



Deploying artificial intelligence in warfare and national security: A qualitative exploration of strategic implications for Pakistan

Shahbaz Ahmed Shahzad, Muhammad Khalid Anser, Ihtisham Ul Haq, Alamzeb Aamir & Khalid Zaman

To cite this article: Shahbaz Ahmed Shahzad, Muhammad Khalid Anser, Ihtisham Ul Haq, Alamzeb Aamir & Khalid Zaman (2026) Deploying artificial intelligence in warfare and national security: A qualitative exploration of strategic implications for Pakistan, *Global Change, Peace & Security*, 37:2, 91-123, DOI: [10.1080/14781158.2025.2611230](https://doi.org/10.1080/14781158.2025.2611230)

To link to this article: <https://doi.org/10.1080/14781158.2025.2611230>



Published online: 12 Jan 2026.



Submit your article to this journal [↗](#)



Article views: 404



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)



Deploying artificial intelligence in warfare and national security: A qualitative exploration of strategic implications for Pakistan

Shahbaz Ahmed Shahzad ^a, Muhammad Khalid Anser ^b, Ihtisham Ul Haq ^c,
Alamzeb Aamir ^d and Khalid Zaman ^{e,f}

^aNUST Institute of Peace and Conflict Studies (NIPCONS), National University of Sciences & Technology (NUST), Islamabad, Pakistan; ^bFaculty of Economics and Administrative Sciences, Department of Economics, Recep Tayyip Erdoğan University, Rize, Türkiye; ^cDepartment of Econometrics, Tashkent State University of Economics, Tashkent, Uzbekistan; ^dDepartment of Management Sciences, FATA University, Kohat, Pakistan; ^eDepartment of Economics, The University of Haripur, Haripur, Pakistan; ^fDepartment of Research, The Sherwan institute of Online Education (SIOE), Abbottabad, Pakistan

ABSTRACT

The study examines Pakistan's artificial intelligence (AI) strategy for national security and defence. It identifies AI trends and effects using qualitative data from 105 military, intelligence, cybersecurity, and government specialists. Thematic research indicates AI improves military decision-making, intelligence synthesis, surveillance, and real-time risk assessment. Participants emphasised the importance of AI in military resource allocation, target precision, predictive analytics for terrorist activities, and border security. The findings reveal that AI enhances operational efficiency by improving situational awareness, threat detection, and reducing human error. Specialists are debating the ethical and strategic implications of algorithmic responsibility and autonomous weapon systems. Many consider the absence of institutional and legal frameworks for AI in defence a significant policy gap. AI may improve digital protective layers while rendering them more vulnerable to attacks. Due to inadequate training facilities and talent development, shortages in domestic AI research and military innovation capabilities are prevalent. Experts recommended investing in AI-driven defensive ecosystems, ethical protections, and localised AI procedures. The findings suggest that AI could transform Pakistan's military strategy with adequate leadership, preparation, and ethical considerations.

ARTICLE HISTORY

Received 21 July 2025

Accepted 25 December 2025

KEYWORDS

Artificial intelligence;
national security; warfare;
military strategies; security
policies; Pakistan

Introduction

Artificial intelligence (AI) is a fast-evolving technology that, in the modern world, is causing many repercussions in various spheres, along with warfare and national security. Artificial intelligence has now become a cornerstone of technological development,

CONTACT Khalid Zaman  khalid_zaman786@yahoo.com  Department of Economics, The University of Haripur, Haripur, 22620 Khyber Pakhtunkhwa, Pakistan Department of Research, The Sherwan institute of Online Education (SIOE), Abbottabad, 22062 KPK, Pakistan

© 2026 Informa UK Limited, trading as Taylor & Francis Group

which has revolutionised effects on global defence policies (Osimen, Newo, and Fulani 2024). Notably, the application of AI to military, intelligence, and national security strategies has become a pressing concern for countries worldwide. Pakistan and other nations in a geopolitically sensitive region should have both the opportunity as well as the challenge of analyzing the implications of AI in war and national security critically to stay prepared and guard national interests in every aspect (Sahu et al. 2025).

Over the past few decades, the face of warfare has drastically transformed, mainly due to the transformation in technology. Among the most significant changes are the emergence of AI in military operations and the impact on states' views of defence and war. Applying AI technologies, it is possible to create very sophisticated systems which can work with huge amounts of information, make their own decisions, and fulfil very complex tasks without the direct involvement of human operators (Al-Dulaimi and Mohammed 2025). These advances are most notable in autonomous weapon systems, intelligent surveillance and reconnaissance, cyber warfare, and military decision-making systems. Even autonomous drones, which AI now powers, can perform surveillance, precision strikes, and targeting functions. The various capabilities produced by the implementation of AI-powered cyber tools have also made military forces well-versed in offensive and defensive cyber operations, and the information on data analytics enriched with AI capabilities could provide unmatched intelligence, potentially in real-time (Garcia 2024).

AI is no longer the prerogative of traditional war. It is now a component of nearly every facet of military strategy, logistics, and supply chain management, as well as soldier training and intelligence collection (Darıcı and El-Bayaa 2024). Artificial intelligence may imitate the behaviour of an opponent, recognise the main threats in real time and help to make important decisions, which would have been impossible to achieve in the past (Hunter 2025). This integration is a great enhancement to military readiness, operational efficiency, and speed of decision, all essential in the contemporary swift battlefield. War is not the only field where a revolution is taking place; the strength of AI is changing national security (Jozaghi 2025). The use of AI has revolutionised how countries operate in matters concerning border management, counterterrorism, prevention of crime and disaster relief (Syllaidopoulos, Ntalianis, and Salmon 2025). AI technologies allow national security agencies to collect and analyze vast amounts of data to follow real-time threats, strengthen law enforcement operations, and defend critical infrastructure against cyber-attacks (Govea, Gaibor-Naranjo, and Villegas-Ch 2024). Artificial intelligence can track terrorist activities, detect obscure trends in large sets of information, and update intelligence on potential threats in real-time.

Cybersecurity is one of the most widely known uses of AI in national security. Due to the increased dependence of nations on digital infrastructures, the risks of cyber attacks have escalated exponentially (Radanliev 2024). Unlike human-operated security systems, AI-based systems can predict, detect, and respond to cyber threats much more quickly and efficiently (Kavitha and Thejas 2024). This becomes essential in assuring the resilience of national defense and security infrastructures, particularly in countries such as Pakistan that are bounded by various external and internal security challenges. AI utility can be used to analyze communications and digital footprints to predict the flow and actions of terrorist groups, enabling security agencies to intercept threats before they escalate (Capodivacca and Giacomini 2024). AI can help drive intelligence-gathering

services by automating tracking operations, identification of significant individuals or organisations involved in illegal practices, and handling intercepted conversations (Sers-cikov 2025). In addition, AI is augmenting border security, as now intelligent surveillance systems and automated checkpoints can be used, and it is simpler to secure and monitor national borders (Yabanci 2025). AI technologies can also help track movement patterns and detect abnormal movements, which cannot be underrated in terms of preventing illegal crossings and human trafficking and smuggling (Mademlis et al. 2025).

AI presents both a challenge and an opportunity for Pakistan. Pakistan, being a strategically located nation in South Asia with a complex security situation, must be cautious in considering the punitive repercussions of initiating AI in warfare and national security (Mir and Nazir 2024). The geopolitical position of the country, its borders with India, Afghanistan and Iran and the complex relations with global powers such as the United States and China predetermine the situation in the country in terms of security (Singh, Raj, and Radha 2024). In Pakistan, security is challenged primarily by cross-border terrorism, internal insurgencies, and the threat of cyber warfare (Azam, Khattak, and ul Ain 2025). Consequently, AI technologies can be instrumental in enhancing security in the country. Pakistan has already been exploring the possibilities of AI in enhancing its military (Akhtar and Sethi 2024). Some military applications of AI include autonomous weapons systems, surveillance technology and cyber security. Furthermore, AI can enhance the effectiveness of Pakistani military logistics and command structures (Wall 2025). By implementing the solutions provided by AI-powered systems, Pakistan can achieve a new level of efficiency and precision in military operations, thereby reducing collateral casualties and enhancing the strategic effectiveness of its safety systems. Nevertheless, the introduction of AI into the Pakistani national security context is not unaccompanied by issues. Questions about the ethical use of AI, particularly in autonomous weapons systems, are of great concern (Ohwo 2025). The possibility of the misuse of AI against international humanitarian law begs the important questions of accountability and the rules of engagement in any future conflicts. Moreover, Pakistan should consider the strategic balance in the region. AI developments on the defence side may trigger an arms race with other nations, especially India, which is also exploring the use of AI in the military (Singh and Tiwari 2025).

Pakistan's approach to AI and national security depends on its perceptions of China and India as regional powers. China, Pakistan's 'all-weather ally', has helped Pakistan's AI trajectory via technological cooperation, military ties, and capacity-building. China-Pakistan Economic Corridor (CPEC) has helped expand digital infrastructure, and Pakistan's defense planners have used China's AI-driven surveillance, data analytics, and military modernisation as models. Pakistan has explored the application of AI in cyber protection, prediction, and automated command systems via this partnership (Feroz et al. 2025). Due to India's rapid advances in AI research for defense applications, notably drone warfare, satellite imaging, and data-enabled military logistics, Pakistan is under strategic pressure to accelerate its AI deployment to maintain regional balance. Pakistan has been closely monitoring India's formation of the Defence AI Project Agency and Defence AI Council, which it sees as regional militarisation of AI. Pakistan's AI strategy uses Chinese technological collaboration to innovate and prepare, and it responds to India's competitive advancements to prevent strategic imbalance (Ali and Cheema 2025). These interrelated regional factors underline Pakistan's AI strategy and its resolve to integrate AI into national security frameworks for geopolitical reasons.

The security agencies in Pakistan also have to deal with issues regarding the applications of AI in cybersecurity. It is not the first time the country has been hit by cyber attacks, with some being linked to state-sponsored attacks (Saleem et al. 2024). Pakistan will need to invest in AI-enhanced systems capable of real-time detection and neutralisation of threats to improve its cybersecurity posture. This would assist in safeguarding vital infrastructure, military systems and government systems against more advanced cyber threats. However, as the significance of AI increases in the sphere of military and national security, the gap in the research, specifically in the case of Pakistan, stands out (Khan and Khan 2025). Although a considerable body of extant literature exists on the technical elements of AI uses in the defence and security spheres, a detailed qualitative study on the strategic effects of such technologies, particularly in a South Asia-type complex security environment, is needed (Taddeo, Blanchard, and Thomas 2024; Weissmann 2025). Besides, the ethical, political, and social consequences of AI in warfare and national security have not been adequately discussed. These gaps are especially well-suited to exploration by a qualitative approach. This study aims to explore the strategic, ethical, and operational implications of AI for Pakistan's defence and national security through in-depth interviews. The qualitative study enable the conducting of an advanced analysis of the perception of AI among defence and security professionals, policymakers, and military leaders and how the perception influences the decision-making process. Furthermore, a qualitative study will help identify the most relevant issues and problems associated with AI integration into the Pakistan national security system, as these may involve accountability, governance, and security implications in the region.

The qualitative research in the area of the strategic consequences of AI also help to create a framework to instruct how Pakistan could implement AI technologies without putting national security and the stability of the region at risk (Davis and Bracken 2025). By analyzing the specifics of the security context of Pakistan and the general geopolitical scenario, this study will contribute to the global discussion on the importance of AI to warfare and national security, particularly in South Asia. AI has the potential to change the future of warfare and national security, at least in countries like Pakistan that are forced to handle complex security dilemmas. The strategic implications of these technologies can only be understood through a holistic, qualitative analysis that goes beyond the technical side of things and factors in the ethical, political, and societal implications (Ndzendze and Marwala 2023). This study addressed this gap by conducting research that gives a more in-depth understanding of the qualitative nature of AI contributions to the defence and national security of Pakistan to inform future policy decision-making.

