Mairaj
Vol 3, Issue 1
https://www.mairaj.pk editor.mairaj@gmail.com
ISSN Online 2959-2089 ISSN Print 2959-2070

Khalid Arbab Khan
Scholar, Govt And Public Policy National Defence University, Islamabad

New Technologies, New Threats: Rethinking The Human Future

Abstract
The rapid development of new technologies has brought about previously unheard-of dangers, changing conventional notions of security and necessitating a reassessment of the future of humanity. By arguing that protecting human rights, dignity, and well-being must continue to be at the core of any response to technological disruption, this article highlights the importance of human security in this changing environment. It explores how the convergence of new technologies ranging from artificial intelligence to cyber capabilities has given rise to novel challenges that transcend borders and institutions. These threats are especially serious for developing nations like Pakistan in a volatile geopolitical environment, necessitating quick, context-specific responses. This study offers practical, flexible, and cooperative solutions for policymakers and defence planners while critically analyzing the risks posed by technology in the modern world, with an emphasis on Pakistan's opportunities and vulnerabilities. It underscores the imperative of rethinking security frameworks to ensure that technological progress does not outpace the mechanisms designed to protect people from its unintended consequences.
Keywords: Security challenges, New Technologies, Human security, future of Humanity, geopolitical, conventional security

Introduction

The rapid evolution of technology continues to reshape human society, presenting both unprecedented opportunities and formidable challenges. From artificial intelligence (AI) and quantum computing to biotechnology and advanced cyber systems, these innovations are transforming the global landscape, including the domains of defense, governance, and societal stability. However, the unchecked or irresponsible application of these technologies poses strategic risks to humankind, including cyber-attacks, misinformation, technological disparities, and environmental degradation. Pakistan, as a developing nation navigating a complex geopolitical environment, faces these challenges acutely. This research examines the technology-mediated threats confronting humanity today, with a focus on Pakistan's perspective, and proposes actionable strategies to address them. It argues that as new technologies spawn novel threats, defense planners and policymakers must adopt agile, innovative, and collaborative approaches to safeguard human security.

The emerging technologies, including advancements in generative AI, 5G networks, and bioengineering, are not merely extensions of past innovations but transformative forces that redefine the art of war, peace, and societal organization. While these tools enhance connectivity and productivity, they also amplify risks such as digital espionage, hybrid warfare, and climate change exacerbation. Pakistan, with its growing digital infrastructure and strategic challenges, is no exception. This paper underscores the need for a paradigm shift in how nations, including Pakistan, approach technology-driven threats to ensure sustainable development and security.

Research Methodology

This study uses a qualitative research methodology and uses secondary sources to investigate how the relationship between emerging technologies and human security is changing. Since the subject is conceptual and exploratory, the research is based on a thorough desk-based analysis that draws from a wide range of sources, including scholarly journals, policy reports, publications from think tanks, international organizational documents, and reliable online resources. In the context of developing countries like Pakistan, special attention was paid to literature that examines technological disruption, cybersecurity, digital governance, and the socio-political ramifications of innovation.

In order to find thematic trends, theoretical insights, and policy gaps, the study instead synthesizes the body of existing knowledge. This approach provides a thorough understanding of how states, especially those in unjustified geopolitical environments, can adjust to and lessen the security threats posed by swift technological advancement by enabling a critical analysis of both global and regional viewpoints.

Literature Review

The global security landscape has undergone a significant transformation due to the advent of new technologies like artificial intelligence (AI), quantum computing, autonomous systems, and advanced cyber capabilities. Scholars argue the swift incorporation of these technologies into society, warfare, and statecraft has brought about both new dangers and previously unheard-of opportunities. According to kello (2017), Cyberspace has emerged as a new arena of conflict, upending conventional ideas of sovereignty and deterrence. Similar to this, Singer and Brooking (2018) point out how propaganda powered by AI and information warfare has muddied the distinction between peace and conflict, with far-reaching effects on human security.

In this context, the idea of human security which places more emphasis on protecting people than states have attracted renewed attention. Human security is defined by the United Nations Development Programme (UNDP, 1994) as encompassing economic, health, environmental, personal, and political aspects, all of which are now directly impacted by technological advancements. The possible misuse of technology presents serious ethical and policy issues in a world where digital systems are influencing society more and more. Zuboff (2019) cautions against "surveillance capitalism," which commodifies personal data and directly jeopardizes democratic governance and individual liberty

Developing nations like Pakistan are especially susceptible to the two-pronged effects of technological progress. While digital innovation offers prospects for improved governance and economic growth, these countries are also vulnerable to cyber threats, disinformation, and digital dependency due to a lack of regulatory frameworks and weak institutional safeguards (Awan, 2020). Furthermore, the calculation of national security is complicated by the geopolitical ramifications of technological superiority, particularly in areas where strategic competition is evident. According to Farrell and Newman (2019), "weaponized interdependence," in which governments use technological networks to influence or impose restrictions on competitors, is becoming a more significant feature of global power dynamics. Scholars and decision-makers stress the necessity of flexible, human-centered security frameworks in this changing environment. This entails reconsidering conventional defense planning, making investments in cyber resilience, and encouraging global collaboration on technology governance (West, 2018). Although the strategic significance of digital transformation is becoming increasingly recognized in Pakistan, there are still large policy and capacity gaps (Khan & Yousef, 2021). In addition to technological advancements,

addressing these vulnerabilities calls for a shift in national security priorities that prioritizes human rights and dignity in the forefront of technological advancement

Theoretical framework

This study is grounded in the Human Security paradigm, which offers a thorough and human-centered method for comprehending current security risks. The 1994 UNDP Human Development Report introduced the human security framework, which stresses protecting people from a wide range of risks, including technological, environmental, economic, and cyber threats. This is in contrast to traditional realist theories that concentrate on state-centric military threats. It makes the case that protecting people's rights, dignity, and well-being must be the main objective of security.

To supplement this lens, the paper also draws upon the theory of Technological Determinism as it states that technological innovation is a major force behind societal change and that, depending on how it is managed, it can either empower or threaten humanity. This theory explains how new technologies, particularly in fragile states, are introducing asymmetric threats and changing power dynamics. Examples of these technologies include cyber tools, surveillance systems, and artificial intelligence. Furthermore, the Copenhagen School's Securitization Theory is used to examine how governments present new technologies as existential dangers to support extraordinary policy responses. This aids in comprehending how digital technologies have become politicized and how national and international security agendas have incorporated them.

The study challenges policymakers to reconsider security frameworks that place a higher priority on human resilience and ethical governance in a rapidly changing technological world by integrating these theoretical lenses and critically examining how technology-driven threats are redefining the essence of security.

Human Security: A Theoretical Perspective

Thinkers and theorists have been debating the definition of security for a long time, and the discussion has continued to this day. In summary, the concept of security has evolved from state-centric, or classic, security to human-centric, or comprehensive, security. The traditional understanding of security limits the state as a serious actor, limits security in a military context, and holds that a state's use of force is the only thing that can threaten another state. In the interdependent world, these are being dismantled due to the evolving nature of non-traditional security perceptions, such as environmental, societal, economic, and cultural. Non-Traditional Security Threats (NTS) are thought to pose just as serious a threat to the nation and its citizens as military threats. In a setting where nation states are becoming more interdependent, these recently added dimensions of security relax the traditional realist definition of security and address issues like the number of non-state actors in the security grid.

According to Barry Busan & lene Hansen, the 21st century security environment is characterized by shifting threats, with economic, human, environmental, and other security measures superseding military security (Busan & Hansen, 2009). It is less important, but the state is still everything. Near the state, new organizations, governments, and regulations have established significant positions. However, a complex web of interconnected social and environmental regulations creates the framework for achieving human security in its entirety, based on the idea that neither can be accomplished without the other.

In addition, Arthur H. Westing states that in order to attain the highest level of social and environmental security, the two aspects of comprehensive human security can be broken down into a sequential set of subcomponents because they are nearly in-separable (Westing, 2013). The components of Social Security can be divided into four categories: established

political securities, economic securities, personal security, and military security. One of the two subcomponents of environmental security is rational resource consumption, which is defined as using resources in a way that "meets the needs of the present without compromising the ability of future generations to meet their own needs." In addition to environmental security, a broader definition of human security also encompasses social security.

The 1994 Human Development Report of the United Nations Development Programme, which makes the case that ensuring "freedom from want" and "freedom from fear" for all people is the best way to address the issue of global insecurity, is frequently cited as a seminal work in the field of human security (United Nations, 1994). Mahbub ul Haq, a Pakistani economist and international development theorist, actually coined and popularized the term "human-economic security" in 1995 while trying to sway the United Nations 10th Anniversary Summit in Copenhagen to honour the August 1988 Declaration on Social Progress and Development.

