REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 7, 2026, 63-77

Cyber Warfare and Pakistan's National Security: Lessons from the Russia-Ukraine War for Developing a National Cyber Deterrence Strategy

Muhammad Haroon*[1], Sumaira Gul[2], Abdur Rehman[3],Gul Munir[4]

Abstract

The Russia-Ukraine war offers an important context for understanding how cyber operations can support conventional military activities through disruption, espionage, attacks on critical infrastructure, and information operations. The conflict shows that cyber activities have often been carried out alongside kinetic operations, while Ukraine's experience demonstrates the significance of cyber resilience, effective threat intelligence, distributed digital infrastructure, and cooperation between government institutions and private-sector organizations. Against this background, the present study examines the implications of cyber warfare for Pakistan's national security and considers the lessons from the Russia-Ukraine conflict that can contribute to the development of a national cyber deterrence strategy. The study employs a qualitative research approach using a comparative case-study design. Data wasss obtained from cybersecurity professionals, strategic analysts, and relevant practitioners, along with government policies, official reports, academic literature, and documented cyber incidents. The study draws on Neo-Realism and Cyber Deterrence Theory to explain cyber capabilities as instruments of state power and as important elements of contemporary security competition. The findings highlight several lessons that may be relevant to Pakistan, particularly the need to strengthen defensive resilience, protect critical infrastructure, improve cyber intelligence, enhance coordination among institutions, promote public–private cooperation, and establish credible deterrence capabilities. Based on these insights, the study proposes key elements of a Pakistan-specific national cyber deterrence framework aimed at strengthening national resilience and reducing the strategic risks posed by emerging cyber threats.

Article History
Received 02 September 2026
Accepted 20 September 2026
Published 24 September 2026
Corresponding Author*
OPEN ACCESS

Keywords
Cyber Warfare; Pakistan's National Security; Russia–Ukraine War; Cyber Deterrence; Cyber Security; Cyber Resilience; Critical Infrastructure.

Introduction

For many years, cyber warfare was mainly considered a possible future element of armed conflict. On February 24th, 2022, however, the Russian invasion of Ukraine on a large scale demonstrated that cyber activities had already become a significant component of today's warfare. Cyber operations have been conducted in parallel with actual conflict, such as espionage, disruption of digital systems, information operations, and attacks on critical infrastructure, since the start of the conflict. Russia has carried out a variety of cyber operations targeting Ukrainian entities and Ukraine, too, has put in place a cyber-defence strategy.Russia has also run a wide range of cyber operations against Ukrainian entities and Ukraine itself has a cyber-defence strategy. The ongoing

[1] Lecturer, Department of Political Science & Pakistan Studies, Kohat University of Science and Technology, KP. mharoonkp94@gmail.com
[2] Lecturer, Political Science, Department of Political Science, Kohat University of Science and Technology, KP. sumairagul526@gmail.com
[3] Lecturer, Department of Political Science, University of Lakki Marwat. rehmanmarwat118@gmail.com
[4] MPhil, Qurtuba University of Science and Information Technology, Peshawar, Pakistan / Elementary and Secondary Education Department, KP. gulmunir14632@gmail.com

conflict has resulted in significant data that can be used to study the role, effectiveness, and scope of cyber operations in a modern conflict. The Russia-Ukraine situation has thus evolved into a valuable example of how wars are waged in the digital era.

Pakistan has good grounds to look into the experience of this war in a careful manner. With its longstanding strategic rivalry with India, there is a special requirement for understanding the security implications arising out of cyber warfare. Meanwhile, the digital economy in Pakistan is growing at a fast pace, and its regulatory and institutional framework is progressing at a relatively slower pace. However, the National Cyber Security Policy was approved in Pakistan in 2021, but it was noted that the policy has failed to be effectively implemented and there is no clear framework to implement cyber security deterrence (Eurasia Review, 20222: ISACA, 2021). It gained importance after the attack on Pahalgam on April 2025 and Operation Sindoor by Indian Army, with the cyber activities of Pakistan linked and India linked groups reportedly rising significantly after the attack. These developments signaled a potential for cyber operations to become more widespread, more fast and more harder to track or attribute in the event of such a threat in the near future (RUSI, 2024/ ORF, 2025).

This study does not suggest that Pakistan should simply adopt or reproduce the strategies used by Russia or Ukraine. The international environment of a Russia-Ukraine war differs from Pakistan's security environment in South Asia. However, conflict has a few lessons that can be applied, in particular, the lesson of preparedness, institutional coordination, cyber resilience, and protection of critical infrastructure. Hence the study takes the help of the existing academic research, Policy documents and current reports to find out the lessons from the Russia-Ukraine conflict for Pakistan. The study aims to formulate a practical and context-specific approach towards enhancing the national cyber deterrence strategy in Pakistan based on these findings.

What is Cyber Warfare?

Cyber warfare is the employment of cyber capabilities by a State or other actor for hostile operations in or through cyberspace for strategic, military, and/or political ends. These operations may involve disrupting, degrading, manipulating, or gaining unauthorized access to an adversary's information systems, networks, or critical infrastructure (Schmitt, 2017).

Research Questions

1. What cyber capabilities and strategies have Russia and Ukraine employed?
2. What cybersecurity vulnerabilities currently exist in Pakistan?
3. Which lessons from the Russia-Ukraine conflict apply to Pakistan?
4. How can Pakistan develop an effective national cyber deterrence strategy?