Literature review

In his book, Roy (2024) claimed that the possibilities that AI opens up are colossal, not only to Russia but to all humanity, and that there are also dangers that it is hard to foresee. AI is going to change international politics to the extent that whoever among the nations and leaders takes over this realm will take over the planet. More recently, AI has evolved as a national security issue since AI assists warfare with the creation of cyber weapons, droning and quadcopter surveillance and attacking the enemy. According to Ndzendze and Marwala (2023), there are three broad categories of AI, which can be categorised into

international politics and policymaking as instrumental factors. They said AI can contribute its part as an analyst in international politics, where it will provide analysis, evaluate, and identify the tendencies of decision-making. Secondly, they suggest that AI will explicitly take on predictive roles and provide policymakers with opportunities to learn about potential future events. AI can foresee the political outcomes of elections, the course of geopolitics, economic results and other political processes. Third, the AI will assume operational roles by equipping a country with a semi-autonomous force and facilitating security initiatives. A country that possesses an independent system is more competent than a non-possessing one. Cummings et al. (2018) explain that AI will become an element of militaries globally. The transformation of autonomous security measures like the war, weapons, and nuclear missiles of China, Russia, and the United States are in progress. The international security environment is undergoing significant disruptions. Sooner or later, states that are rich in financial and intellectual resources will present autonomous weapons and weapons of warfare as their security service. However, this will also cause insecurity among small countries that are underdeveloped and lack economic or intellectual resources, as they perceive the use of AI in warfare as a distortion of the power balance.

Horowitz et al. (2022) extend this discussion to human security, political, social, economic, and quality of life, arguing that the further expansion of AI and manufacturing will impose burdens on the world economy, leading to a new era of rebalancing political and economic influence. Moreover, he speculates that AI has immense potential to empower governments, the global community, and economic sustainability to mitigate human insecurity. AI can offer progress in all walks of life and can benefit in ensuring the basic needs, in curbing poverty and violence and in forecasting peace in the world. Lorenzi and Berrebi (2019) are convinced that the productivity boom of AI is economically possible. The positive change that will emerge in AI is the new form of production; the trends have been shifting, and individuals are not sticking to the old trends but trying to come up with newer methods of economic stability. The effect of AI will be greater on international trade and development. Jensen, Whyte, and Cuomo (2020) define AI by adopting to using the adoption capacity theory and contend that the adoption of AI will render the balance of power since economic and organisational demands of historical innovation determine disruption. They continue to stress that answering the effects of AI on the balance of power, technology adoption capacity theory indicates that AI will transform the nature of war. In World War I, the machine gun significantly impacted those with less advanced weaponry, favouring those who possessed it. Similarly, AI has altered the lethality of battles, military tactics, and the characters involved, shifting the balance of power and international politics. Russia is working intensively on designing uncrewed vehicles, missile systems, submarines, and remotely piloted tanks for security and defence purposes. China views AI as a significant strategic opportunity and outlines an integrated approach. Rickli and Mantellassi (2023) note that the AI debate emphasises the need for interdisciplinary research to assess the positive and negative aspects of AI in a global context, serving as a backup measure to understand the threat. It is in the world economy as well as the military rivalry where the power is going to be shifted with the profound potential of AI. Applications of military advancement and national security in stable economies defend the balance of power. The US, Russia, and China established a national security centre to develop military AI, with the latter being

significantly less advanced than the former and on the vanguard of AI. Hence, China, Russia, the USA, and France are investing heavily in AI. The UK has agreed to cooperate with France. Germany is also investing with China. Israel has taken a 180-degree turn and focused on turning its national security into AI. The US-Israel cooperation in joint military projects like autonomous drones has brought new significance to defence strategies.

Muthusamy and Negi (2018) posit that Japan, Saudi Arabia, the UAE, and India also aim to strengthen their defence capabilities through enhanced bilateral relations in AI. In 2018, India invested a sum of 477 million dollars into its Digital India program. This encompasses machine learning, 3D printing, and advances in technological expertise, offering privileges to people and the military sector as India prepares to develop autonomous weapons for national defence. The study by Ettlinger (2022) contends that the use of machines by adversaries is to establish a system that succeeds in manipulating the beliefs and thoughts of the citizens in a manner that cannot be detected. This school also considers AI as a weapon of mass destruction since it will produce a mass influence that can be applied as leverage in future wars. Thus, the advent of AI-enabled warfare will not be based on a new panacea of one weapon system, technology, or a military concept of operation. Instead, it will revolve around the employment and the deployment of AI-enabled technologies in all aspects of warfighting. Li (2025) highlight that AI integration in military strategies enhances capabilities like autonomous systems and real-time decision-making. They find that while AI strengthens defence, it also raises concerns about warfare automation, cybersecurity risks, and global stability. The study calls for robust regulations to manage AI's impact on security policies. Budacu (2024) present a contrasting view regarding AI as a mechanism of misinformation that could lead to cyber wars, potentially compromising the security of countries. Traditional wars and weapons have ceased to be by state and non-state actors. These players are leveraging cyberspace to manage information and broadcast their agenda, which can compromise national security. These waves of AI are not merely augmenting disastrous action, as they also coordinate action against the government and law enforcement. As Galar, Kumar, and Seneviratne (2020) state, the technology of autonomous systems and, in particular, the unmanned aerial vehicles (UAVs) and the uncrewed ground vehicles equipped with AI are the breakthroughs in terms of information gathering and accomplishing missions in the field. The synergy of AI provides such autonomous systems with an opportunity to operate without direct human intervention and consequently reduce the risk of human life being exposed to direct threats in various operations. UAVs and unmanned ground vehicles (UGVs) can complete reconnaissance, border patrol and search and rescue tasks, as opposed to any other alternative currently available, by using advanced AI algorithms that will make them highly efficient. Malik, Kamal, and Nazar (2023) also validate that through the utilisation of AI, such self-driving cars can perceive and navigate complex environments, read real-time data, and make informed decisions at will. This subsequently not only enhances the pace at which the missions are accomplished and their precision but it enlarges the area that defence and security forces cover. The introduction of AI-supported autonomous motions is one of the grand initiatives to offset human exposure to potential threats and capitalise on the effectiveness of life-saving missions that reveal the overpowering impact of the integration of technology in contemporary militaristic capabilities. Guedes Gonçalves Costa (2024) state that incorporating AI into national security plans

promises both opportunities and challenges like never before. It is therefore important that, in the face of such a complex situation, the balance has to be sought between maximising the advantages of AI in defence and embracing the ethical, legal, and security implications of such an initiative. Adapted and used responsibly, AI can significantly improve the efficiency of national security operations, giving a strategic upper hand in a constantly changing geopolitical world.

Recent academic research and policy publications may assist in explaining Pakistan's military and security usage of AI. In their recent publication of the Peace Research Institute Oslo (PRIO), Roy and Reichberg (2024) examine how Pakistan's strategic stance toward China and India is being influenced by the pursuit of AI-enabled capabilities, despite resource and institutional issues. They found that Pakistan is using AI for border control, data-driven decision-making, and surveillance to compensate for its neighbour's military edge. They also caution that military AI deployment lacks clear regulatory procedures and risks becoming increasingly dependent on foreign vendors, particularly China. Meanwhile, Pakistan's national policy framework may provide further information. Pakistan's National Artificial Intelligence Policy emphasises data infrastructure, human capital, ethics, and inclusive innovation in its AI adoption, but not defense. While the strategy prioritises economy and civil society, it creates the framework for defense-focused AI adoption by demonstrating the state's commitment to the AI ecosystem. Combining the PRIO report's defense-centric research with Pakistan's domestic AI governance framework helps us comprehend local institutional, strategic, and ethical aspects affecting AI in Pakistan's security sector. This connects South Asian viewpoints to global AI in wartime literature.

The convergence of cyber defense, space technology, and AI has been identified by earlier literature in the context of Pakistan's economy and found to be a critical factor in the stability of Pakistan's national security and its foreign policy. Khan and Khan (2025) argued that cyberspace is now part of conventional security, and Pakistan and India are more susceptible due to the lack of deterrent frameworks. Early warning systems, predictive modelling, and AI-enabled threat detection were essential to domestic cyber-deterrence. The study also recommends Cyber confidence building measures (CBMs) to reduce misconceptions, build digital trust, and prevent cyber crisis overreactions. The study suggests that AI-powered cybersecurity might assist Pakistan's defenses in resisting asymmetric assaults and sustaining regional deterrence. Ahmad, Hussain, and Mir (2024) identify regulatory deficiencies in Pakistan's digital governance architecture, particularly in data security, algorithmic transparency, and accountability in defense-related AI applications. These gaps are due to digital transformation regulation and governance. Due to a weak regulatory environment, Pakistan is prone to ethical and technological exploitation. This applies especially to dual-use AI systems, which may be utilised for military and civilian reasons. The study recommends a multi-tiered regulatory structure including capacity development, institutional coordination, and adaptive legislative instruments to align Pakistan's digital policies with global AI governance principles. They support the idea that responsible innovation requires legal and ethical frameworks as well as technical expertise for long-term AI implementation in national security. Amir and Rehman's (2024) study on space technology's influence on Pakistan's military and foreign policy is insightful. The study argued that Pakistan has fallen behind regional competitors like India in developing space-based capabilities, i.e. geospatial mapping,

communications, and satellite surveillance, which have revolutionised warfare. The study cautions that ignoring indigenous space capabilities may be strategically harmful as South Asia militarises space. By comparing India's domestically developed systems to Pakistan's leased satellites, the study highlights a dependency disparity and argues for a robust national space policy. By investing in space and artificial intelligence, Pakistan can strengthen its military's C3I structures – command, control, communication, and intelligence – thereby enhancing operational effectiveness and strategic coordination.

Theoretical framework

The usage of AI in military conflicts and national security requires a theoretical apparatus that might describe how technological changes transform the geopolitical arena. Technological Determinism Theory and Securitisation Theory are two theories that can contribute to the explanation of these changes. Such theories provide conceptual spectacles through which the strategic impact of AI on the defence and national security of Pakistan can be much more comprehensible.

Technological determinism theory

The Technological Determinism Theory (TDT) is a theory that posits that technological innovations are the main agents of social, political and economic change. This theory posits that technology influences human conduct and societal evolution, regularly causing unexpected changes in various spheres, including defence and security (Tessema 2021). Applied to the problem of AI in warfare and national security, technological determinism implies that the development and adoption of AI technologies will not solely revolutionise military capabilities but will also reinvent the approaches to national security, both personal and state-based. TDT owes its origin to the arguments of thinkers, such as Marshall McLuhan and Thorstein Veblen, that tools and technologies that society creates are at the centre of shaping cultural, social and political environments. The latter is embodied in the well-known aphorism of McLuhan, 'The medium is the message', which pointed out the radical influence of technological inventions on the functioning of societies and their self-organisation (Lauwaert and Chomanski 2025). Within the context of military power, TDT holds that new technologies influence shifts in the organisation and practice of war. Being one of the most important technological innovations of the twenty-first century, AI changes the math of military affairs fundamentally. The deployment of AI in military systems, including autonomous drones, intelligent surveillance systems, and AI-based decision-making cycle, turns the balance of power in the international arena (Budacu 2024). This technological change is particularly relevant when applied to a tense security dynamic region like South Asia, where AI can become a force multiplier for nations like Pakistan (Winkel 2025).

Military power transformation

AI technologies prioritise optimisation of performance related to such essential domains of military strategy as intelligence gathering, targeting accuracy, and efficiency (Khayat et al. 2025). AI integration in weapons systems enables drone operations without human control, which are capable of conducting surveillance and making military

attacks on their own. Because of that, military forces will be less dependent on human labour and more on advanced AI systems (Char 2024). Such a change in military actions is a radical one: whereas previously all actions were taken by people based on their decisions, now the actions are guided by data and are executed by AI, which makes them more accurate, quicker, and ultimately possibly more efficient in war situations. Another notion brought forward by AI is network-centric warfare, whereby connected AI systems can plan and synchronise military action in the various military domains. The fact that AI can crunch through large volumes of data and present actionable intelligence in previously unheard-of time scales gives a country a greater capability to plan and conduct military operations with a much higher level of accuracy (Taber 2025). This revolution in military affairs marks a change in the functioning of defence systems, and it highlights the case advanced by technological determinists that new technologies modify the very structure of military capabilities.