Moreover, Rousseau talked about ceding your rights to self-defence or your own will to a superpower, which he referred to as a sovereign or state. For the same reasons that would aid in the protection of individuals within the state and society, once more (Tucker, 2022). According to John Locke, when you work with nature, you own that portion of it. To protect it, including your life and your quest for freedom, you must enter the state. Therefore, human security is not a particularly new concept. It has only been rebranded, reframed, and now re-rehearsed in front of us to reflect on the current state of affairs, where internal violence within states and between ethnic groups is on the rise and international wars are becoming less frequent (Tuckness, 2024). Furthermore, non-traditional threats and emerging challenges from new technologies pose a greater threat to humanity today.

Findings

Challenges Posed by New Technologies

Rapid developments in artificial intelligence (AI), quantum computing, 5G, biotechnology, and the Internet of Things (IoT) define the contemporary technological landscape. Despite being revolutionary, these innovations present a number of complex security issues. An updated analysis of the main threats, emphasising recent advancements, is provided below:

IoT devices and 5G networks have increased the attack surface for state actors and cybercriminals. Cyberattacks worldwide rose 30% in 2024 compared to 2022, with phishing and ransomware focusing on vital infrastructure (Boa, 2024). Pakistan has been the target of cyberattacks, including purported state-sponsored attacks from nearby nations, which have attempted to interfere with defence and financial networks. A data breach in Pakistan's banking industry in 2023, for example, revealed private client data, exposing weaknesses in digital infrastructure.

Generative AI models that drive chat bots and content production tools had made significant progress, allowing for the creation of hyper-realistic deep fakes and disinformation campaigns. Because AI-guided autonomous weapons, such as lethal autonomous weapon systems (LAWS), can function without human supervision, they present ethical questions in the defence industry (Julius, 2024). Although Pakistan's defence industry is investigating AI for precise targeting, there is still a significant chance that enemies will use similar technologies against it.

More than 60% of internet users worldwide will get their news from social media, which will accelerate the spread of hate speech and fake news. Misinformation campaigns on WhatsApp and X have exacerbated sectarian tensions and social unrest in Pakistan (Ihsan, 2024). Coordination of disinformation campaigns during Pakistan's 2024 elections highlighted the necessity of effective counterstrategies.

With the growth of the global data economy, hackers are increasingly targeting personal information. The importance of data protection in Pakistan is underscored by events such as the 2023 Careem data breach and the 2024 revelation of government database leaks on the dark web (Usman, 2018). Along with cybercrime and climate change, data theft is ranked as one of the top five global risks in the World Economic Forum's Global Risks Report (World Economic Forum, 2024).

The use of hybrid warfare, which combines disinformation, psychological operations, and cyberattacks, has increased. Social media and artificial intelligence are tools used by adversaries to sway public opinion and undermine institutions. Both state and non-state actors pose hybrid threats to Pakistan, such as terrorist organizations that use encrypted platforms for propaganda and recruitment.

Half of Pakistan's population have not dependable internet access, highlighting the country's glaring digital divide. This disparity restricts access to education and employment opportunities, exacerbating existing inequalities. Global economic disparities are sustained by the gap between countries that produce and those that consume technology, with developing nations like Pakistan depending on imported solutions.

Energy-intensive data Centres and manufacturing processes are two ways that technology is causing climate change. Floods, heat waves, and water scarcity are becoming more frequent in Pakistan, which was named the 5th most climate-vulnerable nation (Abubakar, 2024). Millions were displaced by the floods in the Indus River in 2023, highlighting the necessity of climate-resilient technologies. On the other hand, although they demand a large financial outlay, green technologies like solar power and AI-powered climate modelling present viable answers.

The state's monopoly on violence is being undermined by advanced technologies that empower non-state actors. In Pakistan, lone actors take advantage of easily accessible technologies for violence, while terrorist organizations such as the TTP use drones and encrypted communication to carry out attacks. This new danger was brought to light by the 2024 drone attack on a military convoy in Karachi (Zia, 2023).

Advances in bioengineering, including CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats) and synthetic biology, hold promise but also risks. With the world's health systems still recuperating from the pandemic of 2020–2022, the risk of bioterrorism or the unintentional release of engineered pathogens has also increased and Pakistan is susceptible to these threats due to its inadequate biosecurity infrastructure.

Low-skilled jobs have been replaced by automation and artificial intelligence; as robotic automation in Pakistan's textile industry is expected to cause a 15% loss in employment. This exacerbates social unrest, especially among Pakistan's youth, who make up 60% of the population (Nasir, 2024).

