The Washington Quarterly

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rwaq20

Emerging Technologies and Southern Asian Nuclear Deterrence

Rabia Akhtar & Manpreet Sethi

To cite this article: Rabia Akhtar & Manpreet Sethi (2024) Emerging Technologies and Southern Asian Nuclear Deterrence, The Washington Quarterly, 47:4, 99-116, DOI: 10.1080/0163660X.2024.2435161

To link to this article: https://doi.org/10.1080/0163660X.2024.2435161

Published online: 18 Dec 2024.

Rabia Akhtar and Manpreet Sethi

Emerging Technologies and Southern Asian Nuclear Deterrence

Southern Asia is home to three nations armed with nuclear capabilities: China conducted its first nuclear test in 1964, followed by India and Pakistan in 1998. Each country has been actively pursuing its own concept of credible minimum deterrence and bolstering its relevant capabilities. The pace of this build-up has been influenced by their individual threat perceptions and levels of capability, as well as the assistance on nuclear and missile technologies that some have received through their strategic partnerships. Over time, the arsenals of all three have undeniably seen significant advancements.[1] Currently, all three possess secure second-strike capabilities, resulting in a state of mutual vulnerability that undergirds the foundation of nuclear deterrence.

However, states paired in nuclear dyads—such as US-Russia, US-China, US-North Korea, China-India, and India-Pakistan—often live in constant fear, worried that their adversary might find a way to escape mutual vulnerability.[2] Technology is believed to hold the key to this escape, which is why emerging technologies are pursued with both aspiration and concern, triggering a race to gain advantage while denying it to the adversary. This competition gives rise

Rabia Akhtar is the director of the Centre for Security, Strategy and Policy Research, the dean of the Faculty of Social Sciences at the University of Lahore in Pakistan and a visiting scholar with the Project for Managing the Atom at the Harvard Kennedy School's Belfer Center. She is also the author of *The Blind Eye: U.S. Non-proliferation Policy Towards Pakistan from Ford to Clinton* (2018) and the editor of *Pakistan Politico*, Pakistan's first strategic and foreign affairs magazine. She can be reached at rabia.akhtar@csspr.uol.edu.pk. Manpreet Sethi is a distinguished fellow at the Centre for Air Power Studies in New Delhi, where she leads the project on nuclear security, and a senior research adviser at the Asia-Pacific Leadership Network. She has authored, co-authored and edited nine books and four monographs. She can be reached at manpreetsethi07@gmail.com.

The Washington Quarterly • 47:4 pp. 99–116
https://doi.org/10.1080/0163660X.2024.2435161

to offense-defense spirals where if one side achieves better ability to defend itself with, for instance, ballistic missile defense, the other side finds ways of saturating or defeating the missile defense with more missiles, or those that have the speed or maneuverability to penetrate it. Such spirals pose a threat to deterrence stability. To avert the risks of instability, especially after the hair-raising experience of the Cuban missile crisis, the United States and the Soviet Union—the sole nuclear superpowers during the Cold War—attempted to rationalize their arms build-up by seeking arms control while maintaining deterrence. Not all agreements achieved their objective, but there was a cooperative effort of sorts to arrest the destabilizing tendencies of the then-emerging technologies. The 1972 Anti-Ballistic Missile Treaty, for example, arrested the deployment of ballistic missile defenses.

That age, however, seems to be over. Not only have the arms control agreements of that time eroded, the prospect of more seems unlikely given that the number of nuclear players has grown. Not only has this resulted in multiple nuclear dyads and chain conundrums, but each nuclear power in a dyad or chain must work out their own conditions for strategic stability. Meanwhile, recent unfettered advancements in emerging technologies—such as hypersonics, cyber weapons, or precision-strike capabilities—have re-ignited fears that nations may escape mutual vulnerability by ensuring their own first-strike ability through a combination of nuclear offense and defense while undercutting the assuredness of an adversary's retaliation. These technologies, it is feared, could impinge on nuclear deterrence in new and not yet fully understood ways.

Emerging technologies could impinge on nuclear deterrence in new, not yet fully understood ways

Unsurprisingly, emerging technologies within major nuclear powers are generating competition among them, especially in view of their stressed political relationships. Simultaneously, these developments are also impacting regional nuclear relationships. More specifically, the demarcation between global and regional dynamics is becoming blurred by the presence of strategic chain conundrums.[3] For example, while the US-China nuclear dynamic unfolds on a global scale, its repercussions extend downstream to shape the China-India and India-Pakistan equations, which are geographically much closer to each other as well.

There are three key issues to consider when it comes to emerging technologies in Southern Asia. Understanding some nuanced specifics of the realities of the region would help build a more granular comprehension of the impact of emerging technologies on regional strategic stability. This can in turn enable the

development of better-informed policies that can hopefully avoid exacerbating security dilemmas.

First, it is important to acknowledge that technologies labeled as "emerging" at the global level might not be the same regionally. What may seem like "old" technologies elsewhere—like ballistic missile defense, multiple independently-targetable reentry vehicle (MIRV) missiles, or the full operationalization of sea-based deterrence capabilities—are still emerging in Southern Asia.

Second, it is important not to automatically assume that every emerging technology will invariably disrupt the already troubled relationships between nuclear nations in the region. While certain technologies may have an impact, others may not. In addition to technical capabilities which could potentially affect nuclear deterrence, regional dynamics are also affected by many other factors such as historical animosities, territorial disputes, cross-border terrorism, and geopolitical power struggles. These factors continue to shape and complicate the overall balance of power in the region.

Third, there are high technological disparities among the three countries. China is far ahead in various military capabilities such as hypersonics and utilization of space-based assets, India has some level of research and development and is steadily moving up the ladder of capability, and Pakistan is yet to demonstrate any such effort. Such disparity significantly complicates the prospects of establishing confidence-building measures, let alone arms control, among the actors involved.[4]

Keeping the above aspects in mind, this paper is divided into four sections. First, it identifies emerging technologies in the region. The subsequent section examines the emerging technologies that currently pose or may have the potential to pose challenges to the stability of regional deterrence relationships. In the third section, we explore opportunities within select emerging technologies that can be leveraged to promote regional deterrence stability. The paper emphasizes the need for dialogues between countries in Southern Asia to better understand each other's threat perceptions and capability developments, as well as to explore the possibilities of collaboratively using relevant emerging technologies such as space technology and artificial intelligence (AI) to deal with shared non-traditional security challenges like climate change, food security, and public health.

Emerging Technologies in Southern Asia

The contemporary concept of "emerging technology" encompasses a range of advanced technologies in the context of major nuclear powers. These include hypersonic glide as well as cruise delivery systems, cyber and space capabilities, and the utilization of artificial intelligence for military applications.

These technologies are expected to improve the performance of various components of national nuclear arsenals such as delivery systems, sensors, data assimilation and processing, and the hardware and software of nuclear command, control, and communications (NC3) architecture. Analysts fear that these developments could have negative repercussions for deterrence stability.

Considering that major nuclear states—namely the United States, Russia, and China—have been developing their nuclear capabilities for sixty to eighty years by now, the efficiency of their nuclear warhead designs, the accuracy and reliability of delivery platforms, and robustness of NC3 architecture have undergone generational improvements. In contrast, India and Pakistan are only a quarter of a century old as nuclear-armed states. Both are still working on improving their missile ranges, accuracy, navigation, and the robustness of launch platforms, as well as their command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities. Therefore, the basket of "emerging technologies" in the region also encompasses some of the "older" technologies that are fully integrated in the arsenals of advanced nuclear states.

Emerging technologies in Southern Asia include some "older" technologies already operational in advanced nuclear nations

Two such technologies, for instance, are ballistic missile defense (BMD) and MIRVed missiles. MIRVed missiles are able to carry several warheads, each of which can independently hit a target. With regard to BMDs, China and India are leading and have conducted several successful interceptions, as well as built an architecture of sensors and shooters to enable area and point defense (which is protection of a small area against incoming missiles, instead of country-wide defense). Their purpose is to bolster the survivability of their retaliatory capabilities by providing protection to warhead storage sites or command and control structures. However, their adversaries haven't always been convinced that this defensive capability wouldn't inadvertently pave the way for using nuclear arsenals offensively.[5] This perception nurtures insecurity and could trigger a destabilizing arms race. In fact, this has been evident in the deployment of MIRVs, as well as maneuverable reentry vehicle (MaRV) missiles, which have warheads capable of maneuvering and thus evading interception as a way of defeating BMD. But while apparently solving one problem of restoring stability upset by BMD, MIRVs and MarVs create additional risks of deterrence instability.[6] Widely perceived as first strike weapons, they induce a "use or lose" predicament for nuclear states, thereby increasing time pressures for nuclear use decisions and the concomitant risk of catastrophic consequences.

Besides these technologies that are just emerging in Southern Asia, the region is also acutely aware of the latest technological developments elsewhere. This is because Southern Asia finds itself impacted by the intense technological competition between the United States and China. China's nuclear capability build-up causes anxiety in India, particularly so in today's severely stressed security environment between Beijing and New Delhi. The impact of India's responses is obviously felt in Pakistan.[7]

Additionally, particularly in India, there is a high sensitivity to staying updated on emerging technologies lest they are blocked off by potential technology denial arrangements. This perception harkens back to past experiences when technology denial regimes such as the Nuclear Suppliers Group created and enforced discriminatory arrangements for access to technologies. Hence, there exists a strong inclination—even an imperative—to engage in research and development of emerging technologies to avoid being left behind.

Of course, given the technological asymmetry within the region, where China possesses the most expansive research and development (R&D) base and abundant financial resources to move rapidly toward advanced capabilities, the other two states are also prioritizing technology developments given their stressed political relations and mutual threat perceptions.[8] There is also a recognition that many of the emerging technologies such as artificial intelligence, autonomous systems, robotics, and data analytics could offer widespread civilian benefits across health care, transportation, agriculture, and more that countries would want to harness for socioeconomic development.

Potentially Destabilizing Emerging Technologies

The introduction of any new technology can disrupt long-standing nuclear deterrence practices, with concomitant implications for geopolitical relations. This is of particular significance given the delicate relations in Southern Asia. This section identifies the technologies that could have a destabilizing impact.

Hypersonic Delivery Systems

A hypersonic delivery system refers to a ballistic or cruise missile capable of flying at speeds exceeding Mach 5 (five times the speed of sound). Notably, unlike intercontinental ballistic missile systems (ICBMs) that achieve similar velocities but only during their launch and terminal phases, hypersonic systems can maintain high speeds throughout the flight, operate at lower altitudes, and exhibit remarkable maneuverability. Thus, they can effectively evade interception by current BMD systems. As a result, the nuclear balance which was perceived to have shifted toward defense appears to have moved, or will move, back in favor of offense.

The introduction of hypersonic delivery systems complicates nuclear deterrence in three ways, all of which are pertinent for Southern Asia. First, hypersonic missiles exacerbate ambiguities in two ways: ambiguity pertaining to the warhead and ambiguity related to the target. In scenarios when an adversary's early warning system detects approaching missiles, but it cannot determine whether they are conventional or nuclear armed, nor ascertain their intended target, the natural inclination could be to assume the worst outcome.[9] This uncertainty could prompt a quick response. According to one analysis, "If states begin using weapons that are more manoeuvrable, and in dual-use fashion, it will risk a return to the policy of launch-on-warning for retaliatory strikes."[10] Undoubtedly, a country possessing a small and relatively less survivable nuclear arsenal facing an adversary with hypersonic missiles and protected by a BMD would harbor concerns over the potential destruction of its nuclear assets (a.k.a. a "use them or lose them" dilemma) by even conventionally armed hypersonic missiles. The tendency could then be to shift to more trigger-ready postures such as launch on warning (LOW) or launch under attack (LUA) to ostensibly enhance deterrence. However, such shifts would also raise risks of inadvertent nuclear use caused by misperception and miscalculation in moments of crisis.[11]

Hypersonic delivery systems complicate nuclear deterrence in three ways

Second, the introduction of hypersonics would lead to an offense-defense spiral and impact arms race stability. According to reports, the United States has embarked on efforts to bolster its BMD system and develop effective countermeasures to counter the threat posed by incoming hypersonic missiles. Additionally, the United States plans to have a robust arsenal of its own hypersonic missiles as a deterrent.[12] US adversaries Russia and China are likely to follow a similar strategy. The stage is thus set for an arms race, as all three key players in this game possess the financial resources and technological prowess to develop offensive capabilities for deterrent purposes while simultaneously constructing a defensive shield to limit damage from adversary attacks. This potential arms race could stimulate instability on the regional level too, since China's involvement in this contest bears implications for India, while Pakistan cannot afford to not respond with measures of its own.[13] This has the potential to be significantly destabilizing.[14]

A third implication of this development would be to take the offense-defense developments into outer space, placing sensors and interceptors as countermeasures to hypersonics.[15] While none of this would be easy or quick, weaponization of outer space would, nevertheless, be a distinct possibility once hypersonic

inductions become the norm. US-China competition in outer space—and the two countries' unwillingness to accept any limitations—is likely to have implications for others, including in Southern Asia.

Increasing Space-based Capabilities

In the past few decades, space-based capabilities have experienced remarkable advancements, transitioning from serving as force multipliers for ground operations to potentially moving toward space weaponization itself.[16] While the placement of weapons in space has not yet taken place, the possibility of maliciously using satellites as weapons—through collisions enabled by advancing in-orbit maneuvering capabilities and use of robotic arms—has grown. Non-kinetic attacks using directed energy weapons (DEWs) can be used to disable or destroy satellites from a distance, including from Earth. The United States, Russia, and China have conducted tests of laser weapons that could be mounted on satellites or ground-based platforms to counter enemy satellites. Any such activity that harms—or is perceived to be capable of harming—another state's satellites that are involved in command and control of nuclear forces can tempt the state towards early nuclear use to obviate the possibility of losing its nuclear force capability.

Meanwhile, in the kinetic sphere, anti-satellites (ASATs), which can disable and disrupt satellite operations, have also been tested by all three global nuclear powers, as well as by India.[17] Were such an act to take place during a crisis against communication and surveillance satellites which are deemed critical for a nation's war-fighting ability, the reduced situational awareness and increased uncertainty could create serious risks and challenges. In fact, the very fear of disruption of satellites which are critical for nuclear targeting or command and control could drive nations toward pre-emptive actions, ultimately leading to heightened instability. As written by Stephen Cimbala, "Loss of satellite network integrity would leave a state blinded with respect to the alert or launch status of other states' forces. During a crisis, worst case assumptions might be made about the other side's intentions based on degraded or missing information."[18]

Another capability that has the potential to be destabilizing in Southern Asia is space-enabled navigation that can enhance missile accuracies, thus opening up the possibility of counterforce targeting against retaliatory nuclear assets.[19] Given that China, India, and Pakistan have premised their deterrence on the idea of inflicting punishment by causing unacceptable damage, the focus of their capability build-up has been on improving ranges (rather than accuracies) of missiles to signal credible countervalue targeting. However, better space-enabled navigation on missiles would likely intensify concerns regarding preemptive conventional missile attacks on nuclear facilities. In fact, this has been a significant concern of China regarding the US conventional global prompt strike capability,

which is one of the reasons for China's increasing nuclear silos with the possible aim of playing the shell game to hide its ICBMs.

Meanwhile, as China's missile accuracy continues to improve, concerns would arise in India about the possibility of Beijing using its conventional missiles to target New Delhi's nuclear assets. Better counterforce capability could also increase the temptation for a first strike and China possibly abandoning its no first use (NFU) doctrine.[20] The combination of BMD systems and high-precision conventional or nuclear missiles creates a destabilizing paradigm anywhere, including in Southern Asia's security landscape.

Offensive Cyber Capabilities

Modern network-centric systems which enable rapid collection, processing, and transmission of data are central to war fighting. Naturally, an enemy would like to blunt this capability using data disruption. Such disruption would acquire a special dimension in the case of nuclear command, control, and communication (NC3) systems, which may be taken to include early warning systems, national command authority centers, and delivery systems. NC3 is designed with two distinct objectives in mind. First and foremost, it ensures "positive control," or the utmost responsiveness to duly authorized commands, thus facilitating a nuclear launch when instructed. Additionally, it serves to provide "negative control," or to safeguard against inadvertent or erroneous commands, effectively preventing any accidental or mistaken launch scenarios.

Cyber attacks can disrupt both positive and negative control of nuclear weapons

Nuclear nations have constantly struggled to optimize positive and negative controls through requisite hardening, redundancy, and finding other ways of enhancing robustness. However, the cyber threats faced by these systems should not be taken lightly.[21] They can disrupt positive controls by interfering with launch activation through jamming, corruption, or deception (aka "spoofing"), as well as undermine negative controls through the use of false alarms or deliberate misinformation. The very fear of compromising nuclear command and control could compel nations to adopt risky nuclear postures, thereby posing a higher threat of inadvertent nuclear war. Moreover, cyber attacks could also disrupt communication channels between different components of the command and control infrastructure, leading to a breakdown in communication and potentially causing chaos in an already tense environment.[22]

A third kind of cyber attack could be carried out by injecting false information into the NC3 to issue "counterfeit launch orders."[23] Non-state actors desirous of

bringing two nuclear-armed nations to nuclear blows could be particularly tempted to do this. This could further escalate tensions between nations, leading to unintended consequences. The threat of such cyber attacks is compounded by the fact that, unlike traditional warfare, their origins can often be concealed, making it difficult for nations to definitively identify the source of aggressive cyber activities. This lack of attribution could potentially lead to a sense of uncertainty and confusion, increasing the risk of miscalculations and unintended escalation.

In Southern Asia, cyber espionage attacks have been reported against critical infrastructure. For instance, a US-based cyber threat intelligence company, Recorded Future, released a report in 2022 which mentioned that "at least seven Indian state load dispatch centres (SLDCs)" and an Indian subsidiary of a multinational logistics company were targeted by a China-linked group that it has code-named TAG-38.[24] SLDCs manage the integrated operations of the power systems. The Indian government also claimed that cyber attackers linked to the Chinese military likely broke into the networks of seven power grid hubs in north India in 2022. Besides power plants, some sensitive organizations in defense and finance have also been targets of Chinese cyber attacks. According to Black Lotus Labs, the threat intelligence arm of US-based Lumen Technologies, Pakistan-based hackers have also attacked critical infrastructure of the Indian power sector and a government organization in 2021.[25] Additionally, a slew of cyber attacks by Pakistani "hacktivists" on Indian government websites took place just a day before the G-20 Summit in September 2023.[26] Meanwhile, the *Global Times* reported in 2021 that a report published by Antiy Labs, one of China's cybersecurity companies, disclosed that an active hacker team in Delhi had been launching cyber attacks against government agencies and defense departments in China and Pakistan.[27]

Were a major cyber attack against a critical infrastructure target mounted—or even perceived to be mounted—by any of the Southern Asian countries against one another during a crisis, it could raise fears and cause misperceptions that could spiral into escalation. Therefore, there is a need for efforts at bilateral or multilateral cyber governance rules and norms to restrain the use of cyber weapons, especially against nuclear systems.[28] Any agreement that mandates non-targeting of nuclear systems through cyber disruptions would be beneficial for all. Even though non-state actors indulging in malicious cyber activity would be difficult to deter, such efforts would at least reduce the risks of misperceptions leading to unwanted escalation.

Military Applications of AI

The true extent of artificial intelligence's applications in robotics, autonomous vehicles, supercomputing, and quantum computing is yet to be fully realized. It

is also unclear how the introduction of such systems in nuclear forces or command or control structures would play out. However, it must be noted that the very perception of an opponent's advancements in AI leading to more robust nuclear offensive capability can create paranoia in the adversary about threats to its ability to retaliate, and thus incline them toward a posture of nuclear pre-emption.

In a crisis situation, the employment of AI-enabled intelligence, surveillance, and reconnaissance (ISR), such as autonomous sensor systems or automated target recognition—or even the perception of availability of such a system with the adversary—could lead to inadvertent escalation. As stated in a 2018 report published by RAND, "AI may be strategically destabilizing not because it works too well but because *it works just well enough to feed uncertainty*."[29] When a nation perceives that its opponent possesses the potential to launch a devastating first strike, it creates a security dilemma. This perception compels the first nation to develop countermeasures like defense systems against counter-force attacks, as well as strategies such as hardening and camouflage to outmaneuver or confuse ISR efforts. Lawrence Freedman, a prominent nuclear strategist, warned in 1981 that "to the extent that AI influences perceptions of intent and capability and alters the calculus of risk and reward, it will inspire new thinking about possible offensive and defensive maneuvers in the evolution of nuclear strategy."[30]

Even the perception of available AI-enabled ISR could lead to inadvertent escalation

The potential impact of AI-enabled technologies on the battlefield may trigger an arms race as nations endeavor to counter perceived disadvantages. This could involve investing in defensive measures to enhance the survivability of their nuclear forces and mitigate potential threats. For instance, Russia defends utilizing AI, specifically referring to its doomsday drone known as the Oceanic Multipurpose System Status 6. This autonomous vehicle is launched from a submarine and possesses the intelligence to elude oceanic defenses. Its purpose is to deliver a nuclear payload, thereby inflicting damage upon adversaries and reinforcing the credibility of its deterrence against US BMD or anti-submarine warfare (ASW) capabilities.

One additional concern regarding AI arises from its role in expediting decision-making by compressing timelines. While this may help a commander by assisting him in making sense of the available information, it could also increase pressures for *immediate* action, thereby reducing time for leaders to weigh options and raising the risk for nations to inadvertently stumble into further escalation. Therefore, speed of decision-making could be both an asset

and a liability. As cautioned by a Centre for Global Security Research report, "the speed at which AI guided ISR could direct and execute kinetic operations could limit options for de-escalation."[31] This speed would shrink the time for political or diplomatic action to resolve a crisis. It would be imprudent to forget that "in practice, slowing things down can be the key to victory, especially when the options include nuclear weapons."[32]

AI's potential to enhance targeting speed and precision while undermining mutual vulnerability and reinforcing one side's ability to degrade the other's deterrence would have destabilizing consequences. Therefore, utilization of AI on the battlefield needs to be intelligently managed for its benefits in providing clarity with a recognition of the risks. The impact of AI can be further understood by examining its implementation in various military applications as briefly described below.

Autonomous Systems.The advancement of autonomous systems—including unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and unmanned underwater vehicles (UUVs)—is on the cusp of revolutionizing warfare. Such systems can make a kill chain more lethal since they are capable of executing a six-step decision-making process—find, fix, track, target, engage, and assess (F2T2EA)—more quickly than human actors, thereby facilitating an advantage in warfare. For example, real-time automatic target recognition (ATR) utilizes deep-learning techniques to identify multiple targets efficiently. By integrating high-power AI-based imagery processing on UAVs, sensor fusion can reduce lag time. This advancement enables increased autonomy for unmanned systems, specifically for launching multi-domain attacks in the battlefield.[33] However, establishing a "closed loop" in the strike chain autonomously and swiftly, without encountering communication lag from ground control, may inadvertently increase the risk of escalation. Deploying such capabilities in environments characterized by contested boundaries and fraught political relations—as in Southern Asia—can lead to significant instability.

All three countries in Southern Asia are using unmanned vehicles for various purposes. In a crisis scenario, autonomous systems can quickly become a source of confusion and misinterpretation. For instance, an unmanned aerial vehicle flying over disputed border territories could be misinterpreted as a hostile act, leading to a swift and aggressive response from the opposing party. The utilization of autonomous systems in military operations brings forth concerns of potential accidental or unintended harm to crucial infrastructure, including nuclear facilities, thereby risking a nuclear crisis. Consequently, these systems introduce uncertainty, making it challenging to preserve a stable strategic balance.

Quantum Computing. Quantum computing is an emerging technology that has tremendous potential for military applications. Unlike classical computers, quantum computers use quantum bits, or qubits, to process information, which allows them to perform complex calculations at unprecedented speeds. Additionally, quantum computers can break current encryption methods that safeguard the security of nuclear command and control systems and communication channels.

Encryption is the process of transforming plaintext into unintelligible ciphertext using an algorithm and a secret key. This ensures that only authorized individuals can access sensitive information such as nuclear codes. This is obviously a critical method of negative control to prevent unauthorized access and tampering. Current encryption methods rely on mathematical problems that are believed to be hard to solve even with the most powerful classical computers. However, a quantum computer could solve these problems using Shor's algorithm, which is specifically designed for quantum computers and can factor large numbers quickly.[34] Similarly, quantum computing could compromise the security of communication channels used to exchange nuclear-related information, allowing unauthorized access and interception. This could lead to deliberate miscommunication, increasing the risk of nuclear conflict.

Little is known in the public domain about how well the military use of this technology is advancing in Southern Asia. At this stage, a deeper understanding of potential risks might help temper its development and future introduction.

Disinformation and Deepfake Technologies. As the world becomes increasingly digital, the emergence of disinformation and deepfake technologies has become a significant threat. Deepfakes are synthetic videos or audio recordings that are manipulated to create a false reality, which can be used to deceive and mislead individuals or groups. The use of such technology in disinformation campaigns is causing major concern for policymakers, as these campaigns can manipulate public opinion and increase tensions between nuclear-armed nations.

Given the increasing sophistication of such technologies, it has now become more challenging to distinguish between real and fake information. In effect, this makes it easier for hostile actors to spread false narratives and create fictitious events which could trigger a military response from nuclear-armed states. Moreover, disinformation campaigns can lead to mistrust and misunderