crucial role in enhancing national cyber defense both in terms of public institutions and the private sector. This human capital base is a significant strategic resource to national level cybersecurity- namely, because competition in the cyber domain is increasingly driven by the ability to have skilled personnel and not necessarily technological capability.
- **The Prevention of Electronic Crimes Act (PECA) 2016**: This law provides a framework of permitted agenda on prosecuting cybercrimes- a critical first step, which is mostly missing in mostly developing countries. Although it mandates the use of apprises, it provides the legal framework of taking action against cyber-terrorism and other related offenses. The presence of any legal agenda makes Pakistan a step in advance to various legal preparations among the regional complements.
- **Active Military Cyber Command:** The establishment of a dedicated cyber facility of the Pakistani military organization demonstrates the understanding of the danger on the highest-security tiers and provides the institutional framework of creating military-level cyber skills to protect the country. This refers to a sizeable institutional guarantee to organize cyber defense aspects.

Weaknesses

- **Fragmented Institutional Responsibilities:** The dispensation of the responsibility of cybersecurity in the case of Pakistan is found in multiple administrative bodies such as the Pakistan Telecommunication Authority (PTA), the Federal Investigation Agency (FIA), the National Centre for Cyber Security (NCCS) and lastly the ministry of Information Technology

and Telecommunication. Practically-these bodies frequently are not visible as lines, and so create confusion as to the responsibilities and authority, this disintegration can create the problem of coordination, institutional drawbacks and slow reaction to cyber actions. Lack of a well defined chain of command in cases where nationally significant cyber attack has occurred, further erodes concerted efforts. In the long run, this inconsistency is a structural vulnerability which can be taken advantage of by strong rivals.

- **Poor Financing and resource distribution:** Generally, in Pakistan, cybersecurity is not a priority compared to the archaic security demands in budgetary allocations. This leads to budgetary underfunding, technology lag, inability to retain talented individuals in the agencies and inability to compete with the private sector in regard to recruitment of the best and most talented cyber security employees as the compensation and career prospects are usually better in the private sector. There is resource disparity between Pakistan and its prospective enemies posing a long-term severe strategic weakness in the cyberspace.
- **Poor Public- Private Cooperation:** The existing partnerships between the state administrative and the corporation are highly inappropriate and voluntary. No transferred structure of information distribution or information-sharing response is in place--and serious infrastructure housed by private telecommunications, banking and energy industry might be left exposed and working alone in countermeasures to national defense purposes. Such inability to integrate portrays a critical layer in our national defense.
- **Low Public Awareness and Cyber Hygiene:** There is still a general level of lack of knowledge about the daily cybersecurity practices of most of the population, both households and small and medium-sized business and even a portion of the government segment. Consequently, such an easy method of attack like a bogus site, phishing, and social engineering remains successful at a high percentage- indicates that this is not a technical malfunction that is the fundamental cause, but a longer-lasting lack of awareness and everyday digital habitude. Human vulnerability in this regard is already a foreseeable area that more advanced cybercriminals will use to cause damage to a business, which not only substantiates the fact that people and not technology are the most vulnerable aspect of the cybersecurity landscape.

Opportunities

- **Leapfrogging with Modern Technologies:** Pakistan, as a relative newcomer to adopting inclusive digital infrastructure, can designate and adopt state-of-the-art security designs (such as Zero-Trust) in new digital politics framework in the first instance instead of retrofitting security into old product systems as most developed countries must, this possibility of technological advancing tree of thought denotes a great strategic choice in regard to cybersecurity environment on the national level.

- **Regional Leadership (RL):** Although, building and enhancing a robust cyber defense ecosystem, the Pakistani country has a historic opportunity of becoming a regional leader in cybersecurity within the south Asian region and the larger Islamic continents. This would enable the International position of Pakistan at the time when cooperation avenues are provided via capacity-building efforts, technical support and cyber diplomacy. It has strategic potential in this leadership that demonstrates a significant opportunity of Pakistan—the ability to turn the potential of domestic cyber security into the opportunity of regional impact and strong power base.
- **Economic Growth and Secure Digitalization:** A long history of investing in cybersecurity might become empowering in the wider digital economy of Pakistan, where robust security agenda can support any self-belief of foreign investors, and specifically denser areas of the emergent economy such as fintech and e-commerce, where trust is a precondition to longer-term economic growth. On the same note, the proliferation of cybersecurity capacity leads to possibilities of domestic firms emerging in this domain to innovate services and products in the field- helping to cut unemployment and technological progress. Lastly, cybersecurity must not be limitations to a defensive cost, but a platform towards long term and long strategy economic growth.

International Cooperation and Assistance

International Cooperation and Assistance (ICA): Today the geopolitical location of Pakistan and the current relations with other states in the field of international relations opens a significant opportunity to engage in international cooperation against cybercrime, including the participation in the activities of higher capacity-building interventions, technological assistance, and organized system of intelligence exchange with other states and international organizations may significantly strengthen the national cyber defense environment. These kinds of corporations are largely useful in sealing the expertise and resource gaps - like assisting Pakistan in speeding up the process of building capabilities, without footing the entire bill on its own.

Threats

- **State-Sponsored Espionage and Disruption:** Pakistan has traditionally been the target of advanced persistent threat (APT) groups who are state-type and are based in the region and globally. The primary interests of these actors include access to military planning, sensitive government communications, exclusive technologies and information regarding robust infrastructure systems. In contrast to opportunistic cybercrime, the defining features of such campaigns are long time horizons, meticulous reconnaissance, and long-term access, which is far outside the range of the protection capabilities of most current security schemes. The magnitude, purpose and technical sophistication of such operations pose challenges that cannot be handled well through conventional cybersecurity controls.

- **Proxy Cyber Warfare (PCW):** In Pakistan the Non-state actors and terrorist groups- possibly sponsored and subsidized by the enemy states, may employ cyber-terrorism tactics to attack the Pakistani CI- in order to generate social conflict via misinformation campaign, or finance their actions via cybercrime. The case of traditional proxy warfare in this threat field that Pakistan has witnessed is quite alarming, and it is likely to enter the digital arena.
- **Critical Infrastructure Vulnerabilities:** The financial institutions, telecommunications systems and energy sector in Pakistan are fast undergoing the digitalization process - often ahead of making sound investments into security. With such segments entering closer interdependence the danger of cascading failures in one set of sectors has a significant influence, or rapidly affects others. In the meantime in the context of Pakistan, the high rate of digital transformation has resulted in security debt which has a large share of vulnerability in the country.
- **Ransomware Epidemic:** The Pakistani Public institutions and private enterprises are becoming more vulnerable to ransomware attacks, which already severely disrupted the global order in many ways. In the meantime, such events can have a long-term disruptive effect on the hospitals, undermine utilities and business activities to cause significant financial losses and disruption of important services. In the vast majority of cases, the weak data backup system, as well as the incident response system, which is highly significant in increasing the effects of such attacks, places organizations at a disadvantage and has little to no choice after the fact that the system has been compromised.
- **Digital Divide and Skill Gap:** The pace of digital adoption is currently already much faster than that of cybersecurity world and user awareness, resulting in a growing digital divide between the current technological level and security standards. This asymmetry creates exploitable vulnerabilities, which are exploited in a more fundamental way by the adversaries, the lack of trained person and institutional capacity has become a structural constraint to the capacity of the country to protect its digital systems.

7. Policy Recommendations in Details

It is on the basis of this evaluation that the paper has come up with an action plan of recommendations to Pakistan economy. These actions are designed in the form of a step-by-step roadmap of short-, medium- and long-term priorities, focused on the gradual reinforcement and upgrading of the cyber defense posture in the country.

1. Let It be Lawfully-Enforced Public-Private Partnerships (PPPs): Pakistan requires a genuine legislation which goes beyond friendly discussions- this would entail creating a formal plan with enforced flow of information and indemnity against those who do invest in certified security system and a crystalline-clear positioning of the private sector in the event of a national scale affair. Identify particular industries such as, energy, finance, telecom, transportation to be implemented initially with gradual development. Such alliances must not simply limit

themselves to mere information sharing but also joint drills, coordinated vulnerabilities tests and well-defined procedures of the cooperation of the public and private in case of incidents at the national level.

2. Establish a National Cyber Resilience Centre (NCRC): Pakistan should have a committed national nerve centre; a 24/7 facility to be manned by government agencies and the business sector professionals. Its main role would be the partaking threat intelligence as it develops and organizing a coordinated incident reaction and sustaining a continuous evaluation of the system-wide cyber threats. In the event of a cyber crisis on a large scale, this body would serve as the expert on the command level as a whole- allowing quick decisions to be made and a national response that is understandable. The National Cyber Response Center (NCRC) must mandate the formal declaration of cyber emergencies and coordinate cross-sectoral efforts and serve as the only point of contact of international cooperation on cyber incidents with national consequences in Pakistan.
3. Refurbish Our Laws: The Prevention of Electronic Crimes Act (PECA) 2016 had a considerable basis, but is now becoming obsolete in terms of the threat landscape. The law must be revised to contain a realistic and clear defined concept of cyber-terrorism, a concept that is not similar to other types of cybercrime. It should also clear out conflicting and unclear mandates between the responsible institutions, which now threaten to cause delays or blind spots across nation during a major incident. Besides that, the legal agenda needs to increase the demands on international cooperation, most of which concern the cross-border data exchange and mutual legal support. Other potential risks, such as, but not limited to, the application of artificial intelligence in cyber-attacks, should also be predicted in any amendment and establish clear guidelines on defensive cyber operations.
4. Create a National Cybersecurity Human Capital Development Program: This is a human capital issue we need to make cybersecurity part of our education system starting with universities reaching through to the technical colleges and secondary education and in the process develop a long term pipeline of cybersecurity experts. Invest in special training of IT personnel in critical areas and law enforcement and conduct large-scale national exercises to model complex multi-vector attacks to test how we react under the pressure. In this program, incentive of scholarships, industry certifications, and opening career paths should be established to ensure that cybersecurity is a desirable career.
5. Risk-Based Security Frameworks and Zero-Trust Architectures: The history of replacing compliance-based security with risk-based security in government and critical infrastructure. In particular, directive that all operatives of specified critical structure gradually evolve to Zero-Trust security model. The best defence of the immediate neighbouring drive which in almost every instance makes such inroads is this never trust—always verify, mode. The government may

assist in this through the emergence of application guides to customized Pakistani industries, and offer technical support in adopting application.

6. Enhance Foreign Relations and establish Cyber Deterrence Posture: It is impossible to strengthen counter-cyber-terrorism without wider ties with international partners it must extend arrangements of mutual intelligence-sharing with trusted partners and be a more active participant in multidimensional forums like the United Nations and the OIC. where norms of responsible state conduct in the cyberworld are discussed and formulated—Pakistan needs a clearly expressed cyber deterrence agenda that offer credible diplomatic, informational, military or economic retaliations to cyber hostilities. Partnership in the position is clearly crucial to convey the purpose- prevent extreme risks, and deter possible rivals.
7. Create Future threats research Program: Pakistan needs to allocate funds towards specific research programs that focus on the asymmetric emerging risks like artificial intelligence security-quantum resistant encoding, and space-based environments vulnerabilities. These interventions are not aimed at merely reacting to the existing threats- but overcoming the obstacles that will characterize the new stage of cyber conflict. The further development of relationships with universities and researchers in the private sector will be invaluable in the context of new home-grown competencies and the minimization of dependence on foreign forces over the long term.

Conclusion

The digital age has been reshaping the security rules radically. The conventional national defense policies are weak and ineffective in the face of cyber-terrorism because of its bordersless nature and the ability to cause hideous disruption. Within the framework of Pakistan, a complicated geopolitical circumstance and a swiftly expanding cyberspace, the danger is not a probability by any means, but it is an evident and current impediment to the society, as well as to the policy makers. The 2021 ransomware attack against the National Bank of Pakistan and other websites that were destroyed due to government portals are clear examples of the imminent threat of this increasing reality. The trends that we have recognized by studying global events indicate that, in the future, the number of attacks on our critical infrastructure will be increasingly advanced, and the effects that come as a result will be so drastic that they will surpass the traditional security risks in speed and the magnitude of their impacts.

We find that our answer must be equally significant, that we need to re-examine our whole strategy, elevating cyber-terrorism to a central national security agenda, and developing a new Whole-of-Nation posture, which is predicated on resilience. It is not something that government alone should do but rather- a requisite that we tear the barriers that exist between the public and the private sectors and promote the existence of real and working alliances in which both parties bear the equal responsibility of national defense. The theoretical frameworks we have utilized, namely securitization, resilience, and cyber-power theory, all lead to the same policy conclusion

that incremental improvements to already systems will not suffice but we have to go further in order to transformational change where, we are able to conceptualize and have our national cyber defense structured.

Our described policy roadmap is ambitious--yet, it is also applicable and feasible. It demands tutored PPPs, a national Resilience Centre, a legal transformation and a comprehensive degree of investment on our human capital. The price of such an investment is high- but it lays down to the freight of an all-encompassing economic and human price the success of a large-scale attack on our national grid or financial institutions. Considering the fact that a large-scale cyber attack may, in fact, result in economic damage, estimated in billions of dollars, and loss of lives through disruption of core services, the business case behind such investments is quite strong.

It is a big challenge but a big opportunity as by acting in a strategic prudence, Pakistan can not only be able to have its own digital future but also emerge as a leader in cyber security in the region and south Asia. We possess the information awareness, we possess the rich talent and now we must be changed on efficient way. The moment has come and it is no tomorrow but today to take the comprehensive action. We should be clear: it is time to take action. We cannot afford to await some cataclysmic event to demonstrate the need of these reforms by the experience which is destructive. It is the strategic foresight that has to propel us today. The policies that we adopt now will either make Pakistan the master of the digital world or a victim of the same. It is our decision but the time to make it proactively is fast running out.

References

Abbas, Hassan. "The Dynamics of Terrorism in Pakistan." *Journal of Strategic Studies* 29, no. 2 (2021): 101–125.

Ahmad, Saima. "Cybersecurity Policy in Pakistan: Challenges and Prospects." *Pakistan Journal of Policy Studies* 15, no. 1 (2022): 45–68.

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, 2020.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998.

Center for Strategic and International Studies (CSIS). "Significant Cyber Incidents." Accessed 2025. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge, 2008.

Denning, Dorothy E. "A View of Cyberterrorism 5 Years Later." In *Internet Security: Hacking, Counterhacking, and Society*, edited by Kenneth Einar Himma, 124-145. Jones and Bartlett Publishers, 2007.

Khan, Amir. "Cyber Terrorism and National Security Policy in Pakistan." *Strategic Studies Journal* 42, no. 3 (2022): 55–78.

Lindsay, James R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365–404.

Ministry of Information Technology and Telecommunication (Pakistan). "National Cyber Security Policy." 2021.

National Institute of Standards and Technology (NIST). "Zero Trust Architecture (SP 800-207)." 2020.

Nye, Joseph S. Jr. *The Future of Power*. PublicAffairs, 2011.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.