Emerging Technologies and the Threat to South Asian Security

Dr Summar Iqbal Babar[1] & Abu Hurrairah Abbasi[2]

The unprecedented advancements in new technologies – artificial intelligence, cyber, autonomous, and advanced conventional weaponry – are set to substantively transform the character of warfare and redefine South Asia's security landscape. Competition for technological dominance will increase the risks of pursuing regional stability. Hence, there is a need for comprehensive cooperation, including arms control measures, such as increased transparency, to prevent accidental or unintended escalation. This paper analyses the interplay between emerging technologies and security dynamics in South Asia through deterrence theory. Due to their intangible nature, inherent imbalances, and unpredictability, emerging technologies can introduce new and less predictable aspects to deterrence. This, in turn, would pose challenges to established conventional deterrence frameworks and alter regional security calculations. India is investing significantly in advanced conventional weaponry and deterrence capabilities, which will compel Pakistan to take necessary measures to maintain balance in South Asia. India's recent military modernization, featuring advancements in conventional weaponry, missile capabilities, and defense technologies, can reshape the regional power equilibrium. This study analyzes these transformations and offers insights for policy-makers and strategists navigating the challenges of current security paradigms in South Asia.

Keywords: South Asia, Emerging Technologies, Deterrence, Security, Artificial Intelligence, Autonomous Weapons, Cybersecurity.

Introduction

The world is currently undergoing the fourth industrial revolution (4IR) characterized by new forms of innovative and transformative technologies.[3] Technology has consistently brought about profound changes in warfare and the strategic mindset of the militaries. A link exists between geopolitical conditions and technological advancement, which undermines the effectiveness of warfare at the tactical, operational, and strategic levels. Past doctrines and techniques seem outdated. Technological advancement not only causes the destabilization of deterrence and the

[1] Dr Summar Iqbal Babar is Assistant Professor at the School of Politics and International Relations (SPIR), Quaid-i-Azam University (QAU), Islamabad.
[2] Abu Hurrairah Abbasi is a graduate of SPIR, QAU, Islamabad.
[3] Evron, Yoram. Bitzinger, Richard A. "The Fourth Industrial Revolution and Military-Civil Fusion: A New Paradigm for Military Innovation?" Cambridge University Press, 2023.

survivability of the nuclear force but also impinges upon geopolitical factors and the ambitions of states driven by their desire for status. These factors encourage states to incorporate these technologies into their current arsenal to gain an advantage.

The emerging technologies are disruptive in nature because they seek to alter the existing state of affairs in their favor once deployed on the battlefield. There are concerns that advancements in Artificial Intelligence (AI) could undermine the basic principles of nuclear deterrence by allowing targeted strikes against hidden and movable nuclear forces. Contemporary studies indicate that these disruptive technologies can potentially weaken the foundations of deterrence, ultimately compromising deterrence stability by impacting nuclear second-strike capability, including command, control, communication, computers, intelligence surveillance and reconnaissance (C4ISR), and force postures.

The effect of disruptive emerging technologies on nuclear deterrence is directly linked to their ability to be put into operation and understanding the military positions of the states they may be used against. Technological advancement has heightened the susceptibility of nuclear forces by instilling assurance in the party that takes the initiative, thus amplifying the likelihood of a preemptive strike to disarm the opponent during a crisis. Alongside, leaders who are concerned about being attacked with nuclear weapons may opt to initiate a nuclear strike before their weapons are taken away.[4]

Furthermore, emerging technologies increase the risk of unintentional or unplanned nuclear escalation. This is due to the vulnerability of dual-purpose command and control assets in outer space and cyberspace. Also, these technologies pressurize decision-makers to choose nuclear use due to a mistaken conviction that an adversary is about to launch a nuclear assault. Within this framework, emerging technologies that have the potential to erode strategic stability and affect deterrence include AI, hypersonic weapons, AI-enabled Lethal Autonomous Weapons Systems (LAWS), drones, and cyber technologies.

