

Title - Joint Framework for Ethical AI, Digital Governance, Digital Sovereignty in South Asia

ABSTRACT

The rapid emergence of Artificial Intelligence and technology, and heavy digital usage, have impacted and transformed several factors, such as governance, security, relations, and cooperation among SAARC nations. SAARC nations face major challenges related to Cybersecurity Vulnerabilities, weak regulatory coordination, Technological Dependency on developed nations and the absence of a joint AI framework. The study also looks at the growing threats from cyber-attacks in the region. These threats include cybercrime, misinformation, infrastructure weaknesses, and tensions between countries over cyber issues. Research also focuses on the SAARC joint framework for Ethical AI, Digital governance, and Cybersecurity. Artificial Intelligence focuses on ethical norms such as Fairness, accountability, Transparency, and human oversight to provide a Secure and Resilient Digital Environment. The research emphasises that if countries in the region work together through SAARC, they can strengthen their cybersecurity, encourage responsible behaviour in cyberspace, and reduce technological weaknesses and dependence that can be exploited against them. The research suggests that countries working together on cyber and digital issues can help build trust and stability in the region, and this can be an important part of digital governance in South Asia, encouraging countries to work towards a better collective future. SAARC can play a big role in this, and Artificial Intelligence can be a key part of this and digital cooperation is essential for the region's stability.

Keywords – Cybercrime, Ethical AI, Digital governance, Cybersecurity, Digital Cooperation, Digital strategic Autonomy.

CHAPTER I

1.1 INTRODUCTION

Vast disparities in preparedness, technological infrastructure, and regulatory capabilities among SAARC nations complicate this issue. Two important aspects in resolving this problem are ethical AI and digital governance. Ethical AI is the use of technology that ensures the principles of fairness, transparency and accountability. Digital governance refers to policies that govern the digital world or space to ensure individual and data protection. Together, these fundamentals contribute to the essence of technology management and help protect democracy and human rights. Despite significant progress in digitalisation in South Asia, urban-rural and economic disparities exist in the region, impeding full participation in the digital economy. Cybersecurity and ethical AI have become more complex than ever, with problems including data breaches, cyberattacks on public and private infrastructure, disinformation campaigns, and the exploitation of AI technology in places with limited capability. The rising competitiveness in digitalisation among external powers, including the US, China, and the EU, has become another significant threat to South Asian countries' technological sovereignty and strategic autonomy. Given these changes, there is an urgent need to focus on SAARC's regional cooperation model, shifting from a conventional trade-oriented approach to a Regional Digital Governance Framework. This paper analyses the digital future of South Asia and calls for the development of a Regional Digital Governance Framework within SAARC, based on the principles of transparency, accountability, inclusiveness, human rights, and digital sovereignty.

1.2 RESEARCH QUESTION

1. What are the Major challenges of digital governance and cybersecurity faced by the SAARC nations?
2. How does the Technological dependence on other nations affect the digital governance and sovereignty in South Asia?
3. How will the Joint AI Framework make a change in SAARC cooperation?
4. How do digital literacy and digital divide impact regional digitalisation?

1.3 RESEARCH OBJECTIVES

- I. To assess the status of ethical AI principles and digital governance frameworks of SAARC member states and the gaps in regional coordination.
- II. Analyse the cybersecurity challenges in South Asia, including cybercrime, data breaches and cross-border cyber threats and assess the adequacy of the existing response mechanisms, as well as the technological transformation.
- III. Study on the impact of external powers, particularly the US and China, on the digital governance decision-making and also examining the example of Huawei's 5G infrastructure expansion in South Asian technological dependencies on the SAARC countries.
- IV. To assess the digital literacy and the digital divide in the region as a precondition for inclusive and effective digital governance.

V. The recommendation of a SAARC framework for ethical AI, cybersecurity cooperation and digital governance, leveraging existing mechanisms, for example, SCCMD, SAARC Satellite, and extending the limited objectives to broader principles.

1.4 RESEARCH METHODOLOGY

This research is based on qualitative data and secondary sources, including SAARC intergovernmental documents, research papers, articles, international organisation reports, and peer-reviewed literature. Research also presents a comparative analysis of literacy and data protection policy frameworks among SAARC nations. Also, the research includes a case study on Huawei's 5G digital infrastructure project in the region. An analytical approach has been used in research about Ethical AI, Cybersecurity, digital governance and digital sovereignty. A recommendation for the Digital Framework of SAARC is built by using these approaches and methods.

CHAPTER II - LITERATURE REVIEW

This research paper is based on digital governance, ethical AI & cybersecurity, which is ultimately a very broad concept in itself, but the major ultimate goal is to protect people & build a joint framework on Artificial Intelligence & ensure digital security with the help of digital governance with the help of cooperation among SAARC nations. This paper focuses on aspects like: ethical AI & digital governance, South Asia digital transformation & challenges about ethical AI & cybersecurity, digital landscape & nations coordination, uneven digital literacy & digital divide in South Asia, impact of external power & technological influence, and, lastly, recommendations & future aspects in digital cooperation under SAARC.