Literature Review

The research study used in this paper falls into three main groups: studies about Russian and Ukrainian cyber operations, studies about Pakistan's cyber security situation, and theories about cyber deterrence.

Cyber Operations in the Russia-Ukraine War

The findings of many studies are the same: Russia's cyber operations both before and during the invasion were far from the level of disruption that analysts predicted. Chatham House (2023) notes that Ukraine had eight years after the 2014 annexation of Crimea to strengthen its defences, so it was far better prepared than it would have been if it had been taken by surprise. The Center for Naval Analyses (2023) takes a more nuanced stance, noting that experts aren't yet sure why the attacks were less effective than planned. According to the separate analysis, published in Technology in Society and summarised by ScienceDirect (2023), the relative success of Ukraine is

due to two reasons: significant support from partner countries and the existence of an already established national cybersecurity strategy before the beginning of the full-scale war.

CSIS (2026) offers more concrete information about the systems used by Russia, such as mobile electronic-warfare platforms like the Leer-3, which includes a drone to jam mobile communications and a system to intercept and broadcast a large-scale propaganda text message. But the same report finds the bigger fault line was the absence of a coherent strategy behind these cyber operations, which in large part accounts for their lack of success. The Lieber Institute (2024) notes that in subsequent days of the conflict, Russia changed its approach, refraining from simultaneous and widespread disruption, and instead "using more subtle methods of intelligence gathering and ongoing pressure against Ukraine's energy infrastructure, often accompanied by the use of missiles.

From the Ukrainian perspective, Microsoft (2022) identified three facets of Russia's cyber campaign: destructive operations within Ukraine, espionage targeting countries that are supporting Kyiv, and information operations targeting audiences around the world. Of these, the information aspect is the hardest to spot and can run for months, largely unnoticed. Lastly, the Atlantic Council (2025) notes that the few sanctions that have proven to have an impact on Russia's cyber capabilities over time are those aimed at the Russian technology sector.

Cyber Security Situation of Pakistan

Most studies on cyber security in Pakistan focus on the National Cyber Security Policy 2021. In 2021, the Ministry of Information Technology and Telecommunication announced that any cyber attack on Pakistan will be considered an attack on the country in line with national and international law.

The policy established a Cyber Governance Policy Committee for national Cyber Security issues (Digital Watch Observatory, 2024). It also advocates better cooperation between the government and private businesses and advocates the development of local technology rather than foreign ones. Most researchers believe that the problem is not the policy itself, but the way it has been implemented. According to a study published in 2022 on Academia.edu and ResearchGate in which Pakistan was ranked 107th out of 131 countries on a global innovation index. This reflects the lack of digital systems in Pakistan to meet threats. The research attributes the failure of the policy to work well to a lack of coordination between government departments.

Similarly, Eurasia Review (2022) notes that the 1998 was a disaster year for Afghanistan. It states that cyber security is still perceived to be only the responsibility of the Ministry of Information and Communication Technology (ICT) and should be handled by the ministries of defence, finance and foreign affairs as well. The policy does not clearly safeguard citizens' digital rights, either. The International Bar Association (2023) is a little more even. It is not clear whether the policy is sound in terms of its implementation and enforcement in Pakistan, which lacks the capacity to do so.

Recent reports of real cyberattacks provide a better picture. Transparent Tribe (or APT36) is a Pakistani hacking group. Since approximately 2013, it has been focused on India Defense, Government and Education sectors (Socradar, 2025; Cyfirma, 2025). Following the attack in Pahalgam in 2025 and Operation Sindoor by Indians, there was a tremendous increase in cyberattacks by both sides. But many of the Pakistani achievements subsequently proved to be untrue or exaggerated (CloudSEK, 2025; Deccan Herald, 2025). This is one of the outstanding facts mentioned by CSIS (2025): Russian hackers have infiltrated a Pakistani hacking group, accessed its own systems and stealing Pakistan government and military data it had collected itself in December 2024. This clearly demonstrates that Pakistan's hackers aren't 100% safe even if they are offensive hackers.

Cyber Deterrence Theory

Deterrence theory was first developed for the use of nuclear weapons, which can make direct application of the theory difficult when it comes to cyberspace. Aslakson and Kempista (2016) tackle this challenge by developing a multi-stage theory of cyber deterrence. They first seek to engage in agreements and sanctions, then to deter through denial, and finally reshape the situation in more powerful ways if needed. However, one of the key issues with cyber deterrence, as Burton (2018) points out, is that a state is unable to credibly threaten an attacker with punishment unless it can determine who was responsible for the attack. It is important to note that the issue of attribution is even more complex when it comes to cyberspace: It can be a lengthy and arduous process to determine who is behind an attack and evidence may be incomplete or inconclusive to prove responsibility in public.

In addition, the study conducted by Senol (2020) about the national cyber strategy of Turkey specifies the significance of institutional coordination. The study suggests that cyber deterrence can be undermined if there is no single, adequately empowered agency tasked with coordinating national cyber security activities. An advisory committee alone is unlikely to give the necessary authority and coordination for an effective deterrence policy in this context.

There has been more recent research which has cast doubt on primary defensive methods. Deterrence by denial, alone, might not be enough to ward off persistent cyber-attacks, suggests the Stimson Center (2025). From this point of view, credible punishment and legal sanctions, and mechanisms to punish, should also be included in effective deterrence, so that cyber attackers can see that there will be real costs if they engage in cyber aggression. Likewise, Georgetown Journal of International Affairs (2024) states that three key components are critical to a successful cyber deterrence strategy: capability, attribution, and credibility. Each of these elements is important, and their lack may render deterrence much less effective.

