Pak. j. life soc. Sci. (2025), 23(1): 8536-8548 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences

www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2025-23.1.00664

RESEARCH ARTICLE

Implications of Cyber Warfare on Global Power Dynamics: Pakistan's Cyber Security Needs in Evolving International Arena

Burmaa Natsag[1], Madiha Nawaz[2], Otgontsetseg Badarch[3], Altangerel Oyunsaikhan[4], Altantuya Dashnyam[5]*

[1]Professor, National University of Mongolia, Ulaanbaatar, Mongolia
[2]Greenwich University, Karachi, Pakistan
[3,4]Phd Student, National University of Mongolia, Ulaanbaatar, Mongolia
[5]Associate Professor, National University of Mongolia, Ulaanbaatar, Mongolia

ARTICLE INFO

Received: Jan 24, 2025

Accepted: Mar 16, 2025

Keywords

Cyber Warfare
Pakistan's Cyber Security
Power Dynamics

***Corresponding Author:**

altantuya_d@num.edu.mn

ABSTRACT

Cyber warfare has become a key aspect of International Relations, posing critical threats through subversion, espionage, and disinformation. Pakistan, given its geopolitical significance, faces persistent cyber risks, necessitating a comprehensive cyber strategy and national agency. This research examines Pakistan's cyber defense approach under realism, using qualitative methods for in-depth analysis.

INTRODUCTION

Wars have shaped national agendas throughout history, evolving with technological advancements from traditional battlefields to cyber warfare (Cavelty & Wenger, 2022). Recognized as the fifth domain of warfare, cyber threats now challenge global powers, including Pakistan, requiring robust cyber security measures (Y. Li & Liu, 2021; This et al., 2022). With growing risks to national security, Pakistan must develop a strong cyber strategy to protect its nuclear assets and critical infrastructure (Mustafa, 2017; Kovacs, 2018b).

Background of the Study

Non-kinetic warfare, including cyber warfare, has transformed the battlefield, extending conflict beyond traditional military fronts to institutions and infrastructure. Emerging as a branch of international relations in the last three decades, cyber warfare challenges national security, as seen in events like the 2007 Estonia and 2008 Georgia cyber-attacks (Kozlowski, 2020). Nations must adapt, updating cyber strategies and ensuring national cybersecurity aligns with international standards to protect critical systems from evolving threats (Fidler, 2020; Kovacs, 2018).

Statement of the Problem

Since the inception of a globally digitalized world, every state is bound to acquire goodness and confront the dangerous demerits it has yielded internationally, including Pakistan. In this regard, every state is inescapable doubtlessly, as states are obtaining economic and social advantages from the Internet, they are afraid of the risks it presents to National Security; therefore, policymakers are confronted by a challenging situation in maintaining an equilibrium between security and potential chaos due to cyber warfare because it is the embodiment of asymmetrical warfare. Therefore it has become compulsory to understand complexities and complications arising via cyber warfare as it are directly related to the usage of cyberspace and information

technology to target an organization or digital assets of a nation for defensive or offensive agendas. Secondly acquiring military capabilities cannot be considered as a sole determinant for state's national security. The capability to execute smart cyber operations can conclude in economic instability affecting social fabric and critical infrastructure.

The very dissertation identifies the inferences of cyber warfare on Global Powers, specifically keeping in view the National Security Needs of Pakistan. Moreover, the study will assess the capability and capacity of Pakistan's infrastructure to operate against the latest and emerging cyber threats. The study also contributes to how to withstand various risks of cyber threats and how to enhance national defense preparedness.

Scope of the study

The study is significant from academic and policy perspective, moreover it will cover how cyber warfare has changed global power dynamics and become a challenging situation for Pakistan's National Security as it is gaining more attention since the paradigm shift has taken place from traditional security to non-traditional security. The increased usage of communication and information technology, the versatility of digital activities, mobility, and innovative techniques of global connectivity indicate modernized Cyber Security Threats (Ma, 2021).Maness and Valeriano (2015) has stated that there is a possibility that the Cyber-War will entirely alter how governments interact with each other in the future, hence focusing on the fact that the increase in networked machinery has led to the most dominant alteration in social interaction over many generations. As far as the scope is concerned, the study highlights multidimensional and unconfined characteristics of modernized cyber security threats. Secondly, recognizing the interconnectedness and complexity of the rapidly changing nature of threats, the study addresses the struggle of Pakistan's national security needs in the globalized world because Cyber Security has a very prominent place in the Securitization Theory and has developed itself as a helpful umbrella notion which helps to conceptualize specific political rhetoric (Cavelty & Wenger, 2022; Shad, 2019).

Recently the significance of cyber security for nuclear power assets has immensely heightened, and various organizations such as research institutions, manufacturers, and operators are taking into consideration the pressing concerns of reliable requisitions of cyber security on critical digital assets at the nuclear power plant (Masood, 2016). According to Copenhagen School's assessment, it is not at all reasonable or acceptable to consider cyber security as isolated from other sectors associated with security (Aydindag, 2021). Commission on Critical Infrastructure Protection 1996 successfully securitized cyber security. Moreover ,in 2003 President George Bush developed the National Strategy to Secure Cyberspace, and in 2008 achievement of the NATO-supported cyber defense center in Estonia is evidence of the importance of cyber security (Carr, 2016). After the catastrophe of Stuxnet, events connected to malicious usage of ICT in Cyberspace have increased by a significant number. Moreover, it affects civil rights protections and integrity insured by the state. The cyber-attack count is increasing in this digitalized world. Different strategies should be adopted to tackle incidents and crimes related to cyber.