In the foundational study, Azizi Othman (Othman, 2025) outlined the foundations of ethical AI, citing the European Union's AI framework and emphasising individual rights and other ethical considerations. Also, this research paper offers glimpses into how individual AI companies approach ethical norms— such as DeepSeek. (DeepSeek Terms of use, n.d.) has norms and terms related to product privacy and security. Another author cited is Benjamin Eshwhic. (Erhirhie, 2026), wrote about AI ethics in public administration, citing the European Union AI Act and norms such as transparency & safety, as well as UNESCO's work on digital governance & the global digital compact. Also, in the South Asian context, SAARC's needs are concluded by comparing the EU and ASEAN. Also, the authors Adhwarya Natrajan and (Natarajan, A. and Murali, V. S., 2020) wrote about the challenges AI faces in South Asian nations.

Another section is on South Asia's digital transformation and challenges to ethical AI and cybersecurity. The article by Svetlana A. Yusarova (Gusarova, Svetlana & Gusarov, Igor & Smeretchinskii, Margarita..., 2023) discusses the digital foundation of South Asia's digital transformation with the arrival of blockchain technology, the strategies nations are pursuing to protect their interests and drive economic and digital development, and R&D investment in digital development. Arshad wrote about how digital innovation has impacted fintech in Sri Lanka, including digital financial services. A journal article by Iqbal Babar (Iqbal, 2024) on digital strategic autonomy in South Asia concludes with cyberspace and data protection, as well as the implementation of fairness algorithms and ethical norms.

The third section of this research explores regional regulatory coordination among South Asian countries. In this section, Amlan's (Mohanty, 2026) Work on AI governance in South Asia describes the current landscape, providing country-wise summaries of regulations and related measures. Md. Mahmud Hasan (Mohammad, 2024), Another author, emphasises Artificial Intelligence & comparative studies in South Asian countries and also quotes the Government AI Readiness Index of 2022, which ranks South Asian countries and provides ground data. The fourth section of the third chapter examines digital literacy and the digital divide in South Asia. In the recent academic literature on South Asia and digital technologies, a common finding emerges: institutional momentum is evident, though uneven. In particular, the regional UNESCO study, based on surveys, institutional case studies, and policy analyses, examines higher education in Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka and concludes that. Some educational institutions are taking steps toward online learning and faculty training, while others are being neglected due to poor connectivity and illiteracy.

The concept of unevenness is examined in the context of a global trend explored in Fietz and Lay's GIGA study (Fietz, 2023), which highlights a significant gap in digital skills between wealthy and poor nations and argues that training programs cannot easily solve the

problem, as these skills are continually evolving. Moreover, the authors highlight that multiple initiatives aimed at improving digital skills have been ineffective and that hardware alone is insufficient. Digital skills and stratification in a broader context are analysed in Mohammad's (Mohammad, 2024) conference paper, which examines how marginalised groups in India and South Asia face the digital divide, in which the role of AI becomes another factor of inequality. The fifth section focuses on the influence of external powers in South Asian countries. Scholars have recently examined the digital infrastructures of South Asian countries through existing theories of great-power competition. In a study conducted by the Carnegie Endowment, (Pal, 2021) analyses Chinese interactions with Bangladesh, the Maldives, Nepal, and Sri Lanka from the perspectives of the fragility of their state institutions, the resilience of their civil societies, and the vulnerability of their elites to capture.

In 2025, (Bukhari., 2025) The analysis of China-Pakistan-India relations and the role of the US presence in the region in shaping disputes over borders, military buildup, economic interests, and diplomatic efforts helps clarify how technological dependence relates to broader strategic dynamics, with CPEC as a focal point of conflict. (Tekir, 2020) provides a clear conceptual framework, arguing that contemporary digital geopolitics is defined by influence over interconnected infrastructure rather than by traditional territorial control. The last section is more about recommendations. The (UNESCAP, 2017) The regional study analyses the feasibility of achieving deeper regional economic integration among South Asian countries from four main perspectives: trade and market integration, regional connectivity, financial cooperation, and collaboration to address shared regional challenges.

The World Bank (Bank, 2022) are presented in the context of a more general discussion on stagnation: even though the 2030 Agenda is emphasising inclusive development and Asia is emerging as a major driver of growth, the region continues to be perceived as the least economically integrated among all Asia-Pacific subregions, with less than 6 per cent intra-

regional trade compared to 26 per cent in Southeast Asia. This analysis of fragmentation and under integration in South Asia provides the structural context for the proposed digital cooperation. (Bank, 2022). Companion analysis synthesises the digital economy assessments of Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan, and Sri Lanka. It highlights the need for regional cooperation on cross-border connectivity and data infrastructure, supportive policies for cross-border data flows, and integrated cross-border payment systems.

CHAPTER III

3.1 The Foundation of Ethical AI & Digital Governance in SAARC.

AI is having effects on society that we could never have imagined, and because of that, it has to be regulated to ensure it is safe and not detrimental to human lives. Ethics in AI changes cyberspace to a safe and secure space where a person's life will be protected and their right to privacy upheld. AI ethics norms restrict algorithmic bias & misinformation, and decisions with transparency allow fairness and accountability. To protect the threat on an individual's privacy, ethical AI provides clear measures and rules in place for this reason, to tackle ethical problems. (Othman, 2025). An example of this is: The UN global digital compact and AI governance efforts recommended by UNESCO. (Digital Governance and Artificial Intelligence AI ethics in Public Administration, 2026) which primarily ensures international cooperation, human rights protection, risk management, digital inclusion, and responsible innovation at the regional level, China's global AI.