Reforms in national security strategies

National security strategies are no exception to technological determinism, with AI becoming the force behind how countries approach their defensive mechanisms. AI technologies enable a more preventative and proactive approach to security. Within the Pakistani framework, AI may contribute to strengthening cyber defences, advancing intelligence collection, and increasing border security (Rogers 2025). Predictive AI-based security solutions capable of detecting cyber threats in real time can secure critical infrastructure against attacks. In contrast, AI-empowered surveillance systems can assist security agencies in border monitoring and improve their capability to track terrorists (Hunter et al. 2024). AI use in national security extends beyond the military as well. AI-powered surveillance drones, facial recognition, and predictive analytics are changing the face of security by allowing it to be more holistic and proactive in approaching national defence. In the case of Pakistan, AI has the potential to transform its approach to counterterrorism and counterinsurgency, allowing the security establishment to implement proactive measures due to the analytical and forecasting capabilities of AI to determine possible threats before they materialise in real-life situations (Holster, Bullets, and Fitness 2025). Furthermore, technological determinism implies that, as countries continue to depend on AI to improve their military, they will start to regard technological superiority as a national security pillar (Parisini 2025). That may create a new arms race, where nations are no longer competing primarily through workforce or even conventional weapons but through technological capability, specifically AI-enhanced defence capabilities.

Securitisation theory

Securitisation Theory centres around how some issue can be constructed as an existential threat to national security and hence warrant extraordinary measures to defend against it (Buzan and Wæver 2009). The process of securitisation is based on the idea that security threats are constructed discursively, and political actors (government officials, experts, and institutions) claim that particular issues are an immediate threat to the state and its citizens (Baele and Jalea 2023). They are then securitised, which is formulated as an issue of urgency that necessitates extraordinary action, usually outside the ordinary course of political or legal procedure. When applied to AI in national security, the

Securitisation Theory can be used to understand the process through which AI technologies have been constructed as essential means of national defence (Wertman and Kaunert 2022). Due to the evolution and increasing integration of AI technologies into military and security strategies, it can serve both as a defensive and offensive capability, making it the primary focus of national security discourse. Nonetheless, securitisation implies not only the creation of AI systems but also the construction of these technologies as crucial to the life and stability of a nation in the popular imagination and government documents (Zeng 2021).

AI as a securitized issue

To become indispensable in national security, AI needs to be recognised as a security concern in the first place. One such framing is the presentation of AI as a defence measure against continuously evolving threats, including cyberattacks, terrorism, and geopolitical competition (Khan, Khurshid, and Cifuentes-Faura 2024a). In nations, where national security is under constant threat by a multitude of external and internal agents, the rhetoric of AI can shift towards establishing AI as an immediate security need (Lukacovic 2025). Positioning AI as a matter of strategic imperative will allow political and security elites to marshal resources, legitimize military spending, and rally the population in support of technological investments (Bächle and Bareis 2022). AI framings are shaped by individuals in national security institutions, including military commanders, national intelligence organisations, and policymakers (Chapman 2020). These actors are important to the securitisation process because they employ rhetoric to frame AI as a high-priority defence mechanism to meet specific security challenges (Livingston 2022). As another instance, it may be suggested that Pakistan needs to adopt AI to prevent the erosion of its national interests by more technologically advanced opponents, thereby supporting the idea of AI as a valuable part of military preparedness.

Justifying exceptional measures

When AI technologies have been securitised, governments might pursue the adoption of exceptional measures to ensure that such technologies are being developed, fielded, and defended. Among them, there may be heavy investments in AI research and development, shifts in national defence policy, and the creation of special AI military forces (Zeng 2021). Securitisation of AI may also result in the establishment of new legal and ethical frameworks to regulate its applications, especially in military activities and cyber security (Mügge 2023). Securitisation of AI in the Pakistan context could lead to a national security policy that dubs AI as the central point of national security efforts. Policymakers might justify the importance of AI by suggesting that it is essential to ensure strategic balance with regional powers and to guard the nation against external aggression, particularly in light of the bitter relationship between Pakistan and its neighbour India (Merrill 2024). Using such a framing, Pakistan would see AI through the lens of existential security threat, therefore ensuring that the pronouncement of AI technologies into the national security complex would be a priority of the highest strategic importance (Wasi 2024). Additionally, another aspect of securitisation is the legitimisation of AI technologies in the discourse. The broader population needs to be persuaded that AI is a necessity when it comes to the national security of the country, not just in terms of military defence but also in cyber defence and internal surveillance (Kihato 2025). Governments

attempt to influence the minds of citizens and establish political legitimacy regarding the use of AI in critical national security sectors through media campaigns, the views of experts, and official government pronouncements.

The regional and global aspects

Securitisation of AI and national security is not a phenomenon restricted to the national level. The securitisation process also has a regional and global aspect as nations such as Pakistan build AI capacities. In addition, the use of AI in defence systems is likely to result in an arms race among the adjacent nations (Devrari, Kumar, and Kuchhal 2024). This viewed AI as a national security issue, which can lead to further escalation of the competition in technological advancements as states rush to gain the upper hand in AI technologies in an attempt to maintain a respected military and strategic future (Horowitz, Kahn, and Mahoney 2020).

Methodology

The current study was anchored on a qualitative research approach, and the study purpose was to explore the strategic, philosophical, and operational considerations of AI in military conflict and national security using the perspectives of Pakistan experts. Through interpretivism, the study aimed to learn about the nuances of the effects of AI on national security and defence in the nation. Patterns, recurring themes, and awareness gained by the participants regarding various sectors were identified through thematic analysis of conducted interviews.

Research design

The study was consistent with the exploratory, interpretive qualitative research design, which is optimal in a situation where the researcher will be interested in exploring the nuances of specialist perception on the subject matter of AI in war and national security. The study is in opposition to the quantitative methods and the focus on testing hypotheses, as it was aimed to gain a more profound knowledge and understanding of the perceptions of AI technologies and their integration with national defence strategies (MacLure 2024). Military officers, policymakers, defence analysts, cybersecurity experts, and AI experts have been interviewed and provided detailed, first-hand experience, observation, and forecasts on the impact of AI. Thematic analysis was used as a method of data analysis. Such a strategy meant identifying popular themes, patterns, and emerging issues throughout interview transcripts to form an overall image of how different experts viewed and responded to the ramifications of AI in the field of national defence. Coding and categorising the data into content areas enabled the researcher to derive some of the significant findings associated with the strategic, operational, and ethical implications of AI usage in warfare and national security.

Sampling strategy

Using a purposive sampling methodology, 15–20 participants were identified within five important sectors of military and national security activity in Pakistan. The main objective

was to ensure that the chosen respondents had the required knowledge and experience to share meaningful information about the topic of AI in defence and security. The sectors where participants were chosen comprised:

- **Military and Defense Institutions:** This group consisted of military officers, defence planners, and specialists who were directly engaged in the management and implementation of defence activities. Their insights played a key role in how AI was influencing military strategies and operations and overall defence capabilities.
- **Intelligence Services:** Intelligence officers who operated in data analysis, surveillance, and counterterrorism operations were involved. By examining the use of AI in intelligence collection, cybersecurity, and surveillance activities, they contributed to the national security picture regarding AI employment (Dehalwar and Sharma 2024).
- **Cybersecurity Professionals:** As the weight of cyber defence gains relevance, it was necessary to have individuals who were knowledgeable in guarding the critical infrastructure against cyber-related threats. Their expertise gave them an idea of how the AI was being used to bolster national security against digital attacks and spy intrusions.
- **Academia (AI and Security Studies Experts):** The members of this category were university professors, researchers, and scholars who dedicated their efforts to AI technology, military strategy, and national security. These professionals provided both theoretical and practical knowledge about integrating AI into security systems, as well as the comprehension of the future trends in the field of AI research.
- **Public Policy Think Tanks:** These individuals participated in the crafting of national security provisions and provided opinions on how AI was being incorporated into the policymaking process involving matters of defence, international affairs, and national security.

Inclusion criteria

To ensure that the selected participants have the relevant knowledge and experience, the study narrowed the respondents to the representatives who had at least five years of experience in their current role and demonstrated awareness of AI technologies or national security-related issues (Smith 2024). The experience instilled confidence in members that it was one of the best sources of information on the connection between AI and national defence, and their contributions would aid the research.

Exclusion criteria

Those who did not fit into the above criteria or had no personal experience in the domain of AI or national security were left out. This requirement allowed researchers to focus on professionals, thereby providing significant assistance in the subject matter of their research (Tisdell, Merriam, and Stuckey-Peyrot 2025).

Data collection

The method of data collection involved a semi-structured, open-ended interview, which allowed the interviewee to provide open answers to the questions. This form of interview

was also chosen because it was designed to cover all necessary areas. This kind of methodology facilitated the discussion of how the participants thought about the prospective role of AI as regards national security and military strategy and ethics. The semi-structured structure provided the researcher with the opportunity to control the discussion, focusing on specific topics while also allowing participants to share their perceptions, views, and concerns (Ren 2025). The interview method followed was characterised by a combination of face-to-face, virtual, and telephone interviews depending on availability, preferences, and sensitivities of respondents. Interviews that could be conducted face-to-face were prioritised for those who could meet in person, as it is a more direct and personal interaction. The interviews took place virtually via secure platforms such as Zoom or Skype, which allowed participation by interviewees who were situated in other regions. Where face-to-face or virtual meetings were impossible because of logistical or security reasons, telephone interviews were an alternative.

The interviews took place between 30–60 min, which allowed participants to share their opinions and experiences in detail. With the express permission of the participants, all interviews were audio-recorded to facilitate accuracy in transcription and analysis. The interview was immediately transcribed, after which data analysis was fully done (Smith 2024). Thematic analyses were done on transcribed interviews. The important themes were discovered during coding, and the pattern analysis was conducted regarding strategic, operational, and ethical implications of AI to create a more complete image of its engagement in the field of national security. They prioritised the ethical considerations and anonymized the data to prevent the identification of participants, particularly given the sensitive nature of the topic of interest. Lastly, purposive sampling, semi-structured interviews, and thematic analysis enabled the study to gather meaningful, qualitative data comprising diverse professionals with adequate background information in the realm of military strategy, national security, and AI technologies. The approach enabled the researcher to delve into the topic of applying AI to the Pakistani defence establishment, uncovering the necessary information and fears that make AI in national security a promising area for discussion.

Sample interview questions

Ten open-ended questions were asked, such as:

- (1) What role do you see AI playing in Pakistan's defense strategy?
- (2) What ethical concerns do you associate with AI in warfare?
- (3) What are the main benefits and opportunities you associate with AI in warfare?
- (4) What challenges or risks do you foresee with integrating AI into military operations?
- (5) How do you view the ethical implications of using autonomous weapons in conflict?
- (6) What is your perspective on Pakistan's readiness to adopt AI-based defence technologies?
- (7) How can AI contribute to counterterrorism and internal security efforts in Pakistan?
- (8) What policies or frameworks are necessary to ensure responsible AI use in defense?
- (9) How do you evaluate the human-machine collaboration potential in the battlefield?
- (10) What are your recommendations for building AI capabilities in Pakistan's defence sector?

Data analysis

The data collected from interviews were analyzed using thematic analysis following the six-step framework outlined by Braun and Clarke (2006). The goal of thematic analysis was to identify, analyze, and report patterns (themes) within the data, which provided rich insights into how AI was perceived and applied within the context of warfare and national security.

- **Familiarization with Data:** The initial phase of the analysis process was to gain profound acquaintance with the data. This involved going through and re-going through the transcriptions of the interviews and immersing myself in the material. At this stage, some preliminary thinking, possible ideas and a sense of the depth and breadth of the data started to develop. The researcher made notes of recurring concepts and preliminary patterns, which proved imperative in the subsequent processes (Hannah et al. 2025).
- **Code Generation:** At this stage, the researcher started to code the data by marking out those particular parts of the text that were of interest to the research questions. These codes summarised important features of the data that were deemed interesting or important. As an illustration, the segments addressing military use of AI, ethical issues, or perceived advantages of AI in cybersecurity received corresponding codes. These starting codes were put in a coding structure in Excel, making it easy to retrieve and compare.
- **Themes creation:** After initial coding had been accomplished, the researcher started to sort these codes into larger themes. Themes were defined according to patterns and correlations among codes. To give some examples, the themes formed around problems like 'the influence of AI on military strategy', 'ethical questions raised by autonomous systems', or even 'the place of AI in cybersecurity'. These themes represented major issues and concerns mentioned by participants in interviews.
- **Reviewing Themes:** Once the possible themes were found, the second step was to review them. This entailed examining whether the themes effectively captured the underlying data and whether they were sensible in relation to the research questions. Certain themes had to be revised, merged, or abandoned. The researcher made sure that every theme made a valuable contribution towards comprehending the role of AI in national security (Sale and Carlin 2025).
- **Defining and Naming Themes:** After the final set of themes was reached, the themes were clearly defined and named. The definitions were aimed at describing the nature of each theme and its relevance in addressing the research questions. As an example, the discussions on the technological and military benefits of AI could have become a theme called AI as a Strategic Asset.
- **Writing the Report:** The final step involved writing up the findings whereby the researcher presented the identified themes together with supporting data. This was accompanied by elaborate examples of the interview transcripts, as well as interpretations and analysis, which described how AI was viewed in the framework of Pakistani national security and military policies (Lim 2025). The report aimed to draw together the lessons learned during the thematic analysis and offered an overarching perspective on the strategic, ethical, and operational aspects of AI in defence. Manual coding was conducted using Excel, which facilitated the organisation of the

data and allowed the researcher to easily track patterns, codes, and themes. Excel served as a simple and effective tool for data organisation and analysis, ensuring that all themes and codes were systematically tracked and reviewed.

Ethical considerations

Ethical issues were taken seriously in this study to ensure that the participants were secure and had rights. The institutional review board obtained ethical approval before data collection. This has been achieved by having a close look at the research protocol to ensure that it could be ethically undertaken, particularly concerning confidentiality, consent and handling sensitive data. Individuals received informed consent. As participants, they were fully briefed about the nature of the research, that the participation was voluntary and that they could abandon it without effect. The consent forms described the potential risks and benefits of participating, the anonymity of their responses and the intended use of data. Anonymity was maintained to ensure the privacy and confidentiality of the participants. No personally identifying details were requested or revealed, and any data which could potentially be utilised to cross-reference a participant with their answers was removed or anonymized in the data used. The research did not report the individual responses but rather confidential results. Considering the sensitivity of the research subject matter, especially on issues of national security, precaution was observed to avoid revealing any classified or sensitive information in the course of interviews (Eden, Chisom, and Adeniyi 2024). Matters touching on national security were handled cautiously, and the participants were reminded not to discuss anything confidential or classified. The researcher also made sure that the data was stored safely and could only be accessed by authorised persons working on the research. Generally, ethical issues were a concern throughout the study, as it was intended to be conducted responsibly and respectfully, ensuring that the participants and the study were not jeopardised.

Results

Table 1 provides the demographic data of the 105 participants, well distributed in different positions, including military members, policymakers as well as researchers. This makes it clear that most respondents are experienced, as most of them have served an average of 15 years in their various positions. The wide geographical distribution, which is Islamabad, Sindh, Khyber Pakhtunkhwa (KPK), and Punjab, has made it possible to have different geographical opinions regarding the incorporation of AI into national security and security. A vast pool of professionals can provide a comprehensive understanding of the potential threats of AI to the Pakistani security system.

About 70% of the 105 participants were commissioned officers from Pakistan's military forces. The poll included 15% captains and lieutenants, 25% majors and colonels, and 10% senior officers (brigadiers and policy experts with strategic supervisory roles). The infantry and armour divisions were less enthusiastic about employing AI for decision-making, surveillance, and predictive threat assessments than the intelligence, cyber, and signals divisions. This difference reflects the operational and technical branches' AI-driven system knowledge. Respondents from Islamabad, Sindh, Khyber Pakhtunkhwa, and Punjab highlighted Pakistan's military ecosystem's geographical and institutional diversity.

Table 1. Respondent demographics [*N* = 105].

Designation	Number of respondents	Average years of experience	Regions	Respondent code
Professors	19	18.5	Islamabad, Sindh, KPK, Punjab	A (Interview conducted in 2025)
Colonel	14	14.5	Islamabad, Sindh, KPK, Punjab	B (Interview conducted in 2025)
Consultant	14	15.2	Islamabad, Sindh, KPK, Punjab	C (Interview conducted in 2025)
Major	12	14.2	Islamabad, Sindh, KPK, Punjab	D (Interview conducted in 2025)
Researcher	12	22.5	Islamabad, Sindh, KPK, Punjab	E (Interview conducted in 2025)
Analyst	10	14.5	Islamabad, Sindh, KPK, Punjab	F (Interview conducted in 2025)
Lieutenant	8	12.5	Islamabad, Sindh, KPK, Punjab	G (Interview conducted in 2025)
Officer	6	14.3	Islamabad, Sindh, KPK, Punjab	H (Interview conducted in 2025)
Brigadier	4	13.5	Islamabad, Sindh, KPK, Punjab	I (Interview conducted in 2025)
Policy Expert	6	16.2	Islamabad, Sindh, KPK, Punjab	J (Interview conducted in 2025)

Table 2 presents the main themes and reactions to the interviews, indicating the variety of opinions on the use of AI in the Pakistan approach to defence. The respondents pointed out the potential of AI in making better decisions, monitoring, and operations.

Table 2. Key open-ended interview questions and summary of responses.

Interview question	Summary of responses
What role do you see AI playing in Pakistan’s defense strategy?	AI enhances surveillance, improves real-time decision-making, and optimises resource management in defense operations.
What ethical concerns do you associate with AI in warfare?	Ethical concerns include accountability, transparency, and the potential for AI to make unethical decisions in combat situations.
What are the main benefits and opportunities you associate with AI in warfare?	AI improves precision, decision-making speed, reduces casualties, and provides predictive capabilities to neutralise threats.
What challenges or risks do you foresee with integrating AI into military operations?	Challenges include infrastructure issues, cybersecurity vulnerabilities, and the lack of skilled personnel in AI and machine learning.
How do you view the ethical implications of using autonomous weapons in conflict?	Ethical concerns center around accountability, proportionality, and the risk of autonomous weapons making lethal decisions without oversight.
What is your perspective on AI’s impact on national security policies?	AI is seen as a transformative tool in improving national security strategies, particularly in threat prediction, surveillance, and cybersecurity.
How can AI assist in counterterrorism and intelligence gathering?	AI aids in processing vast data, improving surveillance, identifying terrorist activity patterns, and providing actionable intelligence.
What infrastructure or technology improvements are necessary for AI adoption in Pakistan’s defense?	Pakistan needs robust data infrastructure, AI research facilities, secure networks, and trained personnel for successful AI integration.
What role do you foresee for AI in cybersecurity and defense?	AI will automate threat detection, strengthen defense systems, and provide rapid response to cyber attacks, ensuring national security.
How do you evaluate the collaboration between human soldiers and AI on the battlefield?	Human-AI collaboration enhances decision-making, improves situational awareness, and helps reduce human errors, with human oversight being essential.

Nevertheless, ethical issues also formed the discussions, especially accountability and using autonomous weapons. Also, the issues of infrastructure, cybersecurity, and lack of qualified labour were identified. The mixed reactions point towards the necessity of a balanced practice akin to integrating the benefits of AI and reasonable control and moral principles.

The detailed responses are as follows:

(1) What role do you see AI playing in Pakistan's defence strategy?

According to Professor A (Interview conducted in 2025), AI will be a game-changer in the Pakistan defence. It will enhance our surveillance mechanism, enabling more effective monitoring of borders and sensitive regions without the need for human fatigue. Faster decision-making will also be made possible by AI, which will enable us to make a move before a matter gets out of control. As noted by Colonel B (Interview conducted in 2025), artificial intelligence is perceived as something that will improve the experience on battlefields. It will assist us in processing large quantities of information more quickly than any human being could. That is important when you are in a fighting arena where time runs fast. When used correctly, it can revolutionise our tactical response. Consultant C (Interview conducted in 2025) explained that AI helps in optimising logistics and using little or no human involvement in doing routine work. It will put us in a position to manage resources and human resources better. Moreover, from a strategic perspective, the faster we can process and react to the data we have, the better we are with our defence strategy. Officer H (Interview conducted in 2025) highlighted that AI is essential in limiting the loss of human lives. We can reduce the risks to our forces by using AI to project threats and carry precision strikes. That will be an additional pair of eyes in the sky. Analyst F (Interview conducted in 2025) pointed out that AI is going to increase situational awareness. It is gigantic to be able to foresee the threats even before they do happen. It is not just about reacting but also about being a step ahead.

(2) What ethical concerns do you associate with AI in warfare?

The view was shared by Major D (Interview conducted in 2025) that the greatest fear is responsibility. In the event of an AI system making an erroneous decision during the battle, who will be the culprit of the decision? How (are we) going to create global accountability when the developers or the military might be held culpable when an autonomous weapon makes an unintended action? Professor A (Interview conducted in 2025) highlighted that the AI decision is a transparently evident problem. These algorithms may be something that we do not entirely comprehend, and these systems are running on it. What happens when anything goes wrong, such as causing harm to civilians; how are we going to justify that to the rest of the world? It is not only a technological matter, but it is a matter of morality as well. Colonel B (Interview conducted in 2025) pointed out that there is also the chance of turning the decision-making abilities of the machines into an autonomous level without involving humans. These AI systems lack compassion and awareness of the situation, as would be the case with a human soldier. They may fail to distinguish between a legal target and a civilian, which is a particularly concerning consideration. As noted by Consultant C (Interview conducted in

2025), the ethical issues of AI during warfare are related to autonomy. The machines will be making decisions without human involvement. How can we ensure they comply with international laws and other ethical standards? When asked about the ethical concerns of using AI, Researcher E (Interview conducted in 2025) argued that the main problem is the unpredictability of AI. These systems can make decisions within a fraction of a second, but can we depend on them to make morally correct decisions?

(3) What are the main benefits and opportunities you associate with AI in warfare?

As noted by Officer H (Interview conducted in 2025), precision is the greatest advantage. Artificial intelligence can read information and identify targets without similar precision speedily. Those translate to fewer lives being lost and less collateral damage. It is also capable of optimising our resources by ensuring that we use our assets where our needs are most significant. Major D (Interview conducted in 2025) highlighted that the immense advantage of using AI in warfare is its speed. They will enable us to make faster decisions because AI can analyze the battlefield's state at any moment. In cases where time is of the essence, AI can provide accurate information in a fraction of a second. Brigadier I (Interview conducted in 2025) suggested that the predictive capabilities of AI usage in warfare should not be forgotten. We can prevent the occurrence of threats by leveraging the analysis capabilities of AI. This puts us in a superior position in stopping the conflict instead of responding to it. Insights from Professor A (Interview conducted in 2025) indicate that AI's potential in counterintelligence is enormous. It helps predict attacks by analyzing patterns and trends, allowing it to prevent attacks before they occur. Analyst F (Interview conducted in 2025) stated that AI provides a possibility to foresee dangers. Given that AI can crunch data, we can begin detecting trends that indicate a scheduled event of attack or movement. Having such a predictive ability would put us at an immense advantage in terms of preventing conflicts from escalating.

(4) What challenges or risks do you foresee with integrating AI into military operations?