Altogether, the literature available highlights an important gap in the literature. Most studies on the Russia- Ukraine war and national cyber security policies have focused on either the cyber dimension of the war or the national security policies of Pakistan. There has been a limited attempt to systematically link the lessons learned from the practical experiences of the Ukrainian situation with the Pakistan context and institutional requirements. To this end, the lessons learned from the Russia-Ukraine cyber conflict are analyzed in this study and how they can be translated to create a better national cyber deterrence strategy for Pakistan is examined.

Research Methodology

Research Design

This study follows a qualitative and descriptive research approach based on existing written sources. Since much of the information concerning military cyber capabilities remains classified and the Russia–Ukraine war is still ongoing, obtaining reliable primary data through interviews or surveys would be difficult and impractical. Therefore, the study relies primarily on document analysis to examine relevant evidence and information. This approach is widely used and considered appropriate in security and strategic studies, particularly when dealing with sensitive and evolving security issues.

Data Collection Sources

The sources used in this paper come from four main groups, shown in Table 1.

Category	Examples used in this paper	Purpose
Government and policy documents	Pakistan's National Cyber Security Policy 2021; Ministry of IT and Telecommunication statements	To understand the official policy
Academic and think-tank publications	Chatham House, CSIS, Stimson Center, Lieber Institute, CCDCOE, Georgetown Journal of International Affairs	To provide theory and case study analysis
Threat-intelligence reporting	Microsoft, CloudSEK, Cyfirma, Socradar, Global Cyber Alliance	To track real, current hacking activity
News and regional analysis	Deccan Herald, ETV Bharat, ORF, RUSI, Eurasia Review	To cover recent India-Pakistan cyber events

Method of Analysis

This study applies thematic content analysis to examine the collected information. The data were organised around three main themes: the cyber tools and methods used during the Russia–Ukraine war, weaknesses and vulnerabilities in Pakistan's cyber security system, and the key elements required for an effective cyber deterrence strategy. These themes were then compared and examined across different sources to develop clear answers to each of the research questions.

Limitations

The study has two main limitations. First, information related to cyber conflicts is often exaggerated or disputed by the parties involved. For instance, several claims examined in this study, particularly those reported following the 2025 Pahalgam attack, were later identified as false. Therefore, the study required careful verification and cross-checking of sources rather than accepting individual claims at face value. Second, the research relies exclusively on publicly available and open-source information. It does not have access to Pakistan's classified or confidential cybersecurity data. Consequently, the study's assessment of Pakistan's actual internal cyber capabilities remains general and is based on publicly accessible evidence rather than confidential government information.

Cyber Warfare's Influence on the Russia-Ukraine War

The one thing that the Russia–Ukraine war did not do was to establish a precedent.One of the most surprising things about the Russia–Ukraine war was that it did not set a precedent. Prior to the war in 2022, many experts thought that before Russia would launch a large-scale cyberattack and disrupt the energy system, banks and government bodies of Ukraine, it would be able to do so in the near future. However, such a devastating cyberattack did not take place. Part of Ukraine's success in holding off these significant cyber threats is due to the preparations that were made over the previous eight years since the 2014 conflict, according to both Chatham House (2023) and the Center for Naval Analyses (2023). This time has given the Ukrainian government, public institutions, and private companies an opportunity to bolster their cyber defenses and build "whole-of-society" resilience, as Chatham House calls it. The role of continued assistance from Western technology firms was also a significant factor in boosting Ukraine's capacities to relate to cyber threats.

The Russia-Ukraine conflict has shown that cyber operations have been a secondary force in the military operation, rather than relying on a single massive cyberattack. CSIS (2026) and the Lieber Institute (2024) describe the Russian use of cyber attacks alongside traditional missile strikes,

especially when they were vulnerable, such as during the winter season. This suggests that when cyber operations are aligned with traditional military operations and integrated in the broader planning process, they can be more effective. Their potential military impact, when they are applied individually, seems to be less effective.

There is also a significant political aspect to the conflict which should be examined. Microsoft (2022) noted that Russia has been carrying out persistent influence operations and espionage beyond Ukraine. These activities were directed at allied governments, NGOs and international organizations. Some of these operations went undetected for many years. They did not destroy digital systems directly but had a more general objective of gathering information and shaping political perceptions and public support for Ukraine in the countries providing assistance. Therefore, cyber operations in the Russia–Ukraine conflict have not only been used for military purposes, but also political and strategic ones, too.

Cyber Capabilities and Strategies Used by Russia and Ukraine

- Russian Capabilities and Strategy

Russia has used numerous cyber weapons in the war, such as destructive malware that can wipe data, distributed denial-of-service (DDoS) attacks, mobile electronic-warfare systems, and coordinated information campaigns (CSIS, 2026; ScienceDirect, 2023). An example of this is the Leer-3 system, which CSIS (2026) defines as a mix of capabilities. The system can also jam drones and can intercept mobile communication and broadcast message floods of propaganda text messages. This capability is, in some ways, like the Western surveillance technologies also known as “Stingray” systems.

Another strategy that Russia has employed is to hack into databases and email accounts, then publish the stolen information. In a few instances, the leak material has been modified to boost its possible effects. CSIS (2026), however, found that this was largely ineffective during the invasion- Western intelligence was quick to publish accurate information, and thus Russian disinformation and misleading claims became harder to sustain. As some of the “more direct” cyber operations failed to meet their objectives, Russia shifted to using stealthy cyber espionage and targeted attacks against specifically Ukraine's energy grid, with the idea being to cause problems on a more local level than a national level (Lieber Institute, 2024).

- **Ukrainian Capabilities and Strategy**

Ukraine's response to cyber warfare has largely emphasized defence, resilience, and international cooperation rather than offensive cyber operations. According to ScienceDirect (2023), Ukraine concentrated mainly on strengthening its cyber defences, in contrast to Russia, which used cyberattacks alongside conventional military operations. Ukraine's national cybersecurity plan, developed before the outbreak of the war, also contributed to reducing the impact of cyber threats and helped the country respond more effectively to attacks. However, much of Ukraine's ability to withstand these attacks was supported by international assistance. Western technology companies, particularly Microsoft, provided important support by identifying cyber threats, sharing threat intelligence, and helping to address security vulnerabilities (Chatham House, 2023; Microsoft, 2022). In addition, Ukraine was able to maintain essential communication during periods when conventional internet infrastructure was damaged by relying on satellite-based internet services (ScienceDirect, 2023).

- **Comparative Summary**

Table 2 compares the two approaches side by side. The comparison shows one clear difference: Russia had strong tools but poor planning, while Ukraine had strong partnerships and

preparation but fewer offensive tools. In this war, the second combination worked better.

Dimension	**Russia**	**Ukraine**
Main tools used	Data-wiping malware, DDoS attacks, mobile electronic-warfare systems (Leer-3), leak-and-spread operations	Defensive monitoring, quick system fixes, satellite internet, national cyber response teams
Main approach	Attack-focused, aimed at disruption and fear	Defence-focused, aimed at staying strong and functioning
Connection to military plans	Weak at first; improved later when combined with missile strikes on energy targets	Different types of connection; worked closely with civilian support and allied partners
Outside support	Limited; mostly relied on its own resources	Strong; Western companies and governments gave real, direct help
Result	Limited, short-term effects; did not achieve its main goals	Systems kept working despite repeated attacks

Cyber Security Vulnerabilities in Pakistan

- Policy and Institutional Weaknesses

In theory, the National Cyber Security Policy 2021 might be in place in Pakistan. However, it has not been used effectively. Eurasia Review (2022) writes cyber security is considered solely a concern of the IT Ministry despite a robust impact on defence, finance, and foreign affairs. It also notes that the policy lacks clarity in defining citizens' digital rights. The study (2022) for the Academia.edu and ResearchGate communities is more straightforward. It states that the government offices in Pakistan aren't well organized and thus their policy is not strong from the top.

- **Digital Infrastructure Vulnerability**

Every year, Pakistan's digital banking, telecom, and online government services continue to be utilized more. This makes it easier for invaders to strike the country. According to the same 2022 study, Pakistan's rank in the list of 131 countries on a global innovation index is 107. It also states that Pakistan is exposed to malware around 18.94 percent per month. The study anticipates that this figure may be even higher since the outbreak of the COVID-19 pandemic has spurred additional services to shift to e-services.

- **Active External Threats**

Pakistan is involved in the cyber conflict with India in two capacities: it is the source of cyberattacks, and it is infrequently mentioned that it is also the target of such attacks. APT36, which has been around since approximately 2013, is the most persistent Pakistan-based hacking group. It has targeted the defense, government, and education industries of India (Socradar, 2025; Cyfirma, 2025; ORF, 2025). But Pakistan is not fully safe, either! A Pakistani hacking group suffered a breach in their own system by Russian hackers in December 2024, according to CSIS (2025). This group gathered government and military information from the South Asian country, which they stole. This is an example of how a country cannot be well protected with the help of offensive hacking tools. The lesson to be learnt from this Pahalgam attack and Operation Sindoor is post-April 2025. Over a million “attempted cyber intrusions” by Pakistan or its allies have been detected in India. However, of those attacks, only a few were successful, according to an independent investigation. Later, it came to light that several popular claims, such as attacks on the power grid and banks, were proven to be incorrect (Deccan Herald, 2025; CloudSEK, 2025). The real lesson in this is not the number

of attacks that succeeded. It's all about information control. The rumours, like those in India, propagated quicker than the truth, and Pakistan was no different in this regard.

Summary of Main Vulnerabilities

- Weak coordination among government departments responsible for cyber security.
- Slow and incomplete application of the National Cyber Security Policy 2021.
- Underdeveloped digital systems combined with a high rate of malware exposure.
- Continued dependence on foreign technology, with limited local research and development.
- Ongoing, active cyber threats connected to the rivalry with India.
- Pakistan's own offensive cyber groups are themselves at risk of being hacked.

Lessons from the Russia-Ukraine Conflict Applicable to Pakistan

The lesson learnt from the Russian-Ukrainian conflicts can not be translated to the case of Pakistan since the two countries have different political, military, technological, and geopolitical environments. Ukraine has been engaged in a conventional conflict with Russia on a massive scale and has gained significant technical and intelligence support from Western governments, technology providers, and others. However, the region in which Pakistan is operating is quite different, especially owing to its special security concerns with India and the critical role of digital technologies in the country. However, the Russia – Ukraine affair has had several useful lessons for the national cyber security preparedness efforts and the formulation of a more adequate Cyber deterrence strategy for Pakistan.

Preparation is more useful than sudden reaction

An important lesson to come from Ukraine is that cyber defence is not something that should be built in the wake of a significant cyber incident. Several years of experience with experience in Russian cyber and information operations contributed to Ukraine's robustness in coping with the Russia-Ukraine war. Based on Russia's actions in Crimea and the start of the conflict in eastern Ukraine in 2014, Ukraine has had about eight years to learn the ropes from the old Soviets, says Chatham House. In this time, Ukrainian institutions had the opportunity to become more aware of the risks of cyber/information operations and become more capable of countering them (Giles, 2023). This lesson is very suitable for Pakistan. Cyber security is not just a “reactive” approach to security, and isn't just a tool that needs to be called into action during a serious cyberattack. On the contrary, Pakistan should continue efforts in vulnerability identification, network monitoring, technical skill development, drills and simulations in security, and learning from past incidents. Pakistan's National Cyber Security Policy 2021 already presents the policy framework of a coordinated national approach to cybersecurity, which also includes the establishment of institutional arrangements to deal with cyber threats (MoITT, 2021).

The Ukrainian experience also proves that preparation isn't just about acquiring cutting-edge technological equipment. It must be regularly assessed for threats, requires sharing of information, trained staff, resourcing on how to respond to an event, and a way of working between government departments and industry. One of the findings from Microsoft's evaluation of the Ukraine situation is that the improvement in cyber-threat intelligence and endpoint security prevented Ukrainian organizations from being overrun by a number of devastating cyberattacks.

The development of "the state of cooperation between the state, technology companies and other stakeholders for the strengthening of cyber defence of Ukraine" was also noted as a priority by Microsoft (2022). It is imperative that, for Pakistan, each cyber incident is perceived as a learning opportunity for the institutions. Failure of intrusion, attempted intrusion, malware infection, data

breach, or disruption should not be just a one-time occurrence closed simply after the immediate issue has been addressed. Rather, it is crucial to document and investigate the incident to establish how the incident occurred, what vulnerabilities were successfully exploited, how fast the incident was detected, and whether the response mechanism was effective. This exercise can help Pakistan to gradually enhance its skills in identification and prevention of future attacks. Such an attitude is more relevant, especially during situations of increasing regional tension. Amidst the general crisis, digital systems reportedly also faced attempts at cyberattacks during Pakistan-India relations in May 2025, with further cyber-related activity and information operations noted throughout the overall crisis. In fact, attributing any individual cyber incident can be tricky; therefore, caution should be taken when attributing incidents to a specific state. However, the time of high anxiety dispels the notion that Pakistan must invest in its defenses as the crisis unfolds, a point that would highlight the need for increased Pakistani preparedness even before the crisis.

The case of Ukraine also shows that preparation should not stop with military and governmental institutions. Microsoft found that a comprehensive technology approach to distributing digital infrastructure, leveraging cloud-based services, enhancing threat intelligence, and collaborating with technology providers boosted Ukraine's ability to remain operational during the crisis. These helped to minimize reliance on vulnerable physical infrastructure and positively helped to sustain Government operations during attacks (Microsoft, 2022). Proactive measures are also important, including proactive threat detection, vulnerability management, regular software updating, data protection, threat intelligence, and testing defensive systems, says Chatham House (Giles, 2023). The measures point to the fact that it is not enough to rely on one policy or one institution to develop cyber resilience; continuous preparation and institutional learning are required. The lesson that needs to be learnt by the state of Pakistan, accordingly, is not that it should follow the cyber strategy adopted by Ukraine, since Pakistan's strategic environment and institutional capacities are different. Instead, what Pakistan needs is to develop a permanent culture of cyber preparedness like what Ukraine did, instead of the normal Emergency Response & Disaster Management mechanisms. All cyber incidents can be entered into a greater national database of threats, vulnerabilities, reaction times, and lessons learned. This experience over time could enhance the capacity of the Pakistani State to prevent, withstand, recover from, and respond to cyberattacks. Thus, continuous preparedness can serve as one of the key elements of Pakistan's future envisioned national cyber-deterrence strategy.

Cyber Strategy as Part of National Strategy

The cyber strategy should be part of a national security strategy and not a technical one. But CSIS (2026) believes part of the reason the Russian cyber operations were ineffective in achieving strategic impacts was due to their lack of linkage to its military goals. In Pakistan, cyber security issues are not closely connected to any policy authority, as there is a lack of institutional linkages such that cyber security is largely perceived as a matter of the IT Ministry (Eurasia Review, 2022). Therefore, shoring up cybersecurity must be planned into the defence and foreign policy menus and coordinated across relevant government agencies.

Strengthening Backup and Resilient Systems

Another example of the need for alternative systems is the Russia–Ukraine conflict. The conflict between Russia and Ukraine further demonstrates that there is a need for alternative systems in the event of a critical infrastructure attack. While damaged parts of conventional internet infrastructure made communication impossible for Ukraine, they were able to do so through satellite internet (ScienceDirect, 2023). Pakistan may give the same treatment to other vital industries like

the Electricity, Banking and Telecommunications industries. Some measure of reliability with the backup systems would help guarantee that if and when one network was successfully attacked, the resulting disruption would not impact the nation at large.

Turning Partnerships into Practical Cooperation

In Ukraine, the defence against cyber-attacks has been greatly assisted by the international and private sector partnerships. Throughout the conflict, companies including Microsoft raised awareness, dealt with vulnerabilities, and disseminated information about threats (Microsoft, 2022). Furthermore, there is a need for interaction and coordination between various organizations in the public sector and the private sector, and one of the key areas in Pakistan's cyber policy is management for this purpose (Digital Watch Observatory, 2024). However, this goal ought to go beyond the area of statements of policy. With enhanced partnership on the practical side with telecom operators, banks, technology firms, and trusted international partners, Pakistan's capacity to identify and deal with cyber threats could be further bolstered.

Addressing Disinformation and False Cyber Claims

Information is handled in part during a crisis, and that is a component of cybersecurity. The availability of timely information has been a major countermeasure to Russian disinformation, CSIS (2026) mentions. In 2025, Pakistan faced a unique information challenge with exaggerated hacktivist claims being spread in a vacuum with reliable information not available (CloudSEK, 2025). A credible and timely public communication channel could thus be useful in establishing or negating any allegations of a cyber attack and thus minimize the potential diplomatic/political impact of misinformation.

Developing Reliable Attribution

Cyber deterrence is so dependent on source attribution that it is easy to conclude that without it there would be no such thing as cyber deterrence. The importance of attribution for credible deterrence has been pointed out by Burton 2018 and the Georgetown Journal of International Affairs 2024. This necessitates the improvement of proven independent skills in investigating and attributing cyber incidents in Pakistan. An effective evidence-based deterrence policy would require the threats or responses to be based upon reliable attribution; without mitigation, this is impossible.

Developing an Effective National Cyber Deterrence Strategy

First, Pakistan is required to increase defence related deterrability; an attack would not be easy to mount, and even if it successfully overcomes the defence line, the attack would come at an expensive price (Georgetown Journal of International Affairs, 2024). It is recommended that the objectives of the National Cyber Security Policy 2021 are realized through adopting suitable security standards, frequent audits and evaluations, and an effective emergency response plan and procedures (Ministry of IT and Telecommunication, 2021; ISACA, 2021).

Second, Pakistan needs to build up the capability of attributing misinformation and disinformation. The difficulty in deterrence arises when it's not clear who the attacker is when it's necessary (Burton, 2018). A nationwide cyber threat analysis capability would be able to study cyber incidents on its own and independently verify that an incident had been attributed to them. It would also significantly alleviate issues of credibility arising from unverifiable claims of cyber attacks, including the India–Pakistan cyber-conflict of 2025, brought about by CloudSEK.

Thirdly, Pakistan should delineate and follow a step-by-step response matrix that includes diplomatic and legal measures, sanctions, defensive measures, and escalating the response only when and if required, instead of relying mostly on offensive cyber operations and/or “hack-back” activities. Specifically, the proposed approach of Aslakson and Kempista (2016) meshes well with

the concept of a graduated approach, as offensive cyber operations can have large implications and side effects.

Eurasia Review (2022) and International Bar Association (2023) to speak for the state notice that, in Pakistan, institutional fragmentation is ranked as a significant issue. Pakistan's coordination process might, therefore, be enhanced by a well-established national cyber authority, having the requisite level of resources and decision-making authority. This would be complemented by new laws concerning data protection, digital rights, etc. This should be backed up with new laws affecting data protection and digital rights, etc. Pakistan should build up resilience by leveraging partnerships and effective public communication techniques – as is evident in Ukraine's case in sophisticated and synchronized cooperation between government and technology companies in sharing threat information and responding to cyber incidents (Microsoft, 2022). The Pakistani side can develop more of such collaboration with local tech companies and a select few international partners. In parallel, a quick and reliable public communication system can be effective in checking claims of cyberattacks and minimise the impact of misinformation (Deccan Herald, 2025; CloudSEK, 2025).

Strategy Pillar	**Main Action**	**Supporting Evidence**
Defence	Protect critical infrastructure; enforce existing NCSP 2021 standards	Ministry of IT and Telecommunication, 2021; ISACA, 2021
Attribution	Build an independent national threat-analysis team	Burton, 2018; CloudSEK, 2025
Response	Use a step-by-step response system instead of an attack-first approach	Aslakson & Kempista, 2016
Governance	Create one powerful national cyber authority with legal backing	Eurasia Review, 2022; IBA, 2023
Resilience	Expand government-private and international partnerships; fast public communication	Microsoft, 2022; Deccan Herald, 2025

Discussion: Direct Answers to the Research Questions

Bringing all the findings together, here are the direct answers to the four research questions:

- **RQ1 - Capabilities and strategies used by Russia and Ukraine**

In the war, Russia deployed a variety of tools including destructive malware, data-wiping malware, DDoS attacks, mobile electronic-warfare systems like Leer-3, and leak-and-spread information campaigns that undermine trust in official processes operating in Ukraine (CSIS, 2026; ScienceDirect, 2023). The primary reason for the relatively limited damage that these tools inflicted on the war, however, was their inadequate linkage to Russia's overall military plan in the early war years (CSIS, 2026; Chatham House, 2023). Toward the end of the war, Russia took a more refined stance, with a greater emphasis on spy activities and repeated attacks on Ukraine's energy infrastructure, sometimes launched alongside missile strikes (Lieber Institute, 2024).

In contrast, Ukraine was more dependent on defense and backup, and on having strong support from Western partners when it came to offensive weapons. It was announced that its national plan for cybersecurity had been in place since before the invasion, and it helped moderate damage wrought by Russian attacks (ScienceDirect, 2023), as companies like Microsoft continued to provide Ukraine with early detection and repair of threats (Microsoft, 2022). Regular communication systems were damaged in Ukraine, and satellite internet enabled them to keep

working (ScienceDirect, 2023). Good planning, preparation, and outside cooperation were more significant than the strength and power of the tools, as indicated in Table 2, and also observed by the Center for Naval Analyses (2023) and the Atlantic Council (2025) in analyses of the conflict.

RQ2 - Cyber security vulnerabilities in Pakistan

The biggest challenge that Pakistan faces is not only about the technical stuff but also structural. The implementation of the National Cyber Security Policy 2021 is not vigorous, largely due to the lack of cooperation between the Ministry of information and Communication Technology and other ministries, like defence, finance and foreign affairs (Eurasia Review, 2022; International Bar Association 2023). Coordination of government departments is often cited as the largest challenge in achieving progress (Khan et al., 2022). On the other hand, Pakistan's increasing reliance on digital banking, telecommunication, and e-government services has increased its vulnerability as evident in its low score on global innovation indicators and the comparatively high Malware Encounter Rate category on a monthly basis (Khan et al., 2022).

Pakistan's active cyber war against India is an additional risk. The ongoing conflict between APT and Pakistan-linked groups demonstrates weaknesses in Pakistan's capabilities (Socradar, 2025; Cyfirma, 2025; ORF, 2025) but offers clear takeaways for Pakistan on how to operate on foreign soil. A CSIS (2025) report describing Russian hackers breaching a Pakistani hacking group's own infrastructure shows that even Pakistan's offensive cyber groups are not immune to compromise. In parallel, it is widely perceived that the information infrastructure of a closed society is just as vulnerable as the communication technology infrastructure, as evidenced by the numbers of exaggerated or dubious statements documented all around the 2025 Pahalgam attack (Deccan Herald, 2025).

RQ3 - Lessons that apply to Pakistan

There are five lessons to be learned from the Russia-Ukraine war that are relevant to Pakistan. First, it's worth noting that the ability to respond after an attack is not nearly as important as sustained long-term learning; eight years of preparation has given Ukraine the resilience it has today and not just a good response at the end of an attack (Chatham House, 2023). Second, cyber strategy must not reside within a single ministry, but be included in the national strategy, a principle that has been applied in the Russian Federation, considering its own coordination flaws (CSIS 2006; Eurasia Review 2022). Third, when there is redundancy in critical infrastructure, for example in Ukraine, reliance on satellite internet results in only partial damage if an attack is successful (ScienceDirect, 2023).

Fourth, government support for private ICT companies as partners is essential, not a mere promise, to be realised as it happened for Ukraine's cyber defence (Microsoft, 2022; Digital Watch Observatory, 2024). Then, there is a need for a prompt, credible public communication system to counter false claims as disinformation spreads among Russians at an unprecedented speed, and hacktivists who are in league with Pakistan also spread exaggerations at the same pace (CSIS, 2026) (CloudSEK, 2025) as and when it is published.

RQ4 - Building an effective national deterrence strategy

Any successful strategy would be a package of goals that have to be used jointly – not individually. Deterrence is rooted in the first element, strong defence; raising the cost of an attack is the building block of deterrence (Georgetown Journal of International Affairs, 2024; Ministry of IT and Telecommunication, 2021). The latter, however, is a real attribution power, as without the capacity to distinguish an attacker, deterrence is not believable (Burton, 2018). The third is a gradual response build-up mechanism from diplomatic and legal measures to sanctions and denial measures

as opposed to an 'attack first' stance, which is more costly and difficult to manage (Asakson & Kempista, 2016).

The fourth is stronger institutional coordination, with a single national cyber authority, as is currently the situation in most countries instead of fragmentation like in Pakistan (Eurasia Review, 2022; International Bar Association, 2023; Senol, 2020). The fifth is resilience that is created through a partnership approach-with local technology companies and selected international partners-and with rapid, public communication to avoid having false claims fuelled by the crisis. (Microsoft, 2022; Stimson Center, 2025). These five parts are directly tied to the evidence adduced throughout this paper, as listed in Table 3.

Conclusion

The warfare between Russia and Ukraine is an example of today's warfare being increasingly dominated by cyber warfare. The war and conflict further confirm that the capabilities of a cyber operation are not only bound by the sophistication of the technology but also by preparation, planning, resilience, and institutional coordination. Despite some strategic gains, Russia's cyber operations failed in a few aspects due to Ukraine investing in the field, establishing connections with Western tech firms, and bolstering infrastructure that could operate if attacked (Chatham House, 2023; Microsoft, 2022; ScienceDirect, 2023). Cyber policy-implementation gap, digital institutional coordination, digital vulnerabilities, and cyber competition in the region are some of the challenges that are relevant in Pakistan's cyber security environment. In the case of Pakistan, the key takeaway from the Russia–Ukraine experience is that there is a need for comprehensive cyber deterrence, which should be achieved through a mix of weapons of defence, efficient identification of threats, response mechanisms, institutional cooperation, and other international partnerships. Achieving cyber resilience does not happen with one-time activities, but it involves ongoing planning, investment, and capacity building. Future studies including in-depth interviews with policy makers, cybersecurity experts and security experts in Pakistan could be conducted to further explore these issues and make further improvement in the proposed recommendations.

References

Aslakson, E. E., & Kempista, L. W. (2016). Developing a conceptual framework for national cyber deterrence and response. Naval Postgraduate School. https://apps.dtic.mil/sti/html/tr/AD1058293/index.html

Atlantic Council. (2025). Learning the lessons from Ukraine's fight against Russian cyber warfare. https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/

Brandefense. (2025). Operation C-Major (APT36): A persistent Pakistan-linked cyber espionage threat. https://brandefense.io/blog/apt36-2025/

Burton, J. (2018). Cyber deterrence: A comprehensive approach? NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf

Center for Naval Analyses. (2023). Assessing Russian cyber and information warfare in Ukraine: Expectations, realities, and lessons. https://www.cna.org/analyses/2023/11/assessing-russian-cyber-and-information-warfare-in-ukraine

Center for Strategic and International Studies. (2025-26). Significant cyber incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chatham House. (2023). Russian cyber and information warfare in practice: Lessons observed.

https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/05-lessons-observed

CloudSEK. (2025). Brief disruptions, bold claims: The tactical reality behind the India-Pakistan hacktivist surge. https://www.cloudsek.com/blog/brief-disruptions-bold-claims-the-tactical-reality-behind-the-india-pakistan-hacktivist-surge

Cybersecurity Intelligence. (2025). Pakistan's cyber offensive: APT36 targets Indian defence. https://www.cybersecurityintelligence.com/blog/pakistans-cyber-offensive-apt36-targets-indian-defence-8491.html

Cyfirma. (2025). Firewalls and frontlines: The India-Pakistan cyber battlefield crisis. https://www.cyfirma.com/research/firewalls-and-frontlines-the-india-pakistan-cyber-battlefield-crisis/

Deccan Herald. (2025, May 12). Pakistan-linked hackers launch 1.5 million cyber attacks on Indian websites, only 150 successful. https://www.deccanherald.com/india/maharashtra/pakistan-allied-hackers-launched-15-lakh-cyber-attacks-on-indian-websites-only-150-successful-3537123

Digital Watch Observatory. (2024). The National Cyber Security Policy 2021 of Pakistan. https://dig.watch/resource/the-national-cyber-security-policy-2021-of-pakistan

ETV Bharat. (2025, May 14). Pakistani hackers launched 15 lakh cyberattacks on Indian websites, but only a few broke through. https://www.etvbharat.com/en/!technology/pakistani-hackers-launched-15-lakh-cyberattacks-on-indian-websites-following-pahalgam-attack-enn25051404842

Eurasia Review. (2022). Pakistan's National Cyber Security Policy 2021: What is achieved and what is yet to be achieved. https://www.eurasiareview.com/17082021-pakistans-national-cyber-security-policy-2021-what-is-achieved-and-what-is-yet-to-achieved-oped/

Eurasia Review. (2025). Digital war: Pakistan's cyber activity against India - Analysis. https://www.eurasiareview.com/18052025-digital-war-pakistans-cyber-activity-against-india-analysis/

Georgetown Journal of International Affairs. (2024). A theory of cyber deterrence. https://gjia.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence/

Giles, K. (2023). *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine.* Chatham House, Royal Institute of International Affairs. Chatham House – Russian cyber and information warfare in practice

Global Cyber Alliance. (2025). AIDE data on APT36: Regional infrastructure risks and security gaps. https://globalcyberalliance.org/aide-data-apt36/

International Bar Association. (2023). The developing cybersecurity framework in Pakistan. https://www.ibanet.org/Developing-cybersecurity-framework-in-Pakistan

ISACA. (2021). Pakistan's cybersecurity policy in 2021: A review. https://www.isaca.org/resources/news-and-trends/industry-news/2021/pakistans-cybersecurity-policy-in-2021-a-review

Khan et al. (2022). Cyber security threat and Pakistan's preparedness: An analysis of National Cyber Security Policy 2021. ResearchGate. https://www.researchgate.net/publication/363168949_cyber_security_threat_and_pakistan's_preparedness_an_analysis_of_national_cyber_security_policy_2021

Lieber Institute, West Point. (2024). Recapping "Cyber in war: Lessons from the Russia-Ukraine conflict." https://lieber.westpoint.edu/recapping-cyber-war-lessons-russia-ukraine-conflict/

Microsoft. (2022). Defending Ukraine: Early lessons from the cyber war. https://blogs.microsoft.com/on-the-

issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Ministry of Information Technology and Telecommunication, Government of Pakistan. (2021). National Cyber Security Policy 2021. https://propakistani.pk/2021/01/28/it-ministry-issues-draft-of-national-cyber-security-policy-2021/

Royal United Services Institute. (2025). Operation Sindoor and India-Pakistan's escalated rivalry in cyberspace. https://www.rusi.org/explore-our-research/publications/commentary/operation-sindoor-and-india-pakistans-escalated-rivalry-cyberspace

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. The Tallinn Manual is an expert analysis of how existing international law applies to cyber operations. https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf

ScienceDirect. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. Technology in Society. https://www.sciencedirect.com/science/article/abs/pii/S1874548223000501

Senol, M. (2020). Creating and implementing an effective and deterrent national cyber security strategy. Journal of Engineering, 2020, Article 5267564. https://onlinelibrary.wiley.com/doi/10.1155/2020/5267564

Socradar. (2025). Dark web profile: APT36. https://socradar.io/blog/dark-web-profile-apt36/

Stimson Center. (2025). Beyond denial: Toward a credible cyber deterrence strategy. https://www.stimson.org/2025/beyond-denial-toward-a-credible-cyber-deterrence-strategy/

The Geostrata. (2026). A hostile grid and undefended borders: Impact of Pakistan's state-sponsored cyber campaign on India's sovereignty and its implications on international legal frameworks. https://www.thegeostrata.com/post/a-hostile-grid-and-undefended-borders-impact-of-pakistan-s-state-sponsored-cyber-campaign-on-india

Trade.gov. (2024). Pakistan - Cybersecurity. U.S. International Trade Administration. https://www.trade.gov/country-commercial-guides/pakistan-cybersecurity