The European AI Union AI Act represented a rights-based and risk-based regulatory model, essentially the world's first comprehensive AI law, focusing mainly on fundamental rights, transparency, human oversight, safety, and state-led frameworks (Digital Governance and Artificial Intelligence AI ethics in Public Administration, 2026). China's model for promoting international AI governance, emphasising AI safety, state responsibility, fairness, and state-led regulation of algorithms and deep synthetic technologies, also ensures social stability as related to DeepSeek's terms or norms. In a service & norms 1:6 "Claus" - avoid sharing your own or other personal information, especially sensitive personal data; ethical

governance of AI & the prevention of digital authoritarianism in South & Southeast Asia; promoting innovation & technologies ethically; protecting society from risks & harms associated with AI (DeepSeek Terms of use, n.d.).

AI requires governance because it is both transformative, systemic and destructive. AI is a neutral technology, so the results are a product of the nature of its governance. While AI can be of help for sectors such as health care, public services, transportation and the economic system, the deployment of this technology can also lead to increased surveillance, discrimination and misinformation. However, AI in war and its applications can cause more devastating consequences. Digitalisation has directly contributed to governance and bureaucratic functions, and this phenomenon is not limited to a specific country or region but has spread across regional and global arenas. Digital governance has been considered one of the important foundational pillars of technological innovation, ensuring democracy, human rights and public trust. Challenges to South Asian countries in Ethical AI & Digital Governance: Poor regional cooperation has aggravated ethical AI and digital governance issues and made these effects contagious within emerging markets.

SAARC digital cooperation needs to be aligned, which is often appealing as a mix of public and private cooperation. The concentration of control authority in some states limits regional aspirations due to countries' national interests; also, the EU and ASEAN are exceptions in South Asia. Cybersecurity vulnerabilities, the rapid digitalisation of government services, and a lack of cyber infrastructure have increased cybersecurity risks and a trust deficit between constituent countries, underscoring the importance of joint cyber-ethical laws to mitigate ransomware attacks, data breaches, and cyber espionage. Due to a lack of ethical norms, misinformation, and a political disinformation campaign, relations between countries are strained (Natarajan, A. and Murali, V. S., 2020).

3.2 Examining the South Asia Digital Transformation and Challenges to Ethical AI and Cybersecurity.

South Asia represents one of the greatest ongoing digital transitions in the developing world. China's impact externally on digital technology is being leveraged as a catalyst for economic development, innovation, governance transformation and social progress, through the impact of the digital transformation in countries like India, Bangladesh, Pakistan, and Sri Lanka that have taken digitalisation as a cornerstone of their strategies of development (Bukhari., 2025). Aspects of Artificial Intelligence, cloud computing, blockchain, e-commerce, and the Internet of Things are driving the transformation of the regional economic framework and digital governance. The post-COVID-19 pandemic boosted the digitalisation and surveillance to maintain Security. Digitalisation across different contexts in South Asia has been directed to different sectors.

In India, blockchain helped differently. In countries like India, Sri Lanka, Bangladesh, and Pakistan, health is handled differently. In India, digital transactions are increasing, e-health services are expanding, Artificial intelligence is affecting job roles, and digital education is expanding. In Sri Lanka, digital technologies impacted insurance, financial tech, and digital finance administration, as well as healthcare management (Arshard, n.d.). Sri Lanka has a strong history of government administration as well, so the digitalisation helped with cyber or digital governance. Afghanistan's economic instability and digitalisation supported financial inclusion, transparency, and institutional efficiency. Bangladesh adopted new digitalisation strategies in 2020, including the National Blockchain Strategy, which helped in sectors such as

Digital identity management, Agriculture insurance, Health services, and Smart cities, similar to India (Gusarova, Svetlana & Gusarov, Igor & Smeretchinskii, Margarita., 2023).

Nepal has been heavily impacted by digitalisation and modernisation, with Digital platforms and social media facilitating youth mobilisation and political participation during recent governance-related protests in Nepal and the establishment of a new government. (Britannica., 2025). Additionally, the Sectoral impact, such as digital banking examples, E-Sewa, digital e-commerce, and online public services, also improves connectivity to remote areas, such as the mountain region, and is working on a strong digital infrastructure. And also increasing R&D investments (Gusarova, Svetlana & Gusarov, Igor & Smeretchinskii, Margarita., 2023). In the case of Pakistan, the main concerns with digital transformation are financial stability and controls, as well as inflation. Adopted blockchain and digital technologies have been promoted to improve transparency, financial monitoring, and administrative efficiency, and to ensure regional Stability.

The emergence of digital governance is changing the infrastructure of global governance and the working styles of national administrations. Cyberspace has become a new Domain of Strategic competition between countries, leading to information warfare that has also impacted countries' sovereignty. Because of digitalisation and technology, the world has become interconnected, and as a result, countries are protecting their confidential information related to military and other sensitive programmes. As Data has become a strategic asset, reliance on digital services from abroad creates or exacerbates national Security vulnerabilities for many countries. To maintain their digital sovereignty, many countries focus on technological self-reliance, which is now linked with political Sovereignty. As cyberspace is both beneficial and a threat to countries' governance and sovereignty, it poses risks to national security, economic growth, and diplomatic influence. However, it is beneficial in areas such as increased awareness of environmental safety, cross-sector cooperation, and global governance,

which help ensure benefits for vulnerable areas. Also, cyber warfare has emerged as the fifth domain of warfare After Land, water, Air, and space. Cyber warfare can disrupt critical infrastructure, economic activities, and national security systems, potentially producing significant societal consequences. In Digital governance, data and information play an important role in policy and decision-making, as well as in shaping policy for a country's population. As a result, domains have developed a strong correlation with the political and social sectors in recent times. Also, the State extended its power from the political domain into the control of data, including data on its surroundings, to forecast and thereby protect the state from threats. In the context of South Asia, Artificial intelligence has extensively reshaped communication and international diplomacy between countries. Security implications relate to the potential cyber risks associated with the exploitation of cyber vulnerabilities, including miscommunication, misinformation, spoofing, and cyber terrorism (Digital Governance and Artificial Intelligence AI ethics in Public Administration, 2026). This, without cyber norms and ethics for AI in the military and the Nuclear Domain more broadly, heightens Nuclear Strategy and raises concerns about nuclear deterrence, ethics, and AI capabilities (Sadiq, 2022).

The relevant ethical issues within AI are transparency, digital data Bias, Data Protection, Fairness, Responsibility, privacy, and accountability. In the context of bias and fairness, an AI system is dependent heavily on historical ideas and societal biases. If the Algorithmic Data related to discrimination is not addressed, then it would lead to discriminatory outcomes in areas such as hiring, lending, and law enforcement (Iqbal, 2024). If discrimination or biases, such as racial or socioeconomic bias, are not mentioned, then outcomes from generative or other AI also tend to be non-discriminatory. The diversity of the data used to train an AI model to ensure equality norms across different demographic & social contexts: also train and implement fairness algorithms to mitigate biases. Ethical norms in privacy & Data protection because personal data raises privacy concerns, particularly when AI

is used for Surveillance, profiling, or decision-making, which indirectly affects individual life. Data protection regulations should govern an AI system.

The algorithmic data should help protect fundamental rights. So, in the context of South Asia, the data should be protected by a regional mechanism for cyber threat information-sharing and cybersecurity cooperation, similar to a cybercrime monitoring desk. One of the important aspects of regulating AI under ethical norms is accountability and responsibility. To counter unethical behaviour, there should be clear standards and guidelines on human rights and outcomes, as well as ethical norms for the development and deployment of AI-unbiased decision-making systems. In the context of SAARC, there should be an ethical framework for the use of AI in the region that mitigates bias and discrimination and ensures transparency, fairness, and data protection.

3.3 Digital Landscape of the South Asian Region: A Regional Assessment in Regional Regulatory Coordination.

South Asian nations face severe challenges due to rapid digitalisation, which is affecting routine government operations and regulations, as well as the expansion of internet connectivity, mobile penetration, digital payments, and e-governance, which help governments expand. Surveillance & policy to reach vulnerable areas & sections of society, which also have positive means for economic growth, social inclusion, and public services (Mohanty, 2026). It raises questions about why AI should be regulated, because it is also embedded in our everyday work, poses a threat to personal and government confidential information, and is not limited to any particular nation. However, while this is worldwide, regional groups have already implemented different frameworks.

SAARC member countries can collaborate to collectively oversee AI and digital data to safeguard not just their own nations but the entire region. AI regulations protect individuals

and governments from the misuse or failure of AI systems, which can lead to detrimental effects and harm not just one nation but an entire area. Additional elements, such as public confidence, human rights, and privacy, are secured by the government through robust regulatory safeguards that balance innovation, privacy, security, and fundamental rights. thereby safeguarding individual rights and upholding transparency and equitable treatment, including safeguards against discrimination, privacy violations, and job loss. Additionally, Regulatory oversight can reduce risks of misuse and strengthen accountability mechanisms for its own selfish interests, which might endanger its populace. South Asia comprises 8 countries, as noted, yet these nations have varying laws. Certain nations implement AI-based regulations; others concentrate exclusively on human centred data protection; and a few, due to external instability, do not emphasise their legal frameworks.

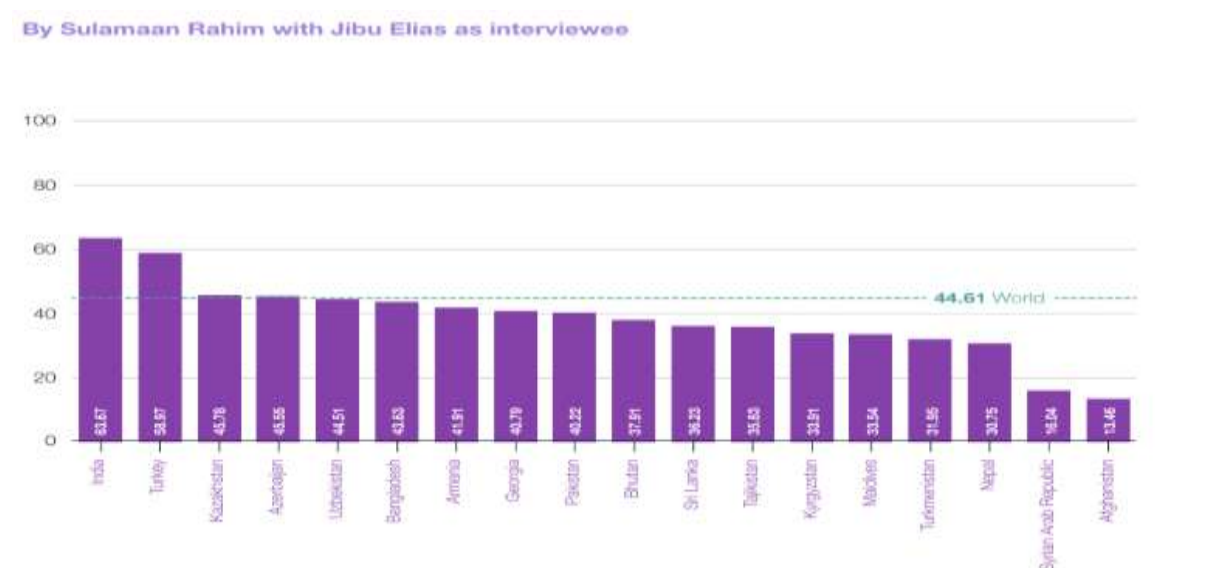
The Indian government issued various reports and policy documents. There is no law, but guidelines have been issued for AI governance and regulation- including sectoral work such as the Digital Personal Data Protection Act, 2023. Moreover, to protect individual data and information, India's AI mission has also issued a national strategy for AI. Rather than regulating the field, the Pakistani government seems concerned about emerging technologies. The main legislations and policies that concern the field of AI in Pakistan include the Personal Data Protection Bill 2021, the Prevention of Electronic Crimes Act 2016, and the National Artificial Intelligence Policy. (Mohanty, 2026).

The ICT Division of Bangladesh has released a revised and updated Bangladesh National Strategy for AI in 2023, which also has positive effects of AI on the country's economy, education, agriculture, and trade. (Hasan, 2024). Moreover, the paper briefly mentions ethical AI and protection against AI-enabled cyber threats. The Nepali government's Digital Nepal framework, launched in 2019, is a five-year initiative that promotes cooperation and develops initiatives. The government also needs a National Cyber Security policy for 2023

and early-stage AI governance. The only explicit legislation addressing AI in Bhutan is the Information, Communication & Media Act of Bhutan of 2018.

Also in 2023, the Bhutan government introduced the Data Protection Act of Bhutan, which aligns with the ethical use of AI and promotes national happiness. A personal data protection regime was implemented in the Maldives in 2022, along with digital governance and cybersecurity regulations. Yet, the country has no overarching legislative framework. Afghanistan (Hasan, 2024) Moreover, the political instability there has left no discernible AI policy, framework, or strategy in place by the Afghan government. As per the Oxford Insight AI Readiness Index 2022, India ranked 32nd among the 181 countries surveyed; Pakistan 90th; Bangladesh 80th; Nepal 139th; Sri Lanka 105th; Bhutan 99th; and Afghanistan 181st (Hasan, 2024). Digitalisation in SAARC nations can be achieved through collective efforts rather than nation-specific policies; there should be joint and collective norms for AI. Also, in the spheres of Ethical AI, data governance, algorithmic accountability, and cross-border digital cooperation. Also have to focus on individual Development in Digital Literacy upliftment.

Figure 1: South Asia Digital Readiness Source —



Oxford Insights (2022). *Government AI Readiness Index 2022*. Malvern: Oxford Insights
Retrieved March 07, 2025, from https://staging2.oxfordinsights.com/wp-content/uploads/2023/11/Government_AI_Readiness_2022_FV.pdf

3.4 Navigating the uneven digital literacy & digital divide in South Asia.

After the COVID-19 pandemic, the Rapid Digital Transformation is worldwide, but reliance on digital equipment and the internet has increased. Countries like India, Bangladesh, Sri Lanka, Nepal, Pakistan and Bhutan are undergoing rapid digitalisation through e-governance, digital financial services, online education and growing internet connectivity. Also, because education in South Asian nations relies on digital modes, the need for digital literacy is greater in such settings. Also, digital culture enhances digital education. The collective mindset values and organisation shape how institutions embrace digital technologies. In digital culture, the supportive factors such as forward-thinking leadership, student engagement and the institution's buy in are not so abundant (Fietz, 2023) Leadership plays a key role in propelling digital transformation by setting priorities for the institution, securing funding for them, and framing policies that favour digital literacy. Faculty engagement is also an important tool for successful transformation and change, helping implement at the institutional level.

At the institutional level, training and certification programmes have been introduced to enhance educators, and they have also been provided with digital equipment to help develop digital literacy skills. Also, the last pillar for change in the literacy sector, institutional support, students in South Asia have shown high adaptability, though institutions also have digital infrastructure and learning resources. Also, a world change in digital or online learning resources. There is strong policy support across all countries, and digital literacy implementation is also high, with internet penetration rates varying across the region: Nepal at

51.3% and the Maldives at 85.8% (Fietz, 2023). If the infrastructure and support policy were not there, then there would be no support for Digital Literacy. The first step is developing a culture of digital literacy; then there is infrastructure and technology adoption, and investment in digital infrastructure. India's institutions lead with significant advancement. In Bhutan, the internet bandwidth reflects the government-led efforts to enhance infrastructure (Mammen, 2025). Nepal and Pakistan face significant challenges, including limited resources and limited adoption. Sri Lanka has made notable progress in digital services, although challenges remain in achieving nationwide digital inclusion. (Mammen, 2025).