1. Challenges of New Technologies: Pakistan’s Perspective

Over the past few decades, digital technology has become a major enabler of productivity growth in Pakistan. Although Pakistan is already reaping some benefits from digitization, more performance improvement is still possible. However, Pakistan's growth has stalled due to its neighbourhood, the unsightly four or more decades of wars, and internal and external geopolitical and geostrategic obstacles.

Although deep-fakes and AI-driven fraud were addressed in the 2023 update to the Prevention of Electronic Crimes Act (PECA) of 2016, enforcement of the law is still lacking. PECA is criticised by digital rights advocates for restricting free speech and putting security and liberty at odds.

Internet penetration is lower in rural areas than in urban areas, at 20% versus 70%. Women make up only 25% of internet users, demonstrating the continued gender gap (Nadia, 2024).

R&D spending is still less than 1% of GDP, which limits innovation, and only 10% of IT graduates are able to meet industry demands (Usman, 2024).

The slow adoption of green technologies in Pakistan makes the country's climate problems worse. Lack of funding impedes the 2024 National Climate Adaptation Plan's efforts to incorporate AI for disaster forecasting.

India is not an exception to the cyclonic offensive's use of cyberattacks against Pakistan. The hacker war between the two countries has so far only involved data theft and website defacement, but if left unchecked, this could spiral into much more dangerous territory.

The laws pertaining to cybercrime have been the most prominent development on Pakistan's cyber front. In 2016, the Prevention of Electronic Crimes Act (PECA) was approved by both houses of parliament. A few of the amendments put forth by advocates for digital rights were given the consideration they deserved by being added to PECA. However, the vocal activist lobby had been engaged in a fierce battle against the bill's provisions that they believed violated their rights as citizens.

Like in other nations, Pakistani terrorist mafia groups have been using the internet to propagate terror in an effort to instill fear, spread propaganda, and persuade people to join them. Funding claims that they have only made requests for funding through online channels (Helen, 2019). The Pakistan Electronic Crimes Act, the Anti-Terrorism Act, and the Fair Trial Act are powerful tools that Pakistan can use to combat the threat of ICT-assisted atrocities. These laws empower us to, for instance, block hate speech on the internet, thwart terrorist recruitment and funding, and interfere with terrorist’s ability to carry out terrorist acts. Additionally, the public can report extremist and terrorist content on the internet through the Safe Pakistan portal, which is an online portal run by the National Counter Terrorism Authority (NACTA).

Pakistan faces many problems and challenges in the technology sector, just like other developing countries that use technology rather than produce it. For example, Pakistan has one of the biggest digital divides between men and women in the world, and efforts to improve employment prospects have concentrated on the country's smaller number of highly skilled workers.

Way Forward

To fight these challenges to the humankind. In this context, the following are of note:

1. All carbon-based life forms are entangled in the challenges posed by emerging technologies, and no individual or nation can confront them alone. A collective, coordinated response is essential. We must come together to shape a unified strategy for the future.
2. It is not timely thinking and progress in military applications of AI. At some point, AI will become a part of all modes of warfare. So concentrated attention and capacity is needed to assess and broaden the spectrum of short, medium and long-term applications of AI into the military arena.
3. Therefore, there is requirement to develop, international or regional Code of Conduct under UN to ensure safeguards against threats arising from indiscriminate use of new technologies.
4. Invest in AI for defence uses, like counterterrorism predictive analytics, while setting moral standards to avoid abuse. Launched in 2024, a National AI Strategy ought to be carried out completely (Civan, 2024).
5. To better coordinate responses to cyber threats, strengthen PECA enforcement and create a National Cyber-security Agency. Partnerships between the public and private sectors can strengthen the protection of vital infrastructure.
6. Increase the availability of 5G infrastructure in rural regions and provide low-income households with internet access subsidies.

7. Adopt renewable energy and climate modelling powered by AI. To help with these initiatives, Pakistan should make use of global climate funds like the 2024 Green Climate Fund.
8. Boost STEM funding and match industry demands with IT curriculum. The 2024 Tech Talent Program demonstrates how public-private partnerships can close the skills gap.
9. Create AI-based tools and public awareness campaigns to identify and flag false information on social media.
10. Discover from international frameworks such as the 2023 WHO Biosafety Accord to bolster biosecurity procedures and make investments in early-warning systems for bioengineered threats.

Conclusion

In nutshell, technological revolution has dualistic sides: it offers tools for advancement but also poses existential threats. Pakistan needs to use flexible and creative tactics to deal with the geopolitical, economic, and environmental limitations it faces. Human security must be given top priority by defence planners, legislators, and the general public, who must strike a balance between ethical protections and technology adoption. Since no country can a ddress these issues on its own, cooperation both domestically and internationally is essential. The maxim "change and change again" emphasizes the necessity of constant adaptation in order to keep up with changing threats. In order to ensure that the tools we develop benefit humanity rather than endanger it, Pakistan can help ensure a safe, just, and sustainable future for all people by using technology responsibly. In the end, what we make of science and technology is a matter of reconciling ourselves to our interactions with them. Yet until we get there, a peaceful and prosperous world probably will be beyond our reach.

Reference

1. Abubakar, S. M. (2022). Pakistan ranked most vulnerable to climate change in 2022: German watch. DAWN.COM. https://www.dawn.com/news/1891272
2. Boa, patent. (2024). 5G & Cybersecurity: Network Threat Stats; https://patentpc.com/blog/5g-cybersecurity-network-threat-stats
3. Buzan, B., & Hansen, L. (2009). The Evolution of International Security Studies (1st edition). Cambridge University Press.
4. Civan, K. (2024). The National Artificial Intelligence Strategy 2024-2025 Action Plan | Cott-Group. https://www.cottgroup.com/en/blog/technology/item/the-national-artificial-intelligence-strategy-2024-action-plan
5. Helen, Mortune (2019); why has Organized crime been used to finance terrorism in the Sahel: A critical analysis of the Crime-Terror nexus of AL Qaeda in the Islamic Maghreb (AQIM). https://www.academia.edu/128279129/Why has Organized crime been used to finance terrorism in the Sahel; A critical analysis of the Crime Terror nexus of AL Qaeda in the Islamic Maghreb AQIM?
6. Ihsan, U. (2024). Pakistan's Social Media Strategy is Being Recognized Worldwide Stratheia. https://stratheia.com/pakistans-social-media-strategy-is-being-recognized-worldwide
7. Julius, E. (2024). Generative AI is the ultimate disinformation amplifier. https:/akademie.dw.com/en/generative-ai-is-the-ultimate-disinformation-amplifier
8. Nadia (2024) the mobile gender gap in South Asia is now widening; https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/the-mobile-gender-gap-in-south-asia-is-now-widening/
9. Nasir, S., Ali, M., Irshad, M., & Wazir, S. (2024); Critical Evaluation of Textile Industry of Pakistan and Way Forward.

10. Tucker, L. (2022). Rousseau's Social Contract Theory. https://open.library.okstate.edu/introphilosophy/chapter/rousseaus social contract theory
11. Tuckness, A. (2024). Locke's Political Philosophy. In E. N. Zalta & U. Nodelman (Eds.), the Stanford Encyclopedia of Philosophy; Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2024/entries/locke-political/
12. United Nations (with UNDP) (1994); Human development report 1994. Oxford University Press.
13. Usman, K. (2018). There are no laws to protect your data in Pakistan. So how can we minimize breaches like the Careem hack? www.dawn.com. https://www.dawn.com/news/1404802
14. Usman, Z. (2024). Pakistan Needs a Private-Sector R&D Revolution Digital Pakistan. https://digitalpakistan.pk/pakistan-needs-a-private-sector-rd-revolution
15. Westing, A. H. (2013). From Environmental to Comprehensive Security; Springer International Publishing. https://doi.org/10.1007/978-3-319-00687-1
16. World Economic Forum (2024). Global Risks Report 2024: Conflict, Environment and Disinformation Top Threats | Global Heat Health Information Network. https://ghhin.org/news/global-risks-report-2024-conflict-environment-and-disinformation-top-threats
17. Zia, R. (2024) Pakistan Waging a Deadly Drone Campaign Inside Its Own Borders-The New York Times. https://www.nytimes.com/world/asia/pakistan-drones-militants.html
18. Awan, A. N. (2020). Cybersecurity in Pakistan: Challenges and Policy Options. Pakistan Institute for Conflict and Security Studies.
19. Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, 44(1), 42–79.
20. Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.
21. Khan, M., & Yousef, H. (2021). Pakistan's National Cybersecurity Framework: A Critical Assessment. Journal of Security and Strategic Analyses, 7(1), 21–40.
22. Singer, P. W., & Brooking, E. T. (2018). Like War: The Weaponization of Social Media. Houghton Mifflin Harcourt.
23. West, D. M. (2018). The Future of Work: Robots, AI, and Automation. Brookings Institution Press.
24. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.