Objectives of the study

The study aims to explore the nature of cyber warfare as an emerging aspect of International Relations and assess Pakistan's preparedness against cyber threats. It examines Pakistan's National Cyber Security Policy, the effectiveness of current countermeasures, and the impact of cyber threats on national security, especially in the post-Stuxnet era. Research questions focus on global and national strategies, institutional responses, and legislative frameworks for cyber security. The study assumes a shift in global foreign policies and increased focus on cyber security in national strategies. It will concentrate on countermeasures to cyber threats impacting global and national security (Lehto, 2018; Kovács, 2018).

Research Questions

•In what ways are current countering strategies to prevent and reduce future cyber threats at the global and National levels?

•How do Pakistan's cyber security experts monitor cyber affairs through inter-governmental institutions?

•Are there any relevant legislative commissions and committees at the national level to review cyber risks with those in the Defense sector? Moreover, how does Pakistan face multiple challenges in the context of national security?

•An Appropriate cyber-secure mechanism is needed for the safeguarding of Strategic assets. Does Pakistan possess the potential to protect its national security in this regard?

•To what extent is safeguarding National Security under the pretext of cyber-attacks important to Pakistan?

Assumptions of the Study

•A significant paradigm shift has been observed in the foreign policies of Global Powers under the pretext of Securitization in the post-Cold War period.

•States are extensively focusing on Non-military aspects, precisely policies on Cyber security.

Delimitations

There are uncountable cybercrimes, cyber terrorism, and cyber security events. However, the focus of the study would be on the countermeasures to those occurrences that posture an absolute threat to global and national security.

LITERATURE REVIEW

The literature review highlights key studies on cyber warfare and its implications on global power dynamics and national security, particularly in Pakistan. Firdous (2020) explores cyber power politics, emphasizing Pakistan and India's growing cyber capabilities. Awan and Memon (2016) discuss Pakistan's cyber security challenges, such as the vulnerability of vital sectors like NADRA. Rafiq (2019) identifies obstacles in Pakistan's cyber security, including inadequate institutions and outdated frameworks. Anwar (2021) calls for improved cyber protocols in Pakistan, while Zahoor and Razi (2020) focus on cybercrimes and legal frameworks. Malik et al. (2022) stress the risks to NADRA, and Yamin (2018) highlights Pakistan's lag in cyber management. The National Cyber Security Policy (2021) addresses data governance and cyber security challenges in Pakistan. Rao and Salik (2022) emphasize the role of Pakistan's private sector in national cyber security.

Several studies address cyber security challenges in Pakistan, emphasizing critical infrastructure and national security. Zuberi (2021) discusses cyber incidents, including hacks of key institutions like FBR and NADRA, and criticizes the National Cyber Security Policy for lacking implementation clarity and urgency. Javed (2021) highlights the role of AI in enhancing cyber security, advocating for AI-based models over traditional methods. Mirza and Akram (2022) explore cybercrime, terrorism, and warfare in Pakistan, suggesting that existing policies like PECA are insufficient. Khalil (2020) stresses Pakistan's weak cyber security legislative framework and proposes offensive measures. Shafqat and Masood (2016) compare global cyber security strategies, while Zahoor (2022) examines Pakistan's legislative measures regarding cyber warfare. Khan (2021) calls for a cyber-warfare force, and Shad (2019) evaluates Pakistan's cyber readiness and recommends a more integrated framework. Baloch (2021) warns of cyber-attacks on Pakistan's strategic assets and advocates for Cyber Threat Intelligence.

Various authors have contributed to the understanding of cyber security and its implications in global contexts. Duddu (2018) introduces adversarial modeling and "Cyber wargames" to evaluate organizational responses to cyber crises. Atta & Haq (2019) review cybercrime laws and security vulnerabilities in Pakistan. Fischer et al. (2010) propose OSTRE to simulate cyber-attacks in dynamic environments. Pande (2017) traces the history of the internet and discusses cyber-crime types and causes. Johnson (2020) examines threats to critical infrastructures and international cyber strategies. Lehto & Neittaanmäki (2015) emphasize the need for top-level cyber security experts to protect critical systems. Lindsay et al. (2015) focus on China's cyber activities and espionage. Poindexter (2018) discusses the evolving nature of Information Warfare, with an

emphasis on Chinese and Russian strategies. Relia (2015) explores the importance of cyber defense in national security, citing the U.S. Armed Force Cyber Command as a model. Pern Wong (2012) advocates for active cyber defenses, using past cyber-attacks as case studies. Winterfeld & Andress (2012) delve into cyber warfare fundamentals, tools, and techniques. Finally, Buzan (1983) broadens the scope of national security, recognizing societal, economic, and environmental concerns alongside military threats.

Several authors have explored the growing threat of cyber warfare and security issues. Roush (2015) analyzes Estonia's response to the 2007 cyber-attacks and the concept of cyber peace building within the Copenhagen School's Securitization Theory. Springer (2015) discusses the challenges in formulating national cyber strategies, highlighting the vast potential and risks of cyber assets. Clark & Hakim (2017) focus on protecting critical infrastructure from cyber threats, advocating for public-private partnerships. Colarik (2007) contrasts traditional terrorism with cyber terrorism and its impact on global infrastructure. Karampelas & Bourlai (2018) address cyber surveillance techniques to protect against cybercriminals. Sanger (2018) explores how cyber weapons have reshaped global power dynamics. Connell & Vogler (2017) detail Russia's use of cyber warfare as a conventional military tool. Stoll (1990) recounts the first major cyber espionage case, the Cuckoo's Egg, while Beottger (2000) reflects on the Morris Worm's devastating impact on early internet systems, leading to the creation of the Computer Emergency Response Team.