Analyst F (Interview conducted in 2025) explained that it involves one of the most significant challenges, which includes a shortage of skilled human resources. Technologically, we can do it, yet we lack the expertise to deal with such AI systems. It has a significant training deficit, which might limit the successful adoption of AI in military practice. Researcher E (Interview conducted in 2025) highlighted that the main issue is cybersecurity. AI systems are not simple and not appropriately secured; it may be a matter of hacking or manipulating in case it is not secured. Consider a scenario where enemy hackers compromise our AI systems. It runs a giant security risk to the country. Professor A (Interview conducted in 2025) stated that dependency is a significant issue that should not be overlooked. As we become increasingly dependent on AI, our ability to make decisions independently will diminish. In the worst-case scenario, if the AI breaks or experiences glitches during critical events, we would be searching for solutions in vain. Consultant C (Interview conducted in 2025) pointed out that the infrastructure needed to support AI is also a significant problem. High bandwidth and safe systems are necessary to run the operations of AI, which would require significant investments in both technology and training. Major D (Interview conducted in 2025) explained that when AI systems

go wrong in the wrong instant, we are in trouble. Reserve systems should be in place, and humans should be able to take over when necessary.

(5) How do you view the ethical implications of using autonomous weapons in conflict?

Colonel B (Interview conducted in 2025) argued that autonomous weapons might work relatively quickly and perform their tasks more effectively than human soldiers, yet they are not as morally sound as us. In case these weapons make a false call, we might break international law or might just kill civilians. It turns out to be a huge moral question. Policy Expert J (Interview conducted in 2025) stated that robot killing machines may travel beyond international law and make decisions on which lives to take and which lives to spare. Who took those actions? Will machines be able to play by the rules of engagement? Analyst F (Interview conducted in 2025) opines that the use of technology is very advanced, but the possibility of machines making life-or-death decisions does not augur well. These systems are in control of who? How do we ensure that they are held accountable when things are going haywire in times of warfare? Brigadier I (Interview conducted in 2025) expresses concern about the possibility of errors. AI may direct itself to the wrong individuals or escalate conflicts when it is not supposed to do so. It is a profound problem that should be thought more deeply prior to its implementation. Lieutenant G (Interview conducted in 2025) believes that we should reevaluate the morality of using autonomous systems. These technologies are developing at a rapid pace, but they cast doubts about the involvement of human judgment during war. Are we ready to lose it?

(6) What is your perspective on AI's impact on national security policies?

Researcher E (Interview conducted in 2025) supported the claim that AI is not only transforming the way we think about national security. As we can study huge quantities of data in real time, it is now possible to develop predictive models, which may fundamentally alter how we predict and act upon security threats. It is not only reacting to the events but also preventing it. Colonel B (Interview conducted in 2025) explained that AI, in military terms, will allow us to have more control over the operations, including troops' movements and cyber safety. It will undoubtedly transform the drafting of security policies, making them more agile and data-driven, which is crucial in today's rapidly evolving security landscape. Policy Expert J (Interview conducted in 2025) emphasised that AI will move national security policies towards a more strategic, technology-oriented direction. Nevertheless, we should possess the appropriate implementation strategies so that AI can be used with a reasonable approach. We will also require global cooperation to establish the guidelines for its application in defence. Major D (Interview conducted in 2025) emphasised the need to enhance security policies by leveraging AI more efficiently. We will even be able to predict the threat even before it becomes a concern. We need to be cautious of the information we use; however, it must be valid and dependable. Professor A (Interview conducted in 2025) believes that it will make national security policies more data-focused, but we also have to offer balance on that with the human factor. AI can offer information on the same, but human judgment is still required to steer such information to the borders of national security.

(7) How can AI assist in counterterrorism and intelligence gathering?

Major D (Interview conducted in 2025) highlighted that AI will free up time to analyze communications, emails, and other data by automating tasks, enabling us to detect terrorist cells or plots that we otherwise would have been unable to detect. It is above any human ability to process information in a faster manner, thus giving us intelligence on how to act in real time. Brigadier I (Interview conducted in 2025) explained that it is possible to follow movements and patterns that we could not follow before as far as AI is concerned. It may assist us in predicting the cells that terrorist groups may use in their next operation, thereby simplifying their arrest ahead of the execution of their plans. Policy Expert J (Interview conducted in 2025) shared their view that AI can also be used to analyze big data-satellite systems, social media, or financial transactions. It can detect suspicious persons or activities that engage in illegal activities, enabling security agencies to recognise the threat more effectively. Lieutenant G (Interview conducted in 2025) stated that AI will enhance our situational awareness. It can scan and scan through enormous data networks in real-time and provides us with means of figuring out potential terrorist acts that would otherwise remain unnoticed. Researcher E (Interview conducted in 2025) emphasised that AI will play an important role in detecting possible threats at early stages. The more effectively we process the data, the more we can anticipate terrorist activity, allowing us to act proactively before it escalates.

(8) What infrastructure or technology improvements are necessary for AI adoption in Pakistan's defence?

Colonel C (Interview conducted in 2025) argued that we should concentrate on the creation of secure networks and strong AI infrastructure. It involves purchasing data centres, ensuring fast and high-quality communication, and implementing cloud computing solutions to process AI-generated data efficiently. Researcher E (Interview conducted in 2025) emphasised that we must also develop training programs to empower our defence personnel with the necessary skills to manage and utilise AI systems effectively. In the absence of competent professionals, we cannot make the most out of these technologies. Policy Expert J (Interview conducted in 2025) shared their view that besides infrastructure and training, we should have unambiguous policies on the ethical use of AI in defence, too. Such policies are expected to govern the application of AI technologies, such as autonomous systems, to ensure their proper usage and compliance with international law. Brigadier I (Interview conducted in 2025) pointed out that we shall be required to consider investing in human capital to facilitate AI. It implies not only training the army staff but also developing educational centres that would focus on AI-related industries and defence-related technologies. Major D (Interview conducted in 2025) believed that the most important thing is securing these AI systems. Regarding the dangers of AI, we should have systems capable of withstanding cyberattacks and ensuring the safety of our sensitive information at no cost.

(9) What role do you foresee for AI in cybersecurity and defence?

Analyst F (Interview conducted in 2025) explained the critical role of AI in cybersecurity. It can automate the identification of anomalies in our networks, and it can respond to

cyber-attacks in real time. Such speed and efficiency are critical in the protection and guarding of vital infrastructure. Professor A (Interview conducted in 2025) emphasised the role of artificial intelligence in detecting loopholes before the enemy can exploit them. Using its forecasting abilities, AI can predict possible cyber-attacks and eliminate them even before they become attacks on their full scale. Lieutenant G (Interview conducted in 2025) argued that as far as defence is concerned, AI can protect communication networks, military systems and any other critical infrastructure by performing automatic threat analysis and responding more quickly to security threats. Its possibilities are enormous in the proactive defence. Colonel C (Interview conducted in 2025) stated that AI would support real-time defence in the cyber. It will process data in real time, enabling us to identify and respond to threats promptly. It is this proactive defence mechanism that we should have in order to remain secure. Consultant C (Interview conducted in 2025) emphasised that AI will be of great help in detecting and responding to cyber-attacks. It can analyze large quantities of data in a split second and spot any anomalies thereafter, taking a corresponding course of action to stop or deal with the threat.

(10) How do you evaluate the collaboration between human soldiers and AI on the battlefield?

Colonel B (Interview conducted in 2025) believed that human-AI partnership is critical. AI will perform the repetitive data-heavy work, yet the soldiers will make the final decisions. The factor of human judgment cannot be left out, particularly in cases that necessitate empathy or complicated analysis. Brigadier I (Interview conducted in 2025) stated that AI will contribute to improving human decision-making by creating real-time insights and predictions. The important point is that man is still in control, particularly with life-and-death decisions on the battlefield. Professor A (Interview conducted in 2025) explained that AI will serve as a complement to augment situational awareness and quicker decision-making. Nevertheless, human soldiers must be under the constant supervision of AI to guarantee that humanity and the laws of the army can be respected in the course of combat. Policymaker J (Interview conducted in 2025) noted that AI will supplement, but its effectiveness depends on providing soldiers with information more quickly. However, there will be instances where human presence is necessary. It is all about balance between capitalising on the strength of AI and keeping the human eye in the loop. Researcher E (Interview conducted in 2025) concluded that it is a subject of teamwork. AI will provide soldiers with tools to make faster and better decisions.

Table 3. Initial codes extracted from interview data.

Statement extract	Initial code
AI helps predict threats faster than humans.	Predictive Capability
Unregulated AI could act without oversight.	Autonomy Risk
AI systems can make decisions based on data analysis.	Data-Driven Decisions
Lack of infrastructure to support AI systems.	Infrastructure Gap
AI in military operations can reduce human casualties.	Humanitarian Benefit
Over-reliance on AI leads to potential system failures.	AI Dependency Risks
AI-enhanced surveillance can enhance border security.	Security Enhancement
Autonomous weapons can make lethal decisions without human oversight.	Ethical Dilemmas in Warfare
Lack of skilled personnel in AI and machine learning.	Skill Gap
AI can enhance national security by predicting and detecting cyber threats.	Cybersecurity Advancement

However, it is important that human beings remain under command, particularly those decisions where there is life and death involved.

Table 3 illustrates the preliminary codes based on the interview material with the most crucial concerns and findings expressed by the respondents. The codes take into consideration the different aspects of the national defence adoption of AI, including the power of prediction, the risk of autonomy, and the humanitarian role of AI, specifically regarding casualties. Moreover, the table also shows the concerns of infrastructure gaps, AI dependency risks, and the ethical issue of autonomous weapons. These starting codes serve as the foundation for further thematic analysis, aiding in the structuring of the oldest issues related to the AI application within Pakistan's national security strategy.

Table 4 offers a classification of the emerged themes and the sub-themes with the interview information. The significant themes are strategic utility, ethics, technology, and geopolitical effects. The major issues are then expanded by sub-themes like threat prediction, cybersecurity, human capital development, and the necessity of it, which constitute some of the main areas of concern and possibilities of using AI in the defence world. These themes can be identified, which makes it possible to perceive the multidimensional nature of the process of AI integration in terms of various risks to its operation, ethical liability, and the surrounding region, in this case, South Asia. The above thematic classification has been used in screening strategic implications in the defence policies of Pakistan.

Table 5 provides a summary of the thematic findings and their strategic implication on the Pakistan defence strategy. The results indicate that AI would enhance the speed of decision-making, accuracy in targeting, and the ability to counter terrorism attacks. According to it, however, the absence of AI warfare policies and excessive dependence on AI can be perilous, such as the failure of systems and the ethics of autonomous weapons. The table highlights the evidence that Pakistan must create control systems to tackle these risks, invest in the infrastructure of AI, and fill the gap in AI know-how. Moreover, it outlines the geopolitical importance of AI, particularly the aspects of regional security patterns and the South Asian arms race, where Pakistan should concentrate on the creation of indigenous AI support so that national security can be addressed.

A thematic analysis of expert interviews identified five main themes of Pakistan's military sector's AI integration, i.e. strategic modernisation, operational efficiency, ethical governance, institutional preparation, and technology reliance. Participants emphasised that AI is a strategic imperative to modernise Pakistan's military. Strategic modernisation experts stressed AI's capacity to boost intelligence and counterterrorism operations'

Table 4. Emergent themes and sub-themes.

Theme	Sub-Themes
Strategic Utility	Threat prediction, Cybersecurity, Efficiency
Ethical Concerns	Civilian protection, Moral responsibility
Technological Challenges	Technological dependency, Lack of digitisation
Human Capital Constraints	Skill gap, Limited AI education in military sector
Geopolitical Impact	Arms Race, AI and Regional Stability, Power Dynamics in South Asia
Operational Risks	System Failures, Over-reliance on AI, Autonomous Decision-making Issues
Security Enhancements	Surveillance, Border Security, Intelligence Gathering, Counterterrorism
AI in Cyber Warfare	Threat Detection, Cyber Defense, Real-time Responses, Data Integrity
AI in Military Strategy	Autonomous Weapons, Precision Strikes, Human-AI Collaboration
Policy & Regulation	AI Governance, Ethical Frameworks, International Collaboration in AI Use

Table 5. Thematic findings and strategic implications for Pakistan.