The widespread application of AI in the nuclear domain poses challenges related to the potential for accidental or intentional nuclear missile launches. The intricate technical limitations and complexities in designing automated intelligent weapon systems make prevention nearly unattainable. While AI and machine learning (ML) are crucial for advancing conventional force deployment against high-value assets, reliance on AI-powered nuclear weapons or missile defense systems is deemed risky due to susceptibility to cyberattacks. Historical incidents, like the Soviet missile alert in 1983,[5] highlight the potential for technical errors leading to catastrophic outcomes, emphasizing the importance of human involvement in decision-making to prevent nuclear disasters. Prolonged conflicts will incentivize utilizing autonomous systems early to gain a strategic advantage and prevent the other from doing so.

---

[4] Bell, Mark S. "Nuclear Reactions: How Nuclear-Armed States Behave." Cornell University Press, 2023. https://library.oapen.org/handle/20.500.12657/62033.

[5] Forden, Geoffrey. "Reducing a Common Danger: Improving Russia's Early-Warning System." Cato Institute, 2001.

Undoubtedly, over more than two decades, the presence of a nuclear deterrent has resulted in a stabilizing impact at the strategic level in South Asia. Both the arch-rivals effectively averted significant conflicts as a result of nuclear deterrence. Nevertheless, introducing new technologies can change the dynamics and nature of warfare in situations where a war may start either inadvertently or accidentally.[6] Instead, technologically enabled smart wars could become strategically advantageous and permissible.

The aspirations of powerful nations, such as the United States and China, to create innovative technologies to maximize security benefits would significantly impact South Asia's strategic stability. Also, the foundational technological agreements between the US and India shall increase Pakistan's security dilemma. In this scenario, India's pursuit of disruptive technological strategies has the potential to vitiate the strategic landscape of South Asia. Given the evolving global and regional political systems, the increasing technological progress in India and the necessary changes in its military strategy challenge the stability of deterrence in South Asia. [7]

This paper primarily examines the future military potential of these emerging technologies, which could upset the current state of affairs and undermine the stability of deterrence[8] and the foundation of nuclear deterrence between Pakistan and India.

Artificial Intelligence: Reshaping South Asian Security Landscape

AI and ML are transformative advancements, significantly shaping the contemporary global strategic landscape. AI encompasses programming, computer systems, and software capable of executing tasks that traditionally require human intelligence. AI's versatility extends to efficiently categorizing vast datasets, enhancing intelligence, surveillance, and reconnaissance capabilities, and facilitating the identification of enemy units.

ML, a subset of AI, focuses on training algorithms to recognize patterns in extensive datasets and refines learning through feedback mechanisms, rewarding the program for practical actions.[9] The synergy of AI and ML presents a dynamic and multifaceted force in modern technological domains.

AI-driven weaponry can be categorized as autonomous or automated.[10] Autonomous systems operate with varying levels of independence, ranging from limited autonomy, where tasks follow predetermined norms, to total autonomy, with no restrictions. Tasks executed by AI can be broadly

---

[6] Gervais, Victor. "Emerging Technologies and the Future of Warfare." Trends Research & Advisory, 2021.
[7] Ali, Iftikhar. S Sidhu, Jatswan. "Strategic Dynamics of the Arms Race in South Asia." Journal of Asian and African Studies, 2023, 00219096231153150.
[8] Johnson, James. "Deterrence in the Age of Artificial Intelligence & Autonomy: A Paradigm Shift in Nuclear Deterrence Theory and Practice?" Defense & Security Analysis 36, no. 4 (2020): 422–48.
[9] Johnson, James. "Artificial Intelligence & Future Warfare: Implications for International Security." Defense *& Security* Analysis 35, no. 2 (2019): 147–69.
[10] Ilachinski, Andrew. "Artificial Intelligence and Autonomy: Opportunities and Challenges." Center for Naval Analysis, 2017, 10–2017.

classified into these two groups. Autonomy is further divided into "at rest" and "in motion."[11] Autonomy-at-rest pertains to systems functioning within the software or virtual realm, while autonomy-in-motion involves systems engaging with the physical environment. An example of autonomy-in-motion is seen in LAWS. These weapons, once deployed, can actively search for and engage targets[12] within a specified operational zone without human intervention.[13]

Recently, states have started integrating AI into the military sector to gain a strategic edge over their adversaries. The rapid competition among states to integrate AI into military systems has intensified due to AI's unparalleled efficiency, heightened sophistication, and error-reduction capabilities. States see AI as a means to manipulate power distribution to their advantage.[14] Within South Asia, India actively strives to acquire AI-based technology without being left behind. India has been proactively advancing AI-based technology for military applications in recent years.[15]