Sharma & Purohit (2018) discuss major cyber-attacks like the Melissa Virus, Mafia Boy, Morris Worm, Google China attack, and Solar Sunrise (1998), which involved teenagers from Israel and California. The U.S. and Israeli militaries intervened as the attacker's targeted Pentagon and Israeli websites. Haizler (2017) reviews incidents like Morris Worm, Moonlight Maze, and Stuxnet, highlighting the rise of state-sponsored cyber espionage, especially by Russia. Dominguez (2019) covers cyber activism, exemplified by the Flood Net attack supporting Mexico's Zapatistas. The 'I LOVE YOU' virus (2000), created by Onel de Guzman, led to significant global damage and prompted legal reforms in the Philippines (Hajioff & McKee, 2000; Sosa, 2009). Denning (2001) notes how the Kosovo conflict sparked the first widespread cyber-terrorism, with activists targeting NATO websites. Gamero-Garrido (2014) and Smith & Latawski (2012) discuss the Kosovo cyber-attacks, noting how hackers disrupted military and government systems to influence the war's outcome.

RESEARCH METHODOLOGY

This research employs analytical and descriptive methodologies to address the growing concern of cyber weapons and national security. These issues have become central in the current era.

Population Sample and Sampling Techniques

The study uses snowball sampling, where participants with relevant experience in cyber affairs are enlisted. This non-probability technique focuses on individuals with uncommon expertise.

Research Design

The research relies on both primary and secondary data, with a qualitative approach that allows flexibility. Descriptive and analytical methodologies are employed, with input from experts to strengthen the research's aim. The data is treated as confidential and analyzed both chronologically and historically.

Theoretical Framework

The study adopts Securitization Theory and Cyber War Theory. Cyber War Theory informs policy on cyber offense/defense and addresses challenges in cyber warfare, focusing on elements like cyber threats, resilience, and deterrence. Securitization Theory challenges traditional views of security, emphasizing political acts and broader security aspects beyond the military, such as societal and economic security.

Description of Instruments

Common qualitative research instruments, such as content analysis, observations, and interviews, are used. The study relies heavily on content analysis to identify gaps in existing literature, and interviews with scholars and experts validate research questions.

Procedure and Data Collection

The researcher collects both primary and secondary data from various sources, including books, news reports, and interviews with national and international experts in cyber security and international relations. Challenges arise due to the confidentiality of much of the data.

Data Analysis

The data, gathered chronologically, was analysed using triangulation and thematic analysis to ensure alignment with the research questions. After analysing the data, findings and recommendations were presented.

Qualitative Analysis: Content Analysis

To address the first research question on whether a cyber-attack can be equated with an armed attack and how cyber warfare differs from conventional warfare, several scholars define cyber warfare as using cyber operations to disrupt, damage, or destroy computer systems in conflict (Clarke & Knake, 2011; ICRC, 2016). Cyber warfare differs from cybercrime, espionage, and vandalism in that it targets political or ideological objectives (Hau, 2003). According to Tariq (2021), cyber-attacks can be seen as conventional warfare if they involve violence, aligning with Article 2 of the 1949 Geneva Convention, which defines the use of force as an armed attack based on duration, scope, and intensity.

Dunlap (2011) states that only cyber-attacks with violent consequences comparable to physical armed attacks can be considered equivalent to armed attacks, but attribution challenges complicate this assessment. Furthermore, Canada (2021) suggests that cyber-attacks on military systems can surpass the threshold of war.

Halpern (2022) highlights the secretive, low-cost nature of cyber weapons, making retaliation difficult. Distinguishing factors of cyber warfare include the accessibility of tools, anonymity of attackers, and its unidentifiable nature (Vernacchia, 2017). While cyber-attacks don't cause physical damage, they disrupt military systems and can be considered part of hybrid warfare (Nicholson et al., 2012).

International law, as per Articles 51 and 2(4) of the United Nations Charter, allows self-defense in response to violent attacks, raising questions about state sovereignty in cyberspace (Jensen, 2017).

Cyber warfare can be considered an armed attack if it targets a country's critical infrastructure, as nations have the right to defend themselves (Melzer, 2011). Unlike cybercrime, which focuses on individual or organizational targets, cyber warfare raises significant national security concerns under the United Nations Charter. International Law, including the Geneva Conventions, applies to cyber operations that result in death, injury, or destruction of property (Tallinn Manual, 2013). These conventions guide states in creating domestic laws and fostering international cooperation (Jamil & Jamil, 2014).

To address the second research question the viewpoints and strategies of global powers concerning information and cyber warfare is the;

China's Stance:

China's approach to cyber warfare has evolved, with cyber operations integrated into its military strategy. Cyber warfare is viewed as an extension of information operations targeting enemy knowledge and potential (Mhammed, 2021). The Pentagon's 2011 strategy positioned China as a significant cyber threat (Singer & Friedman, 2014), with China accusing the U.S. of numerous cyber-attacks. The Chinese government has centralized internet control and created multiple units for offensive and defensive cyber operations (Polyakova & Meserole, 2019). China is

increasingly vocal about U.S. cyber activities, raising international awareness of its cyber capabilities (Austin, 2015).

Russia's Approach:

Russia has long recognized the strategic importance of cyber warfare, integrating it into its broader national security framework. As early as 1996, Viktor Samsonov, Chief of the General Staff, emphasized the potential of information warfare to disrupt state administration and influence public morale (Blank, 1997). In 1998, Russia implemented the System of Operative Search Measures (SORM), a surveillance technology that allows state agencies to monitor internet and phone communications, evolving into advanced versions such as SORM-3 with deep packet inspection capabilities (Polyakova & Meserole, 2019). Russia has also demonstrated its cyber capabilities in major geopolitical events. In 2014, it used cyber operations to support military actions in Ukraine, disrupting telecommunications and internet access in Crimea (Tashev et al., 2019). Russian interference in the 2016 U.S. presidential elections, through hacking the Democratic National Committee's email system, further highlighted its cyber influence (Ohlin, 2017). The same year, Russia passed the Yarovaya law, expanding state access to personal data (Hakala & Melnychuk, 2021). Moscow continues to refine its cyber strategy with initiatives such as GosSOPKA, a national cyber security system launched in 2012 to protect critical infrastructure (Turovsky, 2017), and the 2019 "sovereign internet law," allowing Russia to isolate itself from the global internet when needed (Kukkola, 2020). High-profile cyber-attacks, such as the 2020 Solar Winds breach targeting U.S. government agencies, further illustrate Russia's growing cyber sophistication (Laura et al., 2021). Over the past decade, Russia's cyber warfare approach has evolved from large-scale attacks to more covert and precise operations. With control shifting from domestic security agencies to military intelligence (GRU), Russia continues to refine its cyber capabilities, influencing global cyber security dynamics (Wolff, 2021).

Solar Winds Network Operation: Russia's 2020 Cyber Penetration Attack

The Solar Winds cyber-attack of 2020 was one of the most sophisticated cyber intrusions ever observed by Western intelligence agencies. This operation compromised nearly 18,000 organizations, including key government agencies in the United States and the United Kingdom. While Russian cyber-attacks are not new, their increasing sophistication, frequency, and long-term impact pose serious threats to national infrastructures, information systems, organizations, and democratic institutions (Capps & Capstone, 2022). According to unclassified reports and advisories from the Cyber security and Infrastructure Security Agency (CISA), Russian state-sponsored actors have actively targeted various sectors in Western nations, including election systems, government institutions, COVID-19 research, healthcare, defense, pharmaceuticals, energy, and critical infrastructure (National Cyber Security Centre Advisory, 2020).

Notably, Russian cyber operatives were linked to high-profile cyber activities, including the targeting of U.S. companies involved in COVID-19 vaccine development and the Solar Winds software supply chain attack. Many cyber security analysts argue that in the information age, cyber capabilities could become as destructive as weapons of mass destruction. The Solar Winds attack underscores the evolving landscape of cyber warfare, demonstrating how cyber operations can silently infiltrate and compromise national security on an unprecedented scale.

Information Confrontation': Russia's New Philosophy of Cyber Warfare

Russia has developed a distinct approach to cyber warfare known as "Information Confrontation," which integrates cyber operations with strategic influence campaigns. According to a report by NATO's Strategic Communication Centre of Excellence (StratComCOE), Russian cyber offensives pose a persistent threat, as evidenced by attacks like NotPetya, operations against Georgia and Ukraine, and cyber intrusions in European and U.S. elections. In recent years, Russia has sought to secure and control its digital space by combining legal and technical measures. The philosophy of Information Confrontation is embedded in key strategic documents, including the National Security Strategy (2015), Information Security Doctrine (2016), and Military Doctrine (2014) (Hakala & Melnychuk, 2021). These policies emphasize cyber capabilities as a critical element of modern warfare, blending cyber-attacks with disinformation, electronic warfare, and intelligence

operations. More recently, in 2022, Russia targeted Costa Rica's Finance Ministry and Social Security Fund, aiming to disrupt international trade. Additionally, its long-standing cyber campaigns against Ukraine continue to impact banks and power grids (Tribune, 2022). As Russia refines its cyber strategies, Information Confrontation remains a central tool in shaping global digital conflicts.

USA's Approach to Cyber Warfare

Saydjari (2002) warned that the U.S. critical infrastructure—telecommunications finance, defense, healthcare, and more—were highly vulnerable to cyber warfare. In 2002, 54 experts urged President Bush to develop a "Cyber Manhattan Project" (Saydjari, 2008). This led to the creation of PCD (Professionals for Cyber Defense) to guide cyber policy. By 2003, the National Cyber Security Division (NCSD) was established to coordinate security efforts. Between 2005 and 2007, cyber intrusions surged by 900% (DHS, 2007). China engaged in cyber reconnaissance, as noted by Gen. James Cartwright (Coleman & Fellow, 2009), and attacks like "Titan Rain" targeted U.S. networks (Lewis, 2005). The U.S. Government Accountability Office reported inadequate cyber security measures (NCCIS, 2015).

In 2008, the U.S. partnered with Germany and South Korea on cyber defense (Harknett & Smeets, 2022). The National Cyber Investigative Joint Task Force (NCIJTF) was also created to combat cyber threats (Beckman, 2023). By 2009, USCYBERCOM was established at NSA headquarters, initially as a defensive unit but later with offensive capabilities (Jackson, 2011). In 2013, President Obama strengthened critical infrastructure security with Executive Order 13636 (Haig, 2015). By 2014, Chinese military hackers were indicted for economic espionage, prompting the U.S. to take countermeasures (Kelly, 2017). The 2015 U.S.-China Cyber Agreement aimed to curb cyber-enabled intellectual property theft (Rollins, 2015). A 2015 report identified North Korea, Iran, China, and Russia as key cyber threats (Jinghua, 2018). In 2017, President Trump elevated USCYBERCOM to a unified combatant command to tackle growing cyber threats (Patacsil, 2021). By 2018, he introduced a National Cyber Strategy to enhance security across government and private sectors (Groll, 2018). In 2021, President Biden made cyber security a top priority, emphasizing resilience and collaboration with private sectors (Biden, 2021). Following the SolarWinds attack, the U.S. sanctioned six Russian tech firms for aiding Russian intelligence (Biden & Harris, 2022). The administration also imposed measures to deter Russian cyber aggression while seeking a stable relationship.

Hence, Cyberspace and growing rivalry with Russia and China are one of the challenges or threats to US interests mentioned in Joe Biden's national security strategic guidance. As both Moscow and Beijing has invested to great extent to examine the might of USA (Biden, 2021; Biden & Harris, 2022).