Thematic finding	Strategic implication for Pakistan's defense
AI enhances decision-making speed	Investment in AI-based command & control systems to optimise decision-making processes
Lack of policy on AI warfare	Development of regulatory and ethical AI frameworks to guide AI integration
Over-reliance on AI may result in system failures	Balancing human oversight and AI implementation to avoid dependency risks
Cybersecurity risks due to AI vulnerabilities	Strengthening cybersecurity systems with AI-based real-time threat detection
Ethical concerns in autonomous weapons systems	Formulation of ethical guidelines and accountability protocols for autonomous systems
AI improves military precision and targeting	Adoption of AI-powered autonomous weaponry for precision strikes and minimising collateral damage
AI's role in counterterrorism	Enhancement of surveillance and intelligence gathering systems for counterterrorism
AI-driven surveillance for border security	Deployment of AI technologies to improve border security through predictive analytics
Need for AI infrastructure and skilled personnel	Investment in AI education and the establishment of research and development centers
Regional AI arms race (South Asia focus)	Development of indigenous AI capabilities to ensure national security and sovereignty

decision-making, border management, and monitoring. Operational efficiency showed how AI affects tactical settings via real-time threat assessment, resource management, and human mistake removal. Data privacy, accountability in AI-based decision frameworks, and autonomous system morality have been raised by ethical governance. Respondents wanted legislation and ethical oversight to ensure transparency and global norms. Institutional preparedness underlined the need for new institutions like Centre for Artificial Intelligence and Computing and National Aerospace Science and Technology Park in AI-powered military research. However, agency cooperation is still lacking for long-term innovation. Finally, technological dependence raises concerns about Pakistan's overreliance on foreign artificial intelligence systems and the need to invest in domestic research, cybersecurity, and talent development.

Discussion and analysis

Pakistan is moving closer to incorporating AI into its military architecture as several new groups attempt to align national security goals with technological capabilities. The Pakistan Air Force's Directorate of Research and Development's Centre for Artificial Intelligence and Computing (CENTAIC) represents a major shift (Babar and Sarwar 2025). The CENTAIC strategic institutional program to apply AI seeks data-driven operations, predictive maintenance, automated surveillance, and enhanced military decision-making (Khalid 2025). Its research on autonomous drones, threat pattern analysis, and AI-assisted battle simulations points to a new age of digital warfare. In a similar spirit, the Pakistan Air Force, in conjunction with universities and industries, built the National Aerospace Science and Technology Park (NASTP) to stimulate innovation in the domains of aerospace, AI, cybersecurity, and satellite communication technologies (Awan 2025). NASTP promotes indigenous capabilities and technological sovereignty by creating a military-industrial ecosystem between local R&D institutions, start-ups, and defense manufacturers. Institutional support from the National Centre of Artificial Intelligence (NCAl)

and Pakistan Centre for Advanced Studies in Emerging Technologies (PCASE) enhances human capital development and applied AI research (Khan, Siddiqui, and Farooq 2024b). These platforms suggest that Pakistan is ready to deploy AI, going beyond talking about it and into implementing it, but financial stability, agency coordination, and data security remain major challenges. The creation of CENTAIC and NASTP signals a change in policy toward systemic innovation, where artificial intelligence is now crucial to national security plans. Experts advise Pakistan to invest in long-term AI ecosystems, personnel retention initiatives, and ethical governance frameworks to align technology adoption with strategic autonomy and operational goals. Pakistan's AI readiness is a big step toward modernisation, but it also emphasises the necessity for a strategic vision and institutional consistency in military institutions for the future.

This study uncovers several significant findings regarding the integration of AI into Pakistan's defense and national security strategy. Roy (2024) argued that AI has a significant role in enhancing the rate of decision-making in military events. Command and control systems can be improved by the capability to process large volumes of data as quickly and precisely as possible. This makes decisions more informed and timely, which is highly crucial in the military setting. Thus, Pakistan should invest in command and control systems that operate on AI to maximise efficiency. As of now, Pakistan does not have any extensive policy regarding the use of AI on the battlefield. To address this gap, regulatory and ethical AI frameworks need to be developed, which would help integrate AI into defence systems (Ndzendze and Marwala 2023). Such frameworks would address international laws and ethical principles to assure that the AI systems adhere to any international law and are used responsibly. Although AI has the power to streamline military operations, excessive dependence on the technologies might lead to systems failure or malfunction. A balance between the implementation of AI and human control should be considered to avoid possible threats of AI dependency. Instead, human judgment should be placed at the centre stage when it comes to making critical decisions (Cummings et al. 2018). AI creates new vulnerabilities to cybersecurity. Nevertheless, it can also provide an effective means of enhancing national security. Real-time AI-based threat detection can serve as a strong cyber attack defence mechanism against cyber attacks focused on critical infrastructure. The application of autonomous weapons presents serious ethical questions, specifically the issues of responsibility and unintended consequences (Horowitz et al. 2022). Pakistan needs to formulate ethical guidelines and accountability procedures regarding the use of autonomous systems, and these systems must also comply with international humanitarian law. AI enhances targeting and can be deployed to more successful counterterrorist operations. Surveillance systems using AI will enhance intelligence collection and border control by gaining proactive, predictive insights to deter threats (Jensen, Whyte, and Cuomo 2020). Pakistan should invest in AI education and research and development centres in order to facilitate AI integration. Moreover, building any of the Indigenous AI capabilities is imperative for national security and sovereignty amid the regional arms race.

According to the expert perspective, Pakistan's institutional structure, regional risk environment, and technological capabilities greatly determine how AI will affect its security and military sectors. Pakistan should build AI capabilities while reforming outmoded military systems, unlike technologically advanced countries that have integrated AI into

their digital defense infrastructures. Experts say Pakistan's military operations struggle with AI. Lack of a unified AI governance framework, unequal inter-agency collaboration, and limited high-quality data are these issues. Due to these constraints, AI deployment has been limited to tiny pilot projects and intelligence analysis and terrorist monitoring. Participants said Pakistan requires context-specific AI solutions to address security concerns, including counterterrorism, border surveillance, and internal security stability. Contrary to Western AI systems, which rely on traditional fighting, Pakistan is increasingly using AI for predictive analytics to prevent terrorist attacks, facial recognition in urban security networks, and real-time monitoring of high-risk border regions. AI integration into command and control systems improves situational awareness for the Pakistan Army and intelligence agencies. However, analysts stress that these advancements occur in a low-resource environment where imported technology and a lack of native hardware production put data sovereignty and cybersecurity at risk. Ethical and policy challenges divide Pakistan's AI trajectory from that of developed nations. The absence of a national military AI policy has been replaced by ad hoc decision-making motivated by security rather than governance. The National Centre of Artificial Intelligence (NCAI) and other organisations have increased their focus on digital defense plans, but respondents are still concerned about talent retention, research and development infrastructure, and inter-ministerial cooperation. Using foreign cooperation for AI-powered military solutions raises worries about technological reliance and strategic autonomy. Pakistan needs cost-effective AI models customised to its geography, security dynamics, and operational needs. The findings demonstrate that Pakistan's AI-enabled military modernisation faces several potential challenges. AI improves intelligence accuracy, resource management, and situational awareness, but regional policy changes, domestic R&D funding, and ethical standards tailored to Pakistan's geopolitical situation are needed to maximise its potential. Pakistan's military's AI is an adaptation to its unique strategic, institutional, and developmental terrain, reflecting the intricacies of these local circumstances.

Policy recommendations

Study findings and expert comments recommend many policy changes to improve Pakistan's preparedness and responsible use of AI in national security. First, create a comprehensive National Defense AI Policy Framework detailing the boundaries, duties, and norms of military AI use. This system should clearly identify AI decision-makers, control autonomous weapon systems, and ensure the military complies with international tech norms. Second, CENTAIC, NASTP, and NCAI should improve institutional coordination to improve information exchange, research objectives, and cross-sectoral cooperation. A centralised military innovation council may oversee these efforts to guarantee national security and resource distribution. Thirdly, Pakistan must fund AI research and military data infrastructure. Secure data repositories, military AI laboratories, and public-private partnerships may reduce dependency on foreign technologies and promote technological sovereignty. Transparent performance measurements and targeted funding should support these efforts. Fourth, human capital and competence development are still important. The military should train in algorithmic warfare, cybersecurity, and AI ethics to promote responsible innovation and technical capability. Finally, international cooperation, notably confidence-building and regional partnerships, is essential to

prevent AI-based weapons escalation in South Asia. Pakistan's AI military strategy must balance modernisation, sovereignty, autonomy, accountability, ethics, and inventiveness. These laws will convert AI into a national security asset instead of a technological threat. Pakistan's military and security industry's AI discussion follows national policy aims and practical implications revealed by experts. AI adoption is a key strategic aim to increase operational efficiency, resource management, and predictive intelligence. The findings demonstrate that AI improves military situational awareness, decision-making accuracy, and surveillance. Participants' concerns about ethical use, institutional preparation, and regulatory limitations align with wider policy considerations. This relationship between theoretical reasoning and real findings underscores AI integration's complexity, which offers military advantages but also challenges responsible deployment and control.

Future research directions

The future research directions require research subjects to enlighten policymakers in Pakistan on achieving responsible integration of AI into its military. Research into the ethical requirements of AI in military conflicts, particularly autonomous weapons systems, is warranted. It also means generating structures to address responsibility, openness, and even the ethical implications of AI-enhanced decision-making during war. Moreover, a pivot toward formulating regulatory frameworks to balance security concerns and the ethical application of AI technologies in terms of defence should also be regarded. It is also possible to conduct a study to determine how to find a compromise between the benefits of AI and the fears associated with excessive technology use and its associated threats, including system malfunctions and issues with autonomous decisions. Lastly, intersectoral collaboration among the domains of technology, defence, and policy is a requirement. The results of these studies should inform future research on how these sectors can collaborate to develop mechanisms that mitigate the risks associated with AI and enhance their capacity to protect and remain secure.

Conclusions

AI in warfare, as well as national security, is not only an innovation in the field of military technology but also a strategic prerequisite within the new global security landscape. The need to address the strategic, ethical, and operational roles of AI within Pakistan's defence and national security strategies underscores the transformative impact of AI on enhancing military efficiency, precision, and decision-making speed. Nevertheless, it also presents considerable issues and dilemmas that should be overcome on their way to safe national defence with the help of AI. First, AI can transform how Pakistan handles its defence approach. Its ability to process real-time data, predict threats in advance, and optimise resources significantly improves its effectiveness in war management, border regulation, intelligence, and cyber security. The use of AI in surveillance would get the military to track threats in a highly efficient and effective way. Additionally, autonomous weapons systems armed with AI have the potential to make combat much more accurate, minimising collateral damage and reducing the number of people killed. Such developments also turn AI into an essential tool to modernise the Pakistani military infrastructure and enhance its operational efficiency. Nonetheless, regardless of all the advantages, the

utilisation of AI in warfare omits serious ethical and strategic questions. Accountability of the systems driven by AI, and in particular autonomous weapons, is one of the most urgent questions. Whenever the AI system makes decisions that result in loss of life, nobody is sure who is to be held liable for their acts, be it the creators of the software, the soldiers or the AI system. Such accountability would be a challenge to legal and ethical structures, particularly when AI systems break international laws or cause unexpected harm, e.g. civilian deaths. Also, the issue of transparency in AI decision-making processes is huge. The sophistication of AI code and their black box decision frameworks may result in a time when actions by AI have not been fully comprehended. As such, it becomes challenging to determine whether their actions have the attributes of fairness and legality.