India is a rapidly growing market for venture capital investment in AI-related technology, which is expected to reach USD 881 million in 2023 and can also contribute USD 500 billion to the gross domestic product (GDP) by 2025.[16] India's government has explicitly said that it considers the development of military AI crucial for its national security and strategic aspirations.[17]

During the commencement of the RAISE 2020 Summit, Indian Prime Minister Narendra Modi conveyed India's aspirations by asserting that India has been at the forefront of global knowledge and learning and will persist in surpassing expectations and impressing the world in the digital realm[18] – that India should establish itself as the epicenter of AI. Modi emphasized the use of AI for societal development and acknowledged India's awareness of the military applications of AI.[19]

The pursuit of AI by India, its subsequent use in the military sector, and its evolving strategic positions could potentially affect the stability of deterrence in South Asia. For instance, if India employs AI in nuclear command and control systems and BMD systems, the algorithm biases could lead to inadvertent use and pre-emptive strikes. The use of AI in such systems is bound to fail-deadly, not fail-safe.

---

[11] Blasch et al., Erik. "Autonomy in Use for Space Situation Awareness." vol. 11017 (Sensors and Systems for Space Applications XII, SPIE, 2019), 45–56.
[12] Hunter et al., Lance Y. "The Military Application of Artificial Intelligence Technology in the United States, China, and Russia and the Implications for Global Security." Defense & Security Analysis 39, no. 2 (2023): 207–32.
[13] Boulanin, Vincent. "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk." 2019.
[14] Johnson, "Artificial Intelligence & Future Warfare: Implications for International Security."
[15] Srivastava, Sunil Kumar. "Artificial Intelligence: Way Forward for India," JISTEM-Journal of Information Systems and Technology Management 15 (2018).
[16] "India GDP: AI Adoption to Add $500 Billion to India's GDP by 2025: Nasscom - The Economic Times." accessed December 14, 2023. https://economictimes.indiatimes.com/tech/technology/integrated-adoption-of-ai-and-data-utilization-can-add-500-billion-to-indias-gdp/articleshow/92412781.cms.
[17] "Implementing Artificial Intelligence in the Indian Military." December 14, 2023. https://www.delhipolicygroup.org/.
[18] "RAISE 2020 – Mega Virtual Summit on Artificial Intelligence to Be Held from October 5-9." December 14, 2023. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1658758.
[19] "RAISE 2020 – Mega Virtual Summit on Artificial Intelligence to Be Held from October 5-9."

The Indian Ministry of Defence (MoD) created the Defence AI Council (DAIC) in 2019 to offer strategic guidance for implementing AI in the military sector. India is forming a collaborative alliance between the industry and government to implement these technologies.[20] The AI Task Force[21] has diligently endeavored to build strategic advantage in the military domain. In that regard, India has already set up a Centre for AI and Robotics (CAIR) under the Defense Research and Development Organization (DRDO) to focus on AI applications in the defense industry. The objective is to facilitate the integration of AI into military systems, namely in the domains of net-centric systems for tactical command, control, and communication systems; intelligence systems and unmanned vehicles; and information security.[22]

As emphasized in the policy documents like the Joint Doctrine of Indian Armed Forces (JDIAF)-2017 and Land Warfare Doctrine (LWD)-2018, India is integrating advanced technologies into its military.[23] It is rapidly modernizing its military and incorporating advanced technologies to align with its offensive doctrines and counter its adversaries, driven by strategic objectives.