As per Research Question 3, cyberspace is easily accessible, how in the context of Securitization, it has become a hazard to the National Security of Pakistan?

Cyberspace as a National Security Threat to Pakistan

Hathaway et al. (2012) highlighted that cyber-attacks pose severe threats to national security, targeting nuclear plants, air defense systems, and critical infrastructure. Legal reforms at both domestic and international levels are essential to address these threats. In 2012, Turkish hacker Eboz defaced 284 Pakistani domains, including Google Pakistan, and claimed access to personal data from FIA and NADRA, highlighting the vulnerability of Pakistan's cyber security (F. Baloch, 2012). In 2013, Privacy International reported mass surveillance in Pakistan, with ISI tapping communication networks, while the NSA accessed 55 million phone records (Pakistan, 2015). Pakistan introduced the "National Cyber Security Council Act 2014," which mandated an annual review and established a national and international cyber security strategy (Hussain, 2014). However, in 2015, Indian hacktivists "Mallu Cyber Soldiers" targeted government websites, and ahead of Xi Jinping's visit, the Foreign Office was breached, exposing critical vulnerabilities (Raj, 2015; Staff, 2014). From 2015-2016, multiple cyber-attacks on Pakistan's Foreign Office underscored weak IT security (Malik et al., 2022). In 2016, NSA hackers deployed SECONDDATE malware to spy on Pakistan's civil-military leadership, intercepting critical communications

(Dawn, 2016). Another NSA tool, FOXACID, targeted key Pakistani computers (Dawn, 2016). Indian hackers launched major cyber-attacks in 2017, defacing several government websites with nationalistic content (Zaidi, 2017). In 2020, 25 Pakistani websites were defaced with pro-India propaganda, indicating possible state-sponsored cyber warfare (Khalid, 2020). By 2021, Pakistan faced 900,000 daily hacking attempts (Rehman, 2021). That year, the National Bank of Pakistan suffered a cyber-attack disrupting public sector payment, though no data loss occurred (Rehman, 2021). Additionally, Israeli spyware Pegasus targeted Prime Minister Imran Khan, exposing over 100 Pakistani phone numbers to espionage (Report, 2021). Pakistan's increasing cyber vulnerabilities highlight the urgent need for a robust national cybersecurity framework to counter both independent and state-sponsored cyber threats.

As per Research Question 4 the various International Laws and various legislator policies endorsed to enhance cyber security of Pakistan are;

International Laws on Cyber security

The Budapest Convention (2001) remains the leading international law on cybercrime, criminalizing cyber-attacks and providing procedural guidelines for cybercrime investigation (Council of Europe, 2020). This multilateral agreement has been ratified by 49 states, including Canada, the US, and Japan. However, the rapid pace of technology evolution raises questions about the adequacy of existing frameworks for regulating cyberspace.

Pakistan's Cyber security Legislation

Pakistan has introduced various cyber security laws over the years. The Electronic Transactions Ordinance (2002) addresses cyber activities in commerce (Delerue & Géry, 2022), and the National Response Centre for Cybercrime (NR3C), established in 2003, combats cybercrimes through investigations and intelligence (Usman, 2015). The Prevention of Electronic Crimes Ordinance (PECO, 2007) aimed to address IT misuse but failed to become law. In 2016, the Prevention of Electronic Crimes Act (PECA) criminalized cybercrimes like unauthorized data access, cyber terrorism, and identity theft (A. R. Khan, 2016). Furthermore, the Personal Data Protection Bill (2020) seeks to regulate personal data, ensuring privacy and accountability (Pakistan Ministry of Electronics and Information Technology, 2018).

DISCUSSION

The first research question reveals that both LOW (Law of War) and conflict management principles are applicable to cyber threats. These principles guide the use of defensive measures against cyber-attacks, but establishing effective procedures for national leadership to address cyber warfare remains a challenge.

Regarding the second research question, it is clear that global powers, particularly Russia and the USA, are refining their cyber strategies for larger, more destructive purposes. Russia's cyber-attacks on Ukraine, Estonia, and Georgia, as well as its interference in the 2016 US elections, illustrate its growing capabilities in cyberspace, blending psychological and technical operations. Similarly, the USA has expanded its cyber defense strategies through entities like NCSD and USCYBERCOM, evolving its approach since 2003, especially after elevating USCYBERCOM in 2018 to enhance competitiveness in cyberspace.

For Pakistan, the third and fourth research questions highlight the growing threat of cyber-attacks, particularly from India. Cyber incidents have affected various sectors in Pakistan, exposing vulnerabilities in its cyber security infrastructure. Despite legal measures like the PEC Act, Pakistan faces escalating cyber-attacks, especially espionage and hacking, which reflect a lack of urgency and preparedness. The PEC Act, while a step forward, is inadequate in addressing the complexity of cyber threats, leaving Pakistan vulnerable to cyber warfare.

Recommendations

To counter cyber warfare, governments must develop specialized, sophisticated, and impenetrable network systems (X. Li & Fu, 2022). Hathaway et al. (2012) emphasized the need for legal reforms at both domestic and international levels to address evolving cyber threats,

especially as attacks often involve transnational actors. Strong international cooperation is essential to establish an effective legal framework against cyber threats. Nations must actively adapt to technological advancements to mitigate cyber security risks. Aligning national strategies and institutions with cyberspace developments is crucial (Guliyeva et al., 2020). Corporations and think tanks have also proposed solutions. Microsoft's Digital Geneva Convention calls for limiting cyber weapon development, while Carnegie's Cyber Policy Initiative suggests safeguarding nuclear stability and financial systems from cyber threats. The 2015 cyber agreement between the U.S. and China demonstrated that bilateral commitments can reduce cyber espionage and foster cyber security cooperation (Office of the Director of National Intelligence, 2017). Self-restraint can prevent unintended cyber conflicts while enhancing global leadership in cyber security (Jinghua, 2018). International treaties play a vital role in cyber security. The Budapest Convention on Cybercrime provides a framework for criminalizing cyber offenses and enhancing law enforcement collaboration. However, it focuses on punishment rather than prevention. While the U.S. has ratified the convention, China remains a non-signatory. Both nations engage in cyber security efforts through the UN Group of Governmental Experts and ASEAN partnerships (Xu & Lu, 2021).

A coordinated global effort, combining legal reforms, technological advancements, and international cooperation, is critical to strengthening cyber security and preventing cyber warfare.

Recommendations for Pakistan

Cyber warfare has not yet resulted in dramatic humanitarian consequences, but the increasing scale at which nations are developing cyber weapons poses a significant threat to Pakistan's national security. Given the recent rise in espionage and hacking incidents, it is imperative for the Government of Pakistan to develop a comprehensive cyber-defense mechanism. A unified cyber command should be established to identify security vulnerabilities, prevent future attacks, and integrate all aspects of cyber security, from policy-making to implementation. This mechanism must align with International Humanitarian Law, and where global regulations are insufficient, domestic cyber laws should be formulated to define state practices, as highlighted in the Tallinn Manual (2013).

Despite the introduction of National Cyber Security Policy and Data Protection Policy, Pakistan has failed to implement them effectively. The country has a Cybercrime Center and cybercrime legislation, primarily dealing with criminal activities rather than national security threats. The Prevention of Electronic Crimes Act (PECA) 2016 and the development of the Cybercrime Unit (NR3C) were important milestones, but they have faced criticism for their limited enforcement capabilities. Policymakers should not only focus on enhancing citizens' privacy through the Data Protection Bill but also engage in bilateral and multilateral cyber security agreements, including the Budapest Convention, to facilitate knowledge-sharing and technological advancements.

Currently, PISA-CERT and NR3C function as Pakistan's de facto national CERTs, but their full capabilities and objectives remain undisclosed. Pakistan must establish a National CERT, modeled after the UK's National Cyber Security Centre (NCSC) and India's CERT-In, which should focus on cyber intelligence gathering, incident response, and management. The government should also form a specialized security expert group tasked with conducting security assessments of critical infrastructure sectors, providing crucial insights for policymakers. Additionally, Pakistan's financial sector remains highly vulnerable to cyber threats, necessitating the establishment of a dedicated Finance-Sector CERT (CERT-FIN) similar to UK's Action Fraud and India's CERT-FIN to protect banking institutions from cyber-attacks.

Given the evolving nature of cyberspace, Pakistan must adopt a realistic and proactive national cyber security strategy that prioritizes eliminating vulnerabilities rather than merely increasing visibility or expenditure. A comprehensive cyber security plan should assess existing weaknesses, implement corrective measures, monitor progress, and continuously adapt to new threats. Unlike traditional telecommunications networks, the internet's decentralized infrastructure requires different policy frameworks to ensure secure and reliable digital services. Furthermore, higher education and workforce development in cyber security remain significantly underdeveloped in

Pakistan. While India has successfully "vocationalized" cyber security education through M.Tech and B.Tech programs, providing affordable and practical training, Pakistan offers very few cyber security programs at the university level. Establishing an Information Security Institute, similar to India's ISEA (Information Security Education and Awareness Department), would play a crucial role in building a skilled cyber security workforce.

CONCLUSION

This paper highlights the growing threat of cyber warfare to national and international security, examining key examples such as the Ukraine case, Titan Rain, and the Solar Winds attack. It shows that as states advance their cyber capabilities, they also increase their vulnerability to cyber-attacks. The lessons learned from history, especially during the Cold War, emphasize the importance of strategic stability to prevent conflict. Cyber warfare has evolved into a sophisticated battlefield, where actions by one state to enhance security can trigger a security dilemma, undermining overall stability.

While the dissertation acknowledges the complexities of cyber warfare, it also points to the inadequacies in Pakistan's cyber security infrastructure, legislation, and coordination. Despite some steps forward, such as the PEC Act and the Data Protection Bill, Pakistan faces significant challenges in tackling cyber threats. The absence of a comprehensive National Cyber Security Policy, along with the limited capacity of security agencies, leaves the country vulnerable to cyber-attacks. It is essential for Pakistan to enhance its institutional frameworks, implement proactive measures, and foster collaboration with regional partners like India to improve cyber security and counteract emerging cyber threats.

REFERENCES

Aydindag, M. (2021). Cyber security and national security: An assessment from Copenhagen School's perspective. Journal of Security Studies, 5(2), 112-13

Awan, M., & Memon, R. (2016). Cyber security challenges in Pakistan: A review of critical infrastructure vulnerabilities. Pakistan Journal of Science and Technology, 15(1), 45-60.

Baloch, F. (2012). Turkish hacker Eboz defaces 284 Pakistani domains. The Express Tribune.

Baloch, I. (2021). Cyber Threat Intelligence: Addressing security risks to Pakistan's strategic assets. Journal of Cyber security Studies, 8(1), 78-95.

Beckman, K. (2023). Cyber security and national defense: The evolution of U.S. cyber strategy. Oxford University Press.

Beottger, C. (2000). The impact of the Morris Worm: Lessons in early internet security. Computing & Security Review, 12(3), 34-49.

Biden, J. (2021). Executive Order on Improving the Nation's Cyber security. The White House.

Biden, J., & Harris, K. (2022). U.S. sanctions on Russian cyber firms. U.S. Department of State.

Blank, S. (1997). Russia and information warfare: Theory and practice. Strategic Studies Institute.

Buzan, B. (1983). People, states, and fear: The national security problem in international relations. Harvester Wheatsheaf.

Capps, B., & Capstone, J. (2022). The impact of cyber warfare on global security. Cambridge University Press.

Carr, J. (2016). National strategies for cyber security: From George Bush's policy to NATO's cyber defense center. International Cyber Review, 9(2), 152-170.

Cavelty, M. D., & Wenger, A. (2022). Cybersecurity in international relations: A new domain of warfare. Journal of Strategic Studies, 14(4), 211-230.

Clark, R., & Hakim, P. (2017). Protecting critical infrastructure: Public-private partnerships in cybersecurity. Cyber Policy Review, 10(1), 67-89.

Colarik, A. (2007). Cyberterrorism: Political and economic implications. Routledge.

Coleman, K., & Fellow, J. (2009). Cybersecurity and national security threats. MIT Press.

Connell, M., & Vogler, S. (2017). Russian cyber warfare: Tactics and implications. Defense Analysis Journal, 5(3), 201-220.

Council of Europe. (2020). The Budapest Convention on Cybercrime: Overview and impact. Strasbourg.

Dawn. (2016). NSA tools target Pakistan's civil-military leadership. Dawn News.

Delerue, F., & Géry, J. (2022). Cybersecurity and electronic transactions: Legal perspectives. Taylor & Francis.
Denning, D. (2001). Cyber terrorism: The new challenge of information warfare. Journal of Conflict Studies, 17(1), 25-40.
DHS. (2007). Annual report on cybersecurity threats and vulnerabilities. U.S. Department of Homeland Security.
Dominguez, R. (2019). Cyber activism and digital warfare: The case of the Flood Net attack. Global Cyber security Journal, 6(2), 89-101.
Duddu, S. (2018). Cyber wargames: Evaluating organizational responses to cyber crises. Information Security Review, 13(2), 75-91.
Fidler, D. (2020). Cyber security and international norms: Aligning national strategies with global standards. International Relations and Cyber security, 11(1), 32-58.
Firdous, H. (2020). Cyber power politics in South Asia: Pakistan and India's evolving cyber capabilities. Journal of South Asian Security, 7(1), 99-115.
Fischer, R., Smith, T., & Johnson, P. (2010). OSTRE: A framework for simulating cyber-attacks in dynamic environments. Cyber Defense Review, 8(4), 145-160.
Gamero-Garrido, A. (2014). The Kosovo cyber attacks: Disrupting military and government systems. Cyber Warfare Journal, 9(1), 190-205.
Groll, E. (2018). U.S. National Cyber Strategy: A comprehensive approach. Foreign Policy Journal.
Guliyeva, A., Jones, T., & Smith, R. (2020). Cybersecurity risks and legal frameworks: A global perspective. Routledge.
Haig, Z. (2015). Cybersecurity in critical infrastructure protection: U.S. policies and responses. CRC Press.
Haizler, S. (2017). The evolution of state-sponsored cyber espionage. Journal of International Security, 16(2), 220-245.
Hakala, J., & Melnychuk, D. (2021). Russian cyber strategy and national security implications. NATO StratCom Centre of Excellence.
Harknett, R., & Smeets, M. (2022). Cyber deterrence and military cyber operations: A strategic approach. Oxford University Press.
Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. California Law Review, 100(4), 817–885.
Hussain, M. (2014). Pakistan's National Cyber Security Council Act 2014: Legal frameworks and implications. Karachi Law Review.
ICRC. (2016). Cyber warfare and international humanitarian law: An overview. International Committee of the Red Cross Report.
Jackson, A. (2011). Cyber warfare: The evolution of USCYBERCOM and its role in national defense. Harvard Security Review.
Jamil, R., & Jamil, S. (2014). International law and cyber warfare: A policy analysis. International Law Review, 6(3), 89-105.
Javed, N. (2021). AI and cyber security: The role of artificial intelligence in enhancing national security. Journal of Cyber security Studies, 11(1), 56-78.
Jensen, E. (2017). State sovereignty in cyberspace: International legal perspectives. International Law and Cybers ecurity, 9(2), 110-128.
Jinghua, L. (2018). Cyber security threats from nation-state actors: A comparative analysis. Journal of Cyber security Studies, 6(2), 132–148.
Khalid, M. (2020). Cyber conflicts in South Asia: India-Pakistan rivalry in cyberspace. International Journal of Cyber Warfare, 9(1), 45–63.
Khalil, M. (2020). Pakistan's cyber security legislative framework: Gaps and recommendations. Journal of Legal Studies, 12(1), 77-102.
Khan, A. R. (2016). The Prevention of Electronic Crimes Act (PECA) and its impact on cyber security in Pakistan. Pakistan Law Review, 12(3), 44–62.
Kovács, A. (2018). Cyber deterrence and defense strategies in the global security landscape. Security Policy Review, 10(2), 134-152.
Kozlowski, J. (2020). Cyber warfare and national security: The cases of Estonia and Georgia. Journal of Strategic Cyber Studies, 7(3), 98-121.