The second essential problem is the danger of over-dependence on AI in military operations. Although AI can make military operations many times more efficient, the concerns related to the over-reliance on technology make military operations susceptible to AI system failure or cyberattacks. The use of AI in the military might also present a target to their enemies, who might attempt to use the weaknesses of the AI in their favour. Therefore, the balance between human control and AI autonomy is fundamental to reducing the challenges posed by the eventuality of over-dependence on automated technologies. The human factor remains essential in cases where moral judgment is required, situational awareness is crucial, and decisions must be made in complex situations that AI may not fully capture. Moreover, the moral impact of autonomous weapons systems and the possible role of AI in warfare would put into question the future of war. Although AI's potential to enhance military performance and reduce human injuries is appealing, it also raises concerns about compromising the humanity of war by removing human control over life-ending incidents. Autonomous weapons, lacking a human controller, may not make decisions with the empathy and judgment that humans bring to complex military situations. The fact AI can be used to increase conflicts or be misapplied in a manner that endangers international humanitarian law is a significant concern that cannot be ignored. Concerning national security, AI can be used to revolutionise the national defence measures in Pakistan. The real-time capability of predicting and analyzing the threat to security gives Pakistan a chance to transition into the proactive rather than the reactive approach to national security. The predictive nature of AI will enable security forces to anticipate and respond to potential risks before they occur, thereby enhancing Pakistan's security in a complex and volatile environment. Nevertheless, the integration of AI in the defence and national security infrastructure of the country of Pakistan requires substantial investments in AI infrastructure, research and training. A shortage of personnel skilled in AI and machine learning is one of the most significant obstacles to the successful implementation of these technologies. As such, investment into education and training programs that will create AI expertise in the military and national security fields in Pakistan must be funded.

Furthermore, the primary approach to the implementation of AI in Pakistan's national security policies will be the creation of practical ethical standards and regulation systems. Policymakers must ensure that responsible and controlled humanity uses AI technologies without abuse and possible harm. International cooperation and the creation of international norms and standards of ethical application of AI in defence and national security are also required. Pakistan is to collaborate with other countries to develop systems that

would regulate the creation and application of AI technology in war so that AI technology does not engender instability in world security. The study also notes that AI should be used as an element in an army instead of a soldier replacement. Although AI is capable of doing routine work and offering worthwhile information based on data, human soldiers will maintain their role in decision-making under severe circumstances. The integration of AI and human beings is likely to lead to more efficient and effective military operations. Nevertheless, human judgment should never be sidelined when it comes to making crucial decisions, particularly where there are complicated and ethically involved military scenarios. The application of AI in Pakistan's defence and national security planning presents opportunities and poses significant challenges. The technology has great benefits regarding efficiency, precision, and speed, and its ethical, legal, and operational outcomes should be well addressed. To successfully integrate AI into military practices and national security strategies, Pakistan will have to address accountability concerns, ensure transparency, and maintain human control, accompanied by investments in infrastructure and human resources. In a world where AI is ever-changing, Pakistan must pursue a balanced, ethical, and strategic integration of AI that can both enhance national security and mitigate potential risks. Clearing up the uncertainties and establishing relationships between countries worldwide will play a significant role in ensuring that AI as global security becomes a source of good instead of multiplying the numerous threats or stoking the current tensions.

Authors' contributions

Shahbaz Ahmed Shahzad: Conceptualization, Data Curation, Investigation, Methodology, Formal Analysis, Resources, Validation, Writing-Reviewing and Editing. **Muhammad Khalid Anser:** Methodology, Formal Analysis, Project Administration, Data Curation, Writing-Reviewing and Editing. **Ihtisham ul Haq:** Methodology, Formal Analysis, Investigation, Data Curation, Validation, Writing-Reviewing and Editing. **Alamzeb Aamir:** Methodology, Formal Analysis, Investigation, Data Curation, Validation, Writing-Reviewing and Editing. **Khalid Zaman:** Supervision, Conceptualization, Methodology, Formal Analysis, Resources, Writing-Reviewing and Editing.

Ethics approval and consent to participate

This study was approved by the Ethics Committee of the Department of Research, The Sherwan Institute of Online Education (No. SIOE1299/2025), and relevant survey procedures were in line with the requirements of the Declaration of Helsinki. Written informed consent for participation in this study was provided by the participants.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Availability of data and material

The data supporting the findings of this study were collected through open-ended qualitative responses from participants. These responses are quoted selectively within the

article to illustrate key themes and are not available in full to protect participant confidentiality. Further details may be available from the corresponding author upon reasonable request and with appropriate ethical considerations.

ORCID

Shahbaz Ahmed Shahzad  <http://orcid.org/0009-0000-4290-3011>

Muhammad Khalid Anser  <http://orcid.org/0000-0003-1882-0907>

Ihtisham Ul Haq  <http://orcid.org/0000-0002-3999-9873>

Alamzeb Aamir  <http://orcid.org/0000-0002-5623-2519>

Khalid Zaman  <http://orcid.org/0000-0002-2585-2790>

References

- Ahmad, J. B., M. A. Hussain, and H. A. Mir. 2024. "Developing a Legal Framework for Digital Policy: A Roadmap for AI Regulations in Pakistan." *Law and Policy Review* 3 (1): 162–188.
- Akhtar, R., and M. Sethi. 2024. "Emerging Technologies and Southern Asian Nuclear Deterrence." *The Washington Quarterly* 47 (4): 99–116. <https://doi.org/10.1080/0163660X.2024.2435161>.
- Al-Dulaimi, A. O. M., and M. A. A. W. Mohammed. 2025. "Legal Responsibility for Errors Caused by Artificial Intelligence (AI) in the Public Sector." *International Journal of Law and Management*. <https://doi.org/10.1108/IJLMA-08-2024-0295>.
- Ali, A. A., and A. T. Cheema. 2025. "India's Technological Ascendancy: Implications for Pakistan's Security." *Journal of Development and Social Sciences* 6 (1): 650–660.
- Amir, S., and N. A. Rehman. 2024. "Space Technology and Its Military Application: Options for Pakistan." *Journal of Advanced Military Studies* 15 (1): 136–152. <https://doi.org/10.21140/mcu.20231501008>.
- Awan, S. H. 2025. "Weaponisation of Social Media: A Threat to Pakistan's National Security." *NDU Journal* 39 (XXXIV): 34–47. <https://doi.org/10.54690/ndujournal.39.228>.
- Azam, A., M. U. Khattak, and Q. ul Ain. 2025. "A Comprehensive Assessment of Pakistan's National Internal Security Policy Framework." *Global Change, Peace & Security* 36 (1): 21–42. <https://doi.org/10.1080/14781158.2025.2474242>.
- Braun, V., and V. Clarke. 2006. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3 (2): 77–101.
- Babar, S. I., and M. Sarwar. 2025. "AI-Militarization in South Asia: A Comparative Analysis." *BTTN Journal* 4 (1): 1–19. <https://doi.org/10.61732/bj.v4i1.181>.
- Bächle, T. C., and J. Bareis. 2022. "'Autonomous Weapons' as a Geopolitical Signifier in a National Power Play: Analysing AI Imaginaries in Chinese and US Military Policies." *European Journal of Futures Research* 10 (1): 20. <https://doi.org/10.1186/s40309-022-00202-w>.
- Baele, S. J., and D. Jalea. 2023. "Twenty-five Years of Securitization Theory: A Corpus-based Review." *Political Studies Review* 21 (2): 376–389. <https://doi.org/10.1177/14789299211069499>.
- Budacu, D. 2024. "The Impact of the Artificial Intelligence on Hybrid Conflicts in the 21st Century." *Studia Securitatis* 18 (2): 87–108.
- Buzan, B., and O. Wæver. 2009. "Macrosecritisation and Security Constellations: Reconsidering Scale in Securitisation Theory." *Review of International Studies* 35 (2): 253–276. <https://doi.org/10.1017/S0260210509008511>.
- Capodivacca, S., and G. Giacomini. 2024. "Discipline and Power in the Digital Age: Critical Reflections from Foucault's Thought." *Foucault Studies* 36 (1): 227–251. <https://doi.org/10.22439/fs.i36.7215>.
- Chapman, B. 2020. "How US Government Policy Documents Are Addressing the Increasing National Security Implications of Artificial Intelligence." *Journal of Advanced Military Studies* 11 (1): 209–232.
- Char, J., ed. 2024. *Modernising the People's Liberation Army: Aspiring to Be a Global Military Power*. London: Routledge. <https://doi.org/10.4324/9781003307365>.

- Cummings, M. L., H. M. Roff, K. Cukier, J. Parakilas, and H. Bryce. 2018. "Artificial Intelligence and International Affairs." *Chatham House Report*, 7–18, London.
- Darıcı, A. B., and N. El-Bayaa. 2024. "Using Artificial Intelligence in the Field of Intelligence Operations and Analysis." In *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, edited by M. E. Erendor, 43–57. Boca Raton, FL: CRC Press.
- Davis, P. K., and P. Bracken. 2025. "Artificial Intelligence for Wargaming and Modeling." *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 22 (1): 25–40. <https://doi.org/10.1177/15485129211073126>.
- Dehalwar, K. S. S. N., and S. N. Sharma. 2024. "Exploring the Distinctions between Quantitative and Qualitative Research Methods." *Think India Journal* 27 (1): 7–15.
- Devvari, A., A. Kumar, and P. Kuchhal. 2024. "Global Aspects and Overview of 5G Multimedia Communication." *Multimedia Tools and Applications* 83 (9): 26439–26484. <https://doi.org/10.1007/s11042-023-16549-6>.
- Eden, C. A., O. N. Chisom, and I. S. Adeniyi. 2024. "Integrating AI in Education: Opportunities, Challenges, and Ethical Considerations." *Magna Scientia Advanced Research and Reviews* 10 (2): 006–013. <https://doi.org/10.30574/msarr.2024.10.2.0039>.
- Ettlinger, N. 2022. *Digitalized Dilemmas of Automated Governance and Communitarian Practice*. 1st ed. London: Routledge. <https://doi.org/10.4324/9781003109792>.
- Feroz, E. S., A. Q. Laghari, B. Ahmad, M. T. U. Hassan, M. Rafique, and M. Kamran. 2025. "Unlocking the Potential of Artificial Intelligence and Blockchain: A Pathway to Secure, Efficient, and Intelligent Smart Grids in Pakistan's Energy Sector." *Dialogue Social Science Review (DSSR)* 3 (3): 492–515.
- Galar, D., U. Kumar, and D. Seneviratne. 2020. *Robots, Drones, UAVs and UGVs for Operation and Maintenance*. 1st ed. Boca Raton, FL: CRC Press. <https://doi.org/10.1201/9780429452260>.
- Garcia, E. V. 2024. "The Technological Leap of AI and the Global South: Deepening Asymmetries and the Future of International Security." In *Research Handbook on Warfare and Artificial Intelligence*, edited by R. Geiß and H. Lahmann, 370–387. Cheltenham: Edward Elgar Publishing.
- Govea, J., W. Gaibor-Naranjo, and W. Villegas-Ch. 2024. "Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence." *Systems* 12 (5): 165. <https://doi.org/10.3390/systems12050165>.
- Guedes Gonçalves Costa, L. M. 2024. "'We Have Ethical, Legal, and Security Concerns': An Analysis of Pakistan's Foreign Policy on Lethal Autonomous Weapons Systems." Accessed July 14, 2025. <https://dspace.cuni.cz/bitstream/handle/20.500.11956/197759/120485535.pdf?sequence=1>.
- Hannah, C., L. E. Eriksson, A. Ramwell, and S. Llahana. 2025. "Experiences and Perspectives of Patients Undergoing Colorectal Cancer Surgery: A Qualitative Study." *European Journal of Oncology Nursing* 74:102794. <https://doi.org/10.1016/j.ejon.2025.102794>.
- Holster, B. S., Bullets, I. N., & Fitness, F. B. E. (2025). "Biden Military Reforms." *Intellect*. Accessed July 13, 2025. <https://convo.confex.com/biden-military-reforms>.
- Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2022). *Artificial Intelligence and International Security*. Center for a New American Security. Accessed July 14, 2025. https://csdsafica.org/wp-content/uploads/2020/06/CNAS_AI-and-International-Security.pdf.
- Horowitz, M. C., L. Kahn, and C. Mahoney. 2020. "The Future of Military Applications of Artificial Intelligence: A Role for Confidence-building Measures?" *Orbis* 64 (4): 528–543. <https://doi.org/10.1016/j.orbis.2020.08.003>.
- Hunter, L. Y. 2025. "Artificial Intelligence, Data Centers, Energy Capabilities, and International Security: An Exploratory Analysis." *Armed Forces & Society*. <https://doi.org/10.1177/0095327X241308839>.
- Hunter, L. Y., C. D. Albert, J. Rutland, K. Topping, and C. Hennigan. 2024. "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations." *Defense & Security Analysis* 40 (2): 235–269. <https://doi.org/10.1080/14751798.2024.2321736>.
- Jensen, B. M., C. Whyte, and S. Cuomo. 2020. "Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence." *International Studies Review* 22 (3): 526–550. <https://doi.org/10.1093/isr/viz025>.

- Jozaghi, E. 2025. "National Security during the First AI Revolution: The Case for Transforming Canada's Security Apparatus." *Canadian Public Administration* 68 (2): 285–308. <https://doi.org/10.1111/capa.70020>.
- Kavitha, D., and S. Thejas. 2024. "Ai Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation." *IEEE Access* 12:173127–173136. <https://doi.org/10.1109/ACCESS.2024.3493957>.
- Khalid, U. 2025. "The Digital Battlefield: A Comparative Analysis of AI-driven Cyber Warfare in the US and China and Its Implications for Pakistan's National Security." *ASSAJ* 4 (01): 64–76.
- Khan, A. M., and A. A. Khan. 2025. "Cyber-deterrence and Cyber-CBMs: Way Forward for Managing India-Pakistan Cyber Rivalry." *Journal of Asian and African Studies*, <https://doi.org/10.1177/00219096251332932>.
- Khan, K., A. Khurshid, and J. Cifuentes-Faura. 2024a. "Is Artificial Intelligence a New Battleground for Cybersecurity?" *Internet of Things* 28:101428. <https://doi.org/10.1016/j.iot.2024.101428>.
- Khan, A., Z. Siddiqui, and O. Farooq. 2024b. "Artificial Intelligence in Emerging Economies: A Focus on Pakistan's Technological Advancements and Challenges in 2024." *AlgoVista: Journal of AI and Computer Science* 2 (2): 14–22.
- Khayat, M., E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, and H. M. Khater. 2025. "Empowering Security Operation Center with Artificial Intelligence and Machine Learning – A Systematic Literature Review." *IEEE Access* 13:19162–19197. <https://doi.org/10.1109/ACCESS.2025.3532951>.
- Kihato, C. W. 2025. "Securitization Is (Normal) Politics: Epistemological Insights from Kenya's Forced Migration and Security Experience." *Migration Studies* 13 (2): mna008. <https://doi.org/10.1093/migration/mnaf008>.
- Lauwaert, L., and B. Chomanski. 2025. "Technological Determinism." In *We, Robots: Questioning the Neutrality of Technology, Ethical AI and Technological Determinism*, 81–130. Cham: Springer Nature Switzerland.
- Li, H. X. 2025, May. "Exploration of Wargaming and AI Applications in Military Decision-Making." In *2025 International Conference on Military Technologies (ICMT)*, 1–5. IEEE.
- Lim, W. M. 2025. "What Is Qualitative Research? An Overview and Guidelines." *Australasian Marketing Journal* 33 (2): 199–229. <https://doi.org/10.1177/14413582241264619>.
- Livingston, M. (2022). "AI Vulnerability, National Security, and Private Sector Power: Securitization Theory Meets AI." Accessed July 10, 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5010934.
- Lorenzi, J. H., and M. Berrebi. 2019. *Progress or Freedom: Who Gets to Govern Society's Economic and Technological Future?* Cham: Springer.
- Lukacovic, M. 2025. "Securitization." In *The Handbook of Social and Political Conflict*, edited by S. Samoilenko and S. Simmons, 1–480. Hoboken, NJ: Wiley-Blackwell.
- MacLure, M. 2024. "Qualitative Methodology and the New Materialisms: A Little of Dionysus's Blood?" In *Qualitative Inquiry in Transition - Pasts, Presents, & Futures: A Critical Reader*, edited by N. K. Denzin and M. D. Giardina, 139–152. London: Routledge.
- Mademlis, I., M. Mancuso, C. Paternoster, S. Evangelatos, E. Finlay, J. Hughes, Panagiotis Radoglou-Grammatikis, et al. 2025. "The Invisible Arms Race: Digital Trends in Illicit Goods Trafficking and AI-Enabled Responses." *IEEE Transactions on Technology and Society* 6 (2): 181–199. <https://doi.org/10.1109/TTS.2024.3514683>.
- Malik, M., H. Kamal, and M. T. Nazar. 2023. "Autonomous Weapon Systems: Boon or Bane? The Pakistani Perspective." *RSIL Law Review*. 7:67.
- Merrill, A. 2024. "Start-up War: Venture Capital, Silicon Valley, the Pentagon and the Wars Yet-to-come." PhD diss., University of Toronto.
- Mir, M. A., and T. Nazir. 2024. "South Asian Perspectives on the Nuclear Weapons Ban: Challenges and Prospects for Disarmament." *Peace Review* 36 (2): 256–266. <https://doi.org/10.1080/10402659.2024.2328541>.
- Mügge, D. 2023. "The Securitization of the EU's Digital Tech Regulation." *Journal of European Public Policy* 30 (7): 1431–1446. <https://doi.org/10.1080/13501763.2023.2171090>.

- Muthusamy, A., and R. Negi. 2018. "Global Investment Scenario of Artificial Intelligence (AI): A Study with Reference to China, India and United States." *International Journal of Advance and Innovative Research* 5 (4): 71–77.
- Ndzendze, B., and T. Marwala. 2023. *Artificial Intelligence and International Relations Theories*. Singapore: Palgrave Macmillan. <https://doi.org/10.1007/978-981-19-4877-0>.
- Ohwo, C. A. 2025. "Strategic Partnerships and Nigeria's National Security." *African Journal of Social Issues* 8 (1): 395–420. <https://doi.org/10.4314/ajosi.v8i1.24>.
- Osimen, G. U., O. Newo, and O. M. Fulani. 2024. "Artificial Intelligence and Arms Control in Modern Warfare." *Cogent Social Sciences* 10 (1): 2407514. <https://doi.org/10.1080/23311886.2024.2407514>.
- Parisini, E. 2025. "Governing Artificial Intelligence in the Defence Sector: A Comparative Analysis of EU and US Institutions." *Global Public Policy and Governance* 5:114–138. <https://doi.org/10.1007/s43508-025-00115-x>.
- Radanliev, P. 2024. "Digital Security by Design." *Security Journal* 37 (4): 1640–1679. <https://doi.org/10.1057/s41284-024-00435-3>.
- Ren, C. 2025. "Qualitative Research." In *Encyclopedia of Tourism*, edited by J. Jafari and H. Xiao, 841–844. Cham: Springer Nature Switzerland.
- Rickli, J. M., and F. Mantellassi. 2023. "Artificial Intelligence in Warfare: Military Uses of AI and Their International Security Implications." In *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*, edited by M. Raska and R. A. Bitzinger, 12–36. London: Routledge.
- Rogers, D. 2025. "Deconstructing National Security Strategy as Professional Struggle." *Political Anthropological Research on International Social Sciences (PARISS)* 5 (2): 211–244. <https://doi.org/10.1163/25903276-bja10062>.
- Roy, K., ed. 2024. *Artificial Intelligence, Ethics and the Future of Warfare: Global Perspectives*. Abingdon: Routledge.
- Roy, K., and G. M. Reichberg. 2024. "Artificial Intelligence and Pakistan's National Security." *PRIO Paper*. Oslo: PRIO. Accessed November 5, 2025. <https://www.prio.org/publications/14002>.
- Sahu, K., R. Kumar, R. K. Srivastava, and A. K. Singh. 2025. "Military Computing Security: Insights and Implications." *Journal of the Institution of Engineers (India): Series B* 106 (4): 1091–1115. <https://doi.org/10.1007/s40031-024-01136-6>.
- Sale, J. E., and L. Carlin. 2025. "The Reliance on Conceptual Frameworks in Qualitative Research – A way Forward." *BMC Medical Research Methodology* 25 (1): 1–5. <https://doi.org/10.1186/s12874-025-02461-0>.
- Saleem, B., M. Ahmed, M. Zahra, F. Hassan, M. A. Iqbal, and Z. Muhammad. 2024. "A Survey of Cybersecurity Laws, Regulations, and Policies in Technologically Advanced Nations: A Case Study of Pakistan to Bridge the Gap." *International Cybersecurity Law Review* 5 (4): 533–561. <https://doi.org/10.1365/s43439-024-00128-y>.
- Serscikov, G. 2025. "NOCs and Illegals in the Current Surveillance Landscape: Can Mimicry Help Overcome Evolving Challenges?" *Intelligence and National Security* 40 (3): 507–532. <https://doi.org/10.1080/02684527.2025.2485806>.
- Singh, S. K., R. S. Raj, and Radha. 2024. "The Geopolitical Significance of Afghanistan for India in Emerging World Order." In *Emerging Dynamics of India-Afghanistan Relations*, edited by R. K. Singh and S. K. Singh, 31–48. Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-97-4707-8_3.
- Singh, T. K., and D. Tiwari. 2025. "Disruptive Technologies in Strategic Affairs Threats and Preparedness for India." *Comparative Strategy* 44 (4): 460–472. <https://doi.org/10.1080/01495933.2025.2504854>.
- Smith, J. A. (2024). "Qualitative Psychology: A Practical Guide to Research Methods." Accessed June 5, 2025. <https://www.torrossa.com/en/resources/an/5730629>.
- Syllaidopoulos, I., K. Ntalianis, and I. Salmon. 2025. "A Comprehensive Survey on AI in Counter-terrorism and Cybersecurity: Challenges and Ethical Dimensions." *IEEE Access* 13:91740–91764. <https://doi.org/10.1109/ACCESS.2025.3572348>.

- Taber, N. 2025. "Learning to Share Gendered Military Experiences: An Autoethnographic Exploration of Expressive Writing in Transforming Military Cultures." *New Horizons in Adult Education and Human Resource Development* 37 (4): 225–234. <https://doi.org/10.1177/19394225241312441>.
- Taddeo, M., A. Blanchard, and C. Thomas. 2024. "From AI Ethics Principles to Practices: A Teleological Methodology to Apply AI Ethics Principles in the Defence Domain." *Philosophy & Technology* 37 (1): 42. <https://doi.org/10.1007/s13347-024-00710-6>.
- Tessema, D. 2021. "Technological Determinism versus Social Determinism, a Critical Discussion." *Ethiopian Journal of Science and Sustainable Development* 8 (2): 65–72.
- Tisdell, E. J., S. B. Merriam, and H. L. Stuckey-Peyrot. 2025. *Qualitative Research: A Guide to Design and Implementation*. 5th ed. Hoboken, NJ: John Wiley & Sons.
- Wall, C. 2025. "The Ghost in the Machine: Counterterrorism in the Age of Artificial Intelligence." *Studies in Conflict & Terrorism*, 1–27. <https://doi.org/10.1080/1057610X.2025.2475850>.
- Wasi, N. 2024. "Pakistan's Security Discourse from Geopolitics to Geo-economics." In *The Futures of Borders and Geopolitics in South Asia. Global Political Transitions*, edited by A. Mohsin, A. A. Ashraf, N. R. Biswas, and M. A. Rahman, 273–292. Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-97-6595-9_11.
- Weissmann, M. 2025. "Future Threat Landscapes: The Impact on Intelligence and Security Services." *Security and Defence Quarterly* 49 (1): 40–57. <https://doi.org/10.35467/sdq/197248>.
- Wertman, O., and C. Kaunert. 2022. "The Audience in Securitization Theory." *Strategic Assessment* 25 (3): 67–81.
- Winkel, M. 2025. "Controlling the Uncontrollable: The Public Discourse on Artificial Intelligence between the Positions of Social and Technological Determinism." *AI & Society* 40:1947–1959. <https://doi.org/10.1007/s00146-024-01979-z>.
- Yabanci, B. 2025. "Surveil, Datafy, Publicize: Digital Authoritarianism and Migration Governance in Turkey." *Democratization* 32 (4): 1016–1041. <https://doi.org/10.1080/13510347.2024.2433091>.
- Zeng, J. 2021. "Securitization of Artificial Intelligence in China." *The Chinese Journal of International Politics* 14 (3): 417–445. <https://doi.org/10.1093/cjip/poab005>.