A multi-stakeholder task committee was established in March 2018 under the guidance of PM Modi and Defense Minister Rajnath Singh, which has been examining the application of AI in national security.[24] Multiple branches within the MoD currently employ AI products and technologies or are in advanced implementation stages.[25]

In January 2019, the then Indian Army Chief General Bipin Rawat advocated incorporating advanced technologies, like AI, into military systems. Likewise, the current Army Chief has reiterated that call and has even placed a high premium on fighting hybrid warfare.[26] He underlined the importance of focusing on domestic production and self-sufficiency in the defense industry and declared that India's opponent on the northern border was substantially investing in AI and cyber warfare, necessitating that India prioritize AI and big data analysis instead of limiting attention to mere definitions.[27]

---

[20] Rafiq, Aamna. "Militarisation of Artificial Intelligence and Future of Arms Control in South Asia." Strategic Studies 41, no. 2 (2021): 49–63.
[21] "Artificial Intelligence Task Force." December 14, 2023. https://www.aitf.org.in/.
[22] "Centre for Artificial Intelligence & Robotics (CAIR) | Defense Research and Development Organization - DRDO, Ministry of Defense, Government of India." December 14, 2023. https://www.drdo.gov.in/labs-and-establishments/centre-artificial-intelligence-robotics-cair.
[23] Mitra, Joy. "India's Land Warfare Doctrine 2018: Hoping for the Best, Preparing for the Worst." The Diplomat, January 3, 2019. https://thediplomat.com/2019/01/indias-land-warfare-doctrine-2018-hoping-for-the-best-preparing-for-the-worst/.
[24] Mishra, Abhinandan. "Indian Army Gets Future Ready with AI-Based Equipment." The Sunday Guardian Live (blog), July 16, 2022. https://sundayguardianlive.com/news/indian-army-gets-future-ready-ai-based-equipment.
[25] "Rajnath Singh Launches 75 Newly-Developed AI-Enabled Defence Products." Business Standard, July 12, 2022. https://www.business-standard.com/article/current-affairs/rajnath-singh-launches-75-newly-developed-ai-enabled-defence-products-122071200094_1.html.
[26] Kazmi, Dr Atia Ali. "Indian Grey Zone Aggression and Strategy of Conflict Prosecution." CISS. Indian Grey Zone Aggression and Strategy of Conflict Prosecution - CISS Pakistan.
[27] "Army Chief for Tapping AI, Big Data for Defence Forces." The Economic Times, January 21, 2019. https://economictimes.indiatimes.com/news/defence/army-chief-for-tapping-ai-big-data-for-defence-forces/articleshow/67620009.cms.

India is now developing the Multi-Agent Robotics Framework (MRF), which is expected to function as a group of soldiers to support the army. In addition, the army is equipped with approximately 200 Daksh Autonomous Robots.[28] This remotely operated vehicle (ROV) is used for deactivating explosive devices. These are the signs of advanced capabilities beyond the baseline and usable in advanced military systems.

India is also partnering with other states in AI-related domains. For instance, it is working with Japan on robotics and AI, specifically focusing on their use in military systems.[29] Similarly, India has been actively pursuing advanced applications of AI in the military domain. These tasks encompass analyzing images, identifying targets, determining the optimal distance for engagement, evaluating the effectiveness of missile kill zones, and employing robots in advanced configurations.

China has a significant lead in AI.[30] China and the US compete in AI. The final report on AI published by the US National Security Commission in 2021 characterizes China as a "formidable rival," if not a frontrunner, in terms of AI advancement.[31] Although the US has historically been at the forefront of AI research and business, China is rapidly narrowing the gap and, in certain domains, has surpassed its main competitors.

Using China and its cordial relations with Pakistan as a reason, India is currently making significant efforts to use AI in the military domain.[32] India has unveiled a new national program in its current budget to conduct research and development (R&D) in a so-called response to its neighbor's ambitions of becoming an AI superpower.[33]

India implemented a compellence policy against Pakistan in February 2019.[34] In response, Pakistan maintained its deterrence the following day. If India were to implement an independent system that relies on a compellence strategy, which entails the threat or restricted use of force, it would introduce a new level of escalation in the ladder, undermining the stability of deterrence in South Asia.

---

[28] "Daksh: India's Remotely Operated Vehicle - Explained." December 14, 2023. https://www.defencexp.com/daksh-remotely-operated-vehicle/.
[29] "India, Japan to Introduce AI, Robotics in Defence Sector." The Times of India, January 22, 2018. https://timesofindia.indiatimes.com/india/india-japan-to-introduce-ai-robotics-in-defence-sector/articleshow/62597018.cms.
[30] Zhang, Jiayu. "China's Military Employment of Artificial Intelligence." Christopher Kojm 38 (2020).
[31] "U.S. Unprepared for AI Competition with China, Commission Finds - Nextgov/FCW." December 14, 2023. https://www.nextgov.com/artificial-intelligence/2021/03/us-unprepared-ai-competition-china-commission-finds/172377/.
[32] Kania, Elsa B. "AI Weapons' in China's Military Innovation." Brookings Institution, April 2020.
[33] "India's AI Programme to Be Kinetic Enabler to Achieve $1 Trillion Digital Economy: Rajeev Chandrasekhar." The Times of India, October 13, 2023. https://timesofindia.indiatimes.com/india/indias-ai-programme-to-be-kinetic-enabler-to-achieve-1-trillion-digital-economy-rajeev-chandrasekhar/articleshow/104403787.cms?from=mdr.
[34] Fayyaz, Shabana. "Countering Strategic Coercion: A Case Study of Pakistan." *Margalla Papers* 23, no. 2 (2019).

AI can be utilized to generate deepfakes for disinformation operations, exacerbating a nuclear crisis at a swift pace[35] and destabilizing peace and security. Significant ethical and legal implications also exist.[36] South Asia has faced multiple crises. In the event of a future crisis, the dissemination of manipulated videos, audio, or images could result in disastrous consequences, especially if there is a lack of adequate communication channels between the two states. These applications have the potential to cause disturbance, particularly those that aim to challenge the secure second-strike forces or create increased escalatory threats. Hence, deepfakes provide a potential risk to deterrence stability in South Asia.[37]

As being done worldwide by major powers, AI is being introduced to the security calculus of South Asia. This is part of a comprehensive strategy to effectively utilize and incorporate these cutting-edge developments to gain a competitive advantage. AI can influence the coercive techniques and dynamics of conflict in South Asia. The utilization of AI-based technologies can potentially impact deterrence through their rapid information processing and swift decision-making capabilities, which may inadvertently lead to an escalation of tensions, especially within the strategic context of South Asia.

Hypersonic Weapons in South Asian Security Dynamics

Numerous countries are now investigating the use of ML to create control systems for hypersonic vehicles. The utilization of hypersonic technology poses an escalating risk to current nuclear systems due to its ability to transport both conventional and nuclear weapons at a velocity five times greater than the speed of sound. Powerful states are developing maneuverable hypersonic vehicles that can potentially evade existing missile defense systems.[38]

Currently, two categories of hypersonic weapons are being manufactured: hypersonic glide vehicles (HGVs) and hypersonic cruise missiles (HCMs).[39] The consequences of HGVs and HCMs are frequently mentioned as significant obstacles to nuclear stability.

Firstly, they can be equipped with nuclear warheads and employed to circumvent an opponent's missile defense systems. Furthermore, they can be utilized for extended-range, non-nuclear pinpoint attacks, enabling the execution of disarmament operations against nuclear forces. Hypersonic weapons possess advanced guidance systems and exceptional precision, rendering them potentially well-suited for non-nuclear precision attack operations. In a crisis, it would be

[35] Favaro, Marina. Williams, Heather. "False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation." Journal for Peace and Nuclear Disarmament 6, no. 1 (2023): 28–46.
[36] Kazi, Reshmi. "Nuclear Security in Asia: Problems and Challenges." Strategic Analysis 39, no. 4 (2015): 378–401.
[37] Rickli, Jean-Marc. "The Strategic Implications of Artificial Intelligence for International Security." Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications, 2020, 41.
[38] Johnson, James. "The Fast and the Furious: Drone Swarming and Hypersonic Weapons." in Artificial Intelligence and the Future of Warfare (Manchester University Press, 2021), 128–49.
[39] Noone, Emily. Harriss, Lydia. "Hypersonic Missiles." January 1, 2024. https://post.parliament.uk/research-briefings/post-pn-0696/.

uncertain if the warheads and the intended target were equipped with nuclear weapons or conventional explosives, which would impact operational methods and the principles outlined in official doctrines.

The concept revolves around the notion that the precision of delivery systems and the transparency of sensors in detecting, tracking, and engaging targets have reached such a level that safeguarding and hiding weapon systems has become ever more complex. The contention is that nuclear forces, traditionally perceived as capable of enduring nuclear deterrence, have become increasingly susceptible.

In September 2020, India asserted that it had tested a domestically produced hypersonic weapon.[40] It will provide a stable basis for constructing a hypersonic missile. India has become the fourth state after the US, China, and Russia to possess this advanced technology. Rajnath Singh described the test as a significant milestone in the journey toward self-sufficiency. He declared that it was appropriate to advance to the next stage, as all crucial technologies have been established through the successful flight test, utilizing the domestically created scramjet propulsion system.[41]

The lethality of hypersonic missiles stems from their exceptional velocity and post-launch maneuverability. Notably, the missile possesses the ability to breach missile defense systems as a result of its exceptional velocity and agility. The Indian hypersonic weapon is propelled by a scramjet engine, which achieves a velocity of Mach 6, equivalent to six times the speed of sound. In addition, the DRDO is currently developing BrahMos-II, a hypersonic cruise missile, with Russia's assistance. BrahMos-II is likely engineered to achieve a velocity of Mach 6 by utilizing hypersonic scramjet technology.[42]

Pakistan faces substantial security vulnerabilities because of India's inclusion in the hypersonic club. This technological breakthrough will augment India's capabilities in ballistic missiles. The hypersonic weapon will bolster India's capacity to target Pakistan's military installations with remarkable accuracy and precision. The remarkable speed and maneuverability of the missile allow it to bypass Pakistani missile defense systems easily.

The hypersonic missile system poses significant challenges to the logic behind nuclear deterrence. Although speed remained a crucial element in war, the introduction of hypersonic weaponry provided unprecedented benefits, such as the remarkable maneuverability of the missiles. This greatly diminishes the amount of time nuclear weapon states have to respond, compelling them to rely on pre-emptive strikes.

---

[40] "India Tests Hypersonic Missile, Arms Control Association." Arms Control Association, December 14, 2023. https://www.armscontrol.org/act/2020-10/news/india-tests-hypersonic-missile.
[41] "India Successfully Test Scramjet Technology for Hypersonic Missiles." The Times of India, September 8, 2020. https://timesofindia.indiatimes.com/india/india-successfully-test-scramjet-technology-for-hypersonic-missiles/articleshow/77973889.cms.
[42] Ali, Samran. "Assessing the Implications of India's Hypersonic Technology Test for Pakistan." Centre for Strategic and Contemporary Research (blog), September 11, 2020. https://cscr.pk/explore/themes/defense-security/assessing-the-implications-of-indias-hypersonic-technology-test-for-pakistan/.

The rapid velocity and nimbleness of hypersonic technology have rendered missile defense ineffective in both the present era and the foreseeable future. The malfunction of the missile defense system, coupled with the decreasing response time, may encourage nuclear weapon states to carry out a preemptive strike. Notably, when countries with nuclear weapons cannot withstand a retaliatory attack, the stability of deterrence becomes highly uncertain.

Hypersonic weapons intensify the blurring of the distinction between conventional and strategic categories of weaponry. The distinction between a hypersonic weapon equipped with a conventional warhead and one armed with nuclear capabilities is not possible, and the uncertainty can invoke a "launch under attack" response, where the target state can launch a nuclear strike against the hypersonic cruise or glide vehicle. Hence, the utilization of the hypersonic missile system in both military and civilian capacities heightens the potential for nuclear escalation in South Asia. Armed with hypersonic missiles, India's pre-emptive urge is likely to increase, which will heighten nuclear risk and increase strategic instability.

Cybersecurity Risks in the Digital Age

The utilization of AI-based technologies and autonomous weapon systems, specifically in the nuclear field, suggests a significant increase in the prevalence of information security, data security, network security, and cybersecurity issues. Cyberspace is characterized by unparalleled disruptive and destructive capabilities, making it one of the most intricate and hazardous warfare areas in contemporary times. The US, China, Russia, the UK, and Israel are widely regarded as the frontrunners in their active cyber capabilities for offensive and defensive activities.[43] Stuxnet is widely recognized as the first cyber weapon to be made known to the public. This is a highly potent computer worm that has been created explicitly by the intelligence agencies of the US and Israel to incapacitate a critical component of the Iranian nuclear program.[44]

The utilization of cyber operations in the conflict between Russia and Ukraine has sparked inquiries and shed light on the ever-changing landscape of cyber warfare, providing valuable insights into the contemporary nature of this warfare. Following the use of cyber warfare in the Russia-Ukraine conflict, the importance of cybersecurity has significantly increased for states, enterprises, and critical infrastructure operators.[45] The immense destructive capacity of cyber warfare has elevated it to the status of a distinct domain in military strategy, alongside air, sea, land, and space. Major global powers, including the US, China, and Russia, are adjusting their strategic doctrines and engaging in fierce competition to obtain cyber weapons and assess their counterparts' cyber capabilities and defenses.