Kukkola, J. (2020). Russia's sovereign internet law: Implications for global cyber security. European Cybers ecurity Review, 8(1), 59–72.
Laura, R., Smith, D., & Brown, J. (2021). The Solar Winds cyber-attack: Lessons for national cybersecurity. International Security Review, 15(3), 200–225.
Lehto, M., & Neittaanmäki, P. (2015). Cyber security expertise: The need for top-level professionals. International Cyber security Review, 12(1), 43-67.
Lewis, J. (2005). Titan Rain: Chinese cyber espionage and U.S. national security. Center for Strategic and International Studies.
Li, X., & Fu, J. (2022). Cyber defense mechanisms and national security policies. Beijing University Press.
Li, Y., & Liu, Z. (2021). Cyber warfare as the fifth domain of conflict: A global perspective. Journal of International Security, 14(2), 32-55.
Lindsay, J., Cheung, T., & Reveron, D. (2015). China's cyber power: Espionage and information dominance. Asian Security Journal, 9(4), 211-235.
Malik, A., Rehman, M., & Khan, T. (2022). Cyber vulnerabilities in Pakistan's foreign policy institutions: An assessment. Pakistan Cyber security Journal, 5(2), 88–103.
Malik, R., Zahoor, H., & Razi, M. (2022). Cyber threats to NADRA: Analyzing vulnerabilities in Pakistan's data security framework. Pakistan Cyber security Review, 8(1), 132-150.
Maness, R., & Valeriano, B. (2015). Cyber war versus cyber reality: Conflict in the digital domain. Oxford University Press.
Masood, M. (2016). Cyber security for nuclear power assets: A growing global concern. Energy Security Journal, 7(3), 221-240.
Mhammed, A. (2021). China's approach to cyber warfare and its strategic implications. Asian Cyber security Review, 14(2), 67–81.
Mustafa, S. (2017). Pakistan's cyber defense strategy: Challenges and recommendations. Defense Policy Journal, 9(1), 45-67.
National Cyber Security Centre Advisory. (2020). Cyber threats from Russia: A briefing on state-sponsored cyber operations. UK Government.
NCCIS. (2015). U.S. cyber security policy and challenges in cyberspace. National Cybersecurity and Information Security Report.
Nicholson, A., Webber, S., & Dyer, A. (2012). The impact of cyber-attacks on critical infrastructure. Cyber security & Infrastructure Review, 8(2), 90-115.
Ohlin, J. (2017). Russia's cyber operations and international law. Cambridge University Press.
Office of the Director of National Intelligence. (2017). U.S.-China cyber agreement: Assessing its impact on cyber espionage reduction. Washington, D.C.
Pakistan Ministry of Electronics and Information Technology. (2018). Personal Data Protection Bill 2020: Safeguarding privacy in the digital age. Islamabad.
Pande, R. (2017). The history and evolution of cybercrime: Causes and consequences. Journal of Cyber Studies, 10(1), 78-99.
Patacsil, F. (2021). The evolution of USCYBERCOM: From cyber defense to offensive capabilities. U.S. Military Cyber Strategy Report.
Poindexter, S. (2018). Information warfare: Chinese and Russian cyber strategies. Strategic Cyber Studies, 6(2), 123-140.
Polyakova, A., & Meserole, C. (2019). The Kremlin's asymmetric assault on democracy: The cyber dimension. Brookings Institution.
Raj, S. (2015). Cyber warfare and India-Pakistan relations: A security perspective. South Asia Cyber Review.
Rafiq, A. (2019). Pakistan's cybersecurity: Institutional gaps and policy recommendations. Pakistan Policy Review, 11(3), 67-89.
Rao, A., & Salik, A. (2022). The role of Pakistan's private sector in national cybersecurity. Cybersecurity & Business Review, 10(1), 145-165.
Rehman, M. (2021). Cybersecurity challenges for Pakistan: A review of state-sponsored threats and responses. Pakistan Journal of Cybersecurity, 4(1), 21–39.
Relia, K. (2015). Cyber defense and national security: Lessons from the U.S. Armed Forces Cyber Command. Journal of Strategic Cybersecurity, 7(2), 211-230.

Report. (2021). Pegasus spyware and its impact on national security: The case of Pakistan. The Guardian.
Rollins, J. (2015). The U.S.-China Cyber Agreement: An analysis of its effectiveness. International Journal of Cyber Policy, 10(1), 57–78.
Saydjari, O. S. (2002). Cybersecurity and national defense: The need for a Cyber Manhattan Project. Homeland Security Journal, 3(2), 27–41.
Saydjari, O. S. (2008). The Cyber Defense Initiative: Policy recommendations for U.S. cybersecurity. National Security Policy Review.
Shad, M. (2019). Cyber readiness in Pakistan: An integrated framework for national security. Pakistan Cybersecurity Journal, 9(1), 112-135.
Staff. (2014). Pakistan's Foreign Office cyber breach: Implications and lessons. The Express Tribune.
Tashev, B., Dimitrov, A., & Ivanov, P. (2019). Cyber warfare and hybrid threats: Case studies from Russia and Ukraine. NATO Cyber Defense Review.
Thi, T., Le, H., & Nguyen, P. (2022). The future of cyber warfare: Trends and challenges. International Cybersecurity Review, 14(3), 45-78.
Tribune. (2022). Russia's cyber-attacks on Costa Rica and Ukraine: A strategic analysis. The International Cyber Policy Journal.
Turovsky, I. (2017). GosSOPKA: Russia's national cybersecurity system. Moscow Cybersecurity Review.
Usman, H. (2015). Cybercrime investigations in Pakistan: A review of NR3C's role. Pakistan Law and Policy Review, 7(3), 45–68.
Wolff, J. (2021). Cybersecurity and Russia's evolving strategy: The role of the GRU. Oxford Journal of Cybersecurity, 9(2), 103–119.
Xu, Z., & Lu, Y. (2021). China's cybersecurity diplomacy: Engagements with ASEAN and UN frameworks. Journal of Asian Cyber Affairs.
Zahoor, M. (2022). Cyber warfare and Pakistan's legislative measures: An assessment. Pakistan Journal of Security Studies, 7(2), 78-99.
Zaidi, A. (2017). Cyber conflicts in South Asia: A study of Indo-Pak cyber-attacks. International Journal of Cybersecurity Policy, 12(3), 33-57.
Zuberi, A. (2021). Cyber incidents in Pakistan: A critical assessment of the National Cyber Security Policy. Cybersecurity & Policy Review, 10(1), 98-125.