Advanced technologies such as AI and data analytics remain in their nascent stages across these countries. India's universities in Kerala and Maharashtra illustrate its early knowledge. Sri Lanka's use of Analytics to monitor student engagement makes a step towards being data-driven. Bhutan's innovations and hackathons encourage creativity. In the context of Nepal, the adoption of advanced educational technologies. The SAARC institution has been established in educational institutions such as the South Asian University, where a techno-driven environment has been prioritised. However, individual countries should also increase and promote tech-driven education and courses. Now, in South Asia, digital literacy is being prioritised, with a focus on education and literacy, but the digital South Asia faces its own challenges across different regions. South Asia geography is very diverse in nature.

As a result, uneven access to technological transformation can contribute to digital divides. Geographical terrain is one factor, as some South Asian countries have Himalayan terrain. Also, the gender perspective, like women facing issues in accessing technology, is a factor. Age is also a factor in the digital divide, as is the urban-rural divide. (Mohammad, 2024), These inequalities restrict the ability of large parts of the population to fully harness the potential of digital technologies, particularly between urban and rural areas, between men and women. Between different socio-economic groups, basically the urban population has easily

access to mobile, connectivity, technology, rapid digitalisation, and innovation easily, but the rural population faces serious difficulty accessing technology and innovation due to difficult terrain and lack of knowledge (Mohammad, 2024), also due to this social factor come in the digital divide vulnerable section is also facing problem related to innovation but digital technology has immense potential to enhance development in various sector like manufacturing, Agriculture technology, etc.

Moreover, their telemedicine service has linked remote communities to doctors in city locations. It reduced the distance to consultation and bridged gaps in healthcare, providing better healthcare services in underprivileged areas (Mohammad, 2024) There have been several hindrances to technological advancement in South Asia, despite the opportunities presented by the internet. Lack of infrastructure in remote and underprivileged regions has been the leading hindrance, coupled with regulatory constraints, linguistic variation, and varying levels of technology adoption and development within each country. Data privacy, cybersecurity and digital rights issues are also concerns in the regions.

To solve these issues, intervention from governments, private companies, civil society, and local communities is required, including engagement through different types of diplomacy, such as Track II, III, and IV. Track I - government-to-government relations, Track II - informal or non-government, Track III - people-to-people diplomacy and Track IV - conducted through Business and commercial actors. Although technological advancement can lead to both challenges and opportunities, dependence on external technologies in this interconnected world would surely pose a serious danger to national security (Abdurahmanlı, 2021). The governments in South Asia need to focus on educating their citizens in digital literacy, integrating digital education in schools, training teachers, and providing affordable Internet access to enable inclusion and shrink the digital divide.

3.5 Impact of External Power and its Technological Influence in the SAARC Region.

From a geopolitical perspective, the South Asian area became significant to foreign regional and global entities because of its low-cost labour, extended working hours, and advantageous circumstances for industrial manufacturing. The US's intent to counter China in the Asia Pacific and the influence of the US and China on other South Asian countries extend beyond military and economic terms to include technological ones. Also, the regional reliance on AI or generative AI like ChatGPT, Gemini - US dominated origin and DeepSeek and other AI debuts of Chinese origin, which is purely in use worldwide, especially influencing the population of South Asian nations. In telecommunications and satellite systems, technological transformation took place worldwide. However, its effects are limited because many countries are unable to develop certain technologies in the short term, and the urgent use of tech creates additional technological dependence on external or techno-driven nations such as China, the United States, and Europe.

Chinese technology has multiple interests in the region: Advancing digital infrastructure, facilitating telecommunications sharing, leveraging technological expertise, fulfilling China's national interests, shaping geopolitical strategies, and enhancing the reliability of South Asian nations in digital and trade matters. Countries like Pakistan, Bangladesh, the Maldives and Nepal have been influenced by Chinese investment, which has contributed to telecommunications, modernisation and smart city initiatives (Pal, 2021). It also leads to strategic vulnerability for reciprocal competition between China and other external powers, particularly the US and India.

The dominance of the Chinese in the region is through infrastructure and technology. The explanation of the Chinese companies influences through the case study of Huawei's 5G Expansion in South Asia, with the help of its Digital Silk Road and Belt and Road Initiative,

Huawei has penetrated several South Asian markets through affordable telecommunications infrastructure and a fibre-optic network, and has even introduced 5G technology (Tekir, 2020). The South Asian countries, which had been suffering from poor digital infrastructure, saw Huawei as a means of rapid digitalisation and increased connectivity. In particular, Pakistan, Bangladesh, the Maldives, and Nepal benefited greatly from Chinese investment in telecommunications infrastructure and digital modernisation. On the other hand, Huawei's activities put South Asian countries in a position where they had to consider the geopolitical implications of their economic development (Tekir, 2020). While China was promoting digital connectivity and technological cooperation, the USA was expressing concerns about cybersecurity, data governance, and its strategic dependence on the Chinese technological sector. Thus, South Asian states were forced to think not only economically but also geopolitically to access technology during competition (Bukhari., 2025). In this case, digital infrastructure in South Asia is no longer an exclusively economic problem but a geopolitical one. Hence, the key question for South Asian states is how to balance the benefits of foreign investment in their digitalisation with their digital sovereignty and cybersecurity.

The US has adopted a different approach to technological influence in South Asia, emphasising innovation, digital governance, cybersecurity cooperation, AI, and investment. American tech companies like Google, Microsoft, Amazon, and Apple have a deep influence on the daily practices and use of South Asians, creating an external digital ecosystem for them (Bukhari., 2025). American tech firms are making significant contributions to the software development and digital services sectors, and Debates continue regarding the balance between open internet principles, data governance, and privacy protection. In the broader digital ecosystem. The US aims to develop techno-strategies and offer an alternative to Chinese technological influence. This alternativeness in South Asia has become the ground for techno

rivalry between the US and China. (Bukhari., 2025). The impact of digital infrastructure can lead to both beneficial and disadvantageous outcomes for South Asian (SAARC) nations.

In the case of broadband internet networks, fibre-optic communication, satellite communication, and digital public infrastructure, it facilitates international trade, e-business, and financial inclusion, and offers assistance in various fields. The downside is that it threatens to reduce states' digital sovereignty, place data under external control, and lead to data breaches, cyberattacks, and espionage. Also, external threats, breaches of confidential data, and threats to the country's national interest. Support for external influence in the South Asian region, exemplified by the Chinese company Huawei's 5G technology, helped advance the BRI, China, and the development of digital infrastructure in the region (Tekir, 2020).

The external influence of other powers becomes an important factor in contemporary South Asian geopolitics. For a region like South Asia. Excessive reliance on external technologies may create strategic dependencies and vulnerabilities. Ultimately threatening digital sovereignty and strategic autonomy. Due to the threat of external digital dependence, the region needs to build an indigenous network, increase cooperation to develop telecommunications-related technologies, account for digital culture and digital autonomy, and develop national strategies to address cyberattacks.

3.6 From Vision to Reality: Policy Recommendation & Future of Digital Cooperation in SAARC.

The realisation of digitally integrated South Asia requires moving beyond declarations and fragmented national countries towards a coordinated regional digital cooperation framework. SAARC countries have the potential to transform themselves into a digital Cooperation for economic growth, social inclusion, and addressing disparities in infrastructure, regulatory systems, and digital skills (Bank, 2022). The transition from vision to reality

depends on a comprehensive strategy that combines policy, digital trade, regional integration, and digital cooperation, which becomes a central pillar of South Asia's regionalism. (UNESCAP, 2017). The primary recommendation is to develop the SAARC digital cooperation framework that focuses on collaboration in digital governance, cybersecurity, data protection, data trade & emerging technologies, and digital literacy. Countries such as India, Bangladesh, Sri Lanka, and Nepal are developing individual country digital policies, which creates regional fragmentation due to the absence of regional regulation on digitalisation. A common framework would facilitate cross-border digital services and improve trust among SAARC nations.

The SAARC should prioritise digital infrastructure, including joint regional satellites for GPS and telecommunications, such as the SAARC Satellite, launched on 5 May 2017, for communication and meteorological purposes (Graham, 2017), thereby enhancing connectivity and cooperation in digital communications. As part of a SAARC initiative to counter cyber threats, the establishment of the SAARC Cyber Crime Monitoring Desk (SCCMD) is proposed to facilitate intelligence sharing, coordinate law enforcement efforts, and collectively combat cyber threats (SAARC, 2014). SCCMD was established, but it was not sufficient to meet current global requirements. The monitoring of cybercrime should also include fighting together against external malware attacks and misinformation. A regional cybersecurity framework could facilitate information sharing and provide an incident response handbook to prevent and coordinate against cyber threats.

To enhance digital security, there should also be a focus on digital literacy and on addressing the skills gap, SAARC should establish a regional digital skills initiative. There should also be a focus on the impacts of digitalisation on human mental health. As SAARC's primary focus broadens beyond physical health, such as HIV & AIDS, there should be emphasis on mental health as well, thereby supporting digital skill development. Techno driven

governance has boosted the use of AI, fintech, blockchain, cloud computing, and digital public infrastructure to support cyber governance and digital transformation, thereby also leading to digital Sovereignty. In this regard, a deep cooperation will be promoted to encourage integration, increase trust among members, decrease political friction, promote commercial exchange and strengthen social relations, thus revitalising the wider SAARC Integration Agenda (UNESCAP, 2017)

CHAPTER IV: CONCLUSION

South Asia is on the threshold of its digital evolution. The sheer growth in the application and deployment of AI technology across all SAARC member countries carries both significant potential to bring about transformational changes and significant structural risks. This paper proposes creating a regional platform based on regional ownership to effectively manage the SAARC region's digital evolution. The first step was to identify the relevant issues and to prove that the technology should be used in a manner that is responsible and just. Given that the systems based on artificial intelligence have already begun being embedded in many fields, including healthcare, administration, financial and security sectors, it is imperative for the SAARC region to come up with some guiding principles to avoid recurrence of algorithmic bias and surveillance, as well as various other problems associated with non-regulated behaviour.

The degree of digital evolution among countries in South Asia is highly uneven, as assessed by studies of digital transformation in the region, with India and Bangladesh as the leading and most digitally advanced countries, while countries like Afghanistan, Nepal, and Bhutan suffer due to limitations in institutional capacities and connectivity infrastructure. Cybersecurity is of great concern. From trans-national attacks to ransomware, cyber espionage, to the propagation of disinformation, cyber issues know no boundaries. And with ad-hoc

country-specific policies, the SAARC region becomes vulnerable. An efficient SAARC Cyber Crime Monitoring Desk and a mutual incident response mechanism could take us a long way in this regard. The impact of external players and geopolitics on our path should not be undermined. The competition between the US and China is unfolding across our technological landscape and will further compromise our digital sovereignty and strategic autonomy in the absence of a proactive regional response. In a nutshell, this research-based framework is far from utopian or unrealistic, countries such as the European Union and the Association of Southeast Asian Nations are already working towards providing a harmonised framework for digital infrastructure and governance. Given the potential and the available infrastructure in SAARC, we must endeavour to construct a similar framework for the South Asian region.

REFERENCES

- i. Abdurahmanlı, E. .. (2021). DEFINITION OF DIPLOMACY AND TYPES OF DIPLOMACY USED BETWEEN STATES. *Anadolu Üniversitesi Sosyal Bilimler Dergisi.*, 3, 580-603.
- ii. Arshard, A. &. (n.d.). *DIGITAL INNOVATION AND IMPLEMENTATION OF FINTECH ON BANKING AND FINANCIAL SECTOR IN SRI LANKA*. <https://zenodo.org/records/10578923>
- iii. Bank, W. (2022). *South Asia's Digital Opportunity: Accelerating Growth, Transforming Lives*. WORLD BANK.
- iv. Britannica., E. (2025). *Nepalese Gen Z Protests | Background, Social Media Ban, & .* https://www.britannica.com/event/2025-Nepalese-Gen-Z-Protests_Political-Breakdown
- v. Bukhari., D. S. (2025). South Asia's Power Play: Pakistan, India, China, and the USA in Strategic Relations. *Advance Social Science Archive Journal*, 4(01), 111–122. .
- vi. *DeepSeek Terms of use*. (n.d.). DeepSeek. <https://cdn.deepseek.com/policies/en-US/deepseek-terms-of-use.html>
- vii. Digital Governance and Artificial Intelligence AI ehics in Public Adminsiattration. (2026). *Journal of Political Science and leadership Reserach*, 12 no.3, 64-72. <https://doi.org/10.56201/jpslr.vol.12.no3.2026.pg64.72>
- viii. Erhirhie, B. (2026). Digital Governance and Artificial Intelligence AI Ethics in Public Administration . *Journal of Political Science and Leadership Research*, Vol. 12 No.3, .pg64.72. <https://doi.org/10.56201/jpslr.vol.12.no3.2026>
- ix. Fietz, K. &. (2023). Digital skills in the global South: Gaps, needs, and progress. *GIGA Focus global*, 13. <https://doi.org/https://doi.org/10.57671/gfgl-23022>
- x. Graham, W. (2017). *India's GSLV rocket successfully launches GSAT-9*. . NASASpaceFlight.com. . <https://www.nasaspaceflight.com/2017/05/indias-glsv-gsat-9-launch/>

- xi. Gusarova, Svetlana & Gusarov, Igor & Smeretchinskii, Margarita.. (2023). Digital Transformation of the South Asia Region: Challenges and Prospects. *E3S Web of Conferences.* , 403. <https://doi.org/10.1051/e3sconf/202340306016>.
- xii. Hasan, M. .. (2024). Regulating artificial intelligence: A study in the comparison between south asia and other countries. *Legal Issues in the digital Age*, 5 (1), 122-149. <https://doi.org/DOI:10.17323/2713-2749.2024.1.122.149>
- xiii. Iqbal, S. &. (2024). Digital Strategic Autonomy in South Asia: Artificial Intelligence and Cyberspace. . *Journal of Security & Strategic Analyses.*, 10, 72-86. <https://doi.org/10.57169/jssa.0010.01.0300>.
- xiv. Mammen, A. (2025). *digital transformation in higher education in South Asia*. UNESCO Office Bangkok and Regional Bureau for Education in Asia and the Pacific.
- xv. Mohammad, H. &. (2024). *Navigating the Digital Divide: Empowering Marginalized Communities in India and South Asia*". Research GATE.
- xvi. Mohanty, A. (2026, january). *AI Governance in South Asia Shared Priorities, Challenges & Future Trajectories*. center for responsible AI, IITM. <https://cerai.iitm.ac.in/docs/AI-Governance-In-South-Asia.pdf>
- xvii. Natarajan, A. and Murali, V. S. (2020). *Regulating Artificial Intelligence in South Asia: Projections for the Future*. . Institute of South Asian Studies (ISAS) & Konrad-Adenauer-Stiftung (KAS).
- xviii. Othman, A. (2025). *The Foundations and Challenges of AI Ethics*. ResearchGate.
- xix. Pal, D. (2021). China's influence in South Asia: Vulnerabilities and resilience in four countries. *Carnegie Endowment for International Peace*.
- xx. SAARC. (2014). *SAARC 18TH SUMMIT*. SAARC.ORG. <https://www.saarctb.org/the-18th-saarc-summit-2014-kathmandu-declaration/>
- xxi. Sadiq, M. &. (2022). Challenges of Nuclear Deterrence Stability in South Asia. *Journal of Asian Security and International Affairs*, 58(8), 1-20. <https://doi.org/https://doi.org/10.1177/00219096221090636>
- xxii. Tekir, G. (2020.). Huawei, 5G Network and Digital Geopolitics. *International Journal of Politic and Security*, 2. , 113-135.
- xxiii. UNESCAP. (2017). *Regional Economic Cooperation and Integration in South Asia*. United Nations publication .