---

[43] Breene, Keith. "Who Are the Cyberwar Superpowers." World Economic Forum, May 4, 2016. Who are the cyberwar superpowers? | World Economic Forum (weforum.org).
[44] Danks, David. Danks, Joseph H. "Beyond Machines: Humans in Cyber Operations, Espionage, and Conflict." 2015.
[45] Bateman, Jon. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." 2022.

South Asia is subject to this trend, primarily because India aspires to attain technological supremacy in cyberspace. India's information technology industry, as reported by the Indian National Association of Software and Service Companies (NASSCOM), achieved a revenue of USD 227 billion in the fiscal year 2022, marking a growth rate of 15.5 percent.[46] On India's independence day, PM Modi said that the country would unveil a novel cybersecurity policy. India is actively striving to attain the status of a global power, and specifically, establishing supremacy in cyberspace within South Asia is a key component of its overarching goals.[47]

India has developed a substantial cyber warfare capability directed at Pakistan, involving malware assaults and espionage activities. Pakistan's defensive capabilities are not as substantial. Recently, there has been a notable increase in cyberattacks targeting Pakistan.[48] Approximately one million cyberattacks were recorded in Pakistan's online domain between January and November 2021.[49]

Pakistani intelligence authorities uncovered an Indian spy network cyberattack to target Pakistan's armed forces and government leaders. Pakistan had detected a significant cyberattack conducted by Indian intelligence agencies.[50] This attack encompasses various cybercrimes, such as the false manipulation of government officials and military personnel's personal mobile devices and technical equipment through hacking.

A form of malicious software called Pegasus was utilized between April and May 2019.[51] This virus impacted almost 1400 high-ranking government and military officials in 20 states, including Pakistan. In this regard, Pakistan has contacted the management of WhatsApp to obtain user information supposedly targeted by Israeli spyware (NSO Group) and to receive guidance on preventive measures to prevent future hacking events.[52]

India is the leading purchaser of weaponry manufactured in Israel,[53] including cyberspace technologies. Both have signed a memorandum of understanding to strengthen collaboration in cybersecurity, aiming to address the potential issues resulting from the rapid digitization brought about by the Covid-19 pandemic. This Israel-India partnership may evolve into significant

---

[46] "Aatmanirbhar Bharat - The Need for Digital in India | HSC." December 14, 2023. https://www.hsc.com/resources/blog/aatmanirbhar-bharat-digital-india-initiative/.
[47] Bhardwaj, Ananya. "India to Get New, 'robust' Cyber Security Policy Soon, Says PM Modi." The Print (blog), August 15, 2020. https://theprint.in/india/india-to-get-new-robust-cyber-security-policy-soon-says-pm-modi/482356/.
[48] Babar, Summar Iqbal. Mirza, Muhammad Nadeem. Qaisrani, Irfan Hasnain. "Evaluating the Nature of Cyber Warfare between Pakistan and India." Webology 18, no. 6 (2021): 6973–85.
[49] "Cyber Security Challenges and Response." The Express Tribune, November 6, 2021. https://tribune.com.pk/story/2328017/cyber-security-challenges-and-response.
[50] "Inter-Services Public Relations Pakistan." December 14, 2023. https://www.ispr.gov.pk/press-release-detail.php?id=5806.
[51] Pegg, David. Cutler, Sam. "What Is Pegasus Spyware and How Does It Hack Phones?" The Guardian, July 18, 2021.https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.
[52] Nishat. "WhatsApp Attacks: Pegasus Spyware Hacks 1400 Users." Open Access Government (blog), October 30, 2019. https://www.openaccessgovernment.org/pegasus-spyware-3/76933/.
[53] "India & Israel to Co-Develop Hi-Tech Weapon Systems." The Times of India, September 26, 2020. https://timesofindia.indiatimes.com/india/india-israel-to-co-develop-hi-tech-weapon-systems/articleshow/78327521.cms?from=mdr.

alliances in cyberspace. The former is seen as a dominant force in the global competition of cyber warfare, while the latter benefits greatly from its sophisticated cyber capabilities. Hence, the escalating intricacies of the online realm coupled with India's procurement and subsequent utilization of its aggressive cyber capabilities have posed a significant threat to Pakistan's cybersecurity.[54]

Pakistan prioritizes its security measures to address the challenges arising from emerging technologies in a complex environment. However, cybersecurity is considered an issue that needs to receive more attention. According to a survey, Pakistan ranks among the least prepared countries regarding its ability to safeguard itself in the digital realm.[55] Pakistan would need to develop a comprehensive cybersecurity plan to effectively address the cyber threats posed by India. To ensure regional deterrence stability, cultivating the necessary capabilities in all areas, including cyberspace, is necessary.

Emerging technologies will significantly enhance the impact of cyber-led combat, and their possible integration into the cyber domain will also create extra hazards in conflict-prone South Asia. Implementing these emerging technologies is expected to increase the magnitude of cyberattacks, as there will be many undisclosed flaws in these evolving technologies that hackers can exploit. Within the domain of nuclear operations, the cyber issue pertains to the potential threat of unauthorized individuals infiltrating the software, hardware, data, networks, and procedures of computer systems that oversee weapons, command and control systems, communication systems, and warning systems, as well as the personnel and information involved in their operation.

The susceptibility of a nuclear weapon system to hackers is determined by its dependence on digital software, the strength of its security measures, and the degree to which it is isolated from insecure networks. Any intruder seeking to undermine a network-centric system, its data, and individuals could employ diverse avenues. The most challenging task would involve launching targeted assaults against weapons and command and control systems, specifically by infiltrating these heavily fortified networks to deploy malicious software. The supply chain for hardware and software utilized in the nuclear industry could potentially be subjected to targeting.

Another potential hazard involves the potential disruption of the data and information required by these systems and the human operators who depend on them. These findings have evident ramifications for the transmission of messages, management of emergencies, and unintentional intensification of conflicts between states possessing nuclear weapons.

India's pursuit of advanced, revolutionary technology and the implementation of new monitoring methods instill anxiety and uncertainty in Pakistan, ultimately diminishing its security against

[54] Ayub Khan, Muhammad Imad. "Cyber warfare: implications for the national security of Pakistan." NDU Journal, 2019.
[55] "Pakistan Ranked among Least Cyber Secure Countries." The Express Tribune, February 13, 2019. https://tribune.com.pk/story/1909680/pakistan-ranked-among-least-cyber-secure-countries.

India.[56] Incorporating emerging technology into military capabilities and strategic positioning will fuel an intractable arms race dilemma in the region.

Conclusion

Emerging technologies are reshaping the traditional concept of deterrence, ushering in a new era of warfare. The changing geopolitics and the ongoing technological advancement drive strategic developments in South Asia. The transformation of US-China relations and intensifying rivalry and the US-India strategic partnership aimed at surpassing China would affect South Asian security dynamics. India's enhanced technological prowess in the wake of this partnership will disturb the regional balance. Its aggressive pursuit of military AI applications and the exploration of ML for hypersonic vehicles suggest a trajectory toward increased autonomy in military operations. Integrating disruptive technologies, particularly in cyberspace, introduces new dimensions of escalation and misjudgment, heightening the risk of deployment of nuclear weapons. The advent of AI, hypersonic weapons, LAWS, drones, and cyber technologies in South Asia can undermine established nuclear deterrence strategies and blur the lines between nuclear and conventional systems. The resulting competition to incorporate advanced technologies into military capabilities will create an imbalance and a new arms race, causing Pakistan to reassess its security measures against India and contribute toward the regional balance of power as a responsible state.

[56] Sadiq, Muhammad. Ali, Iftikhar. "Challenges of Nuclear Deterrence Stability in South Asia." Journal of Asian and African Studies 58, no. 8 (2023): 1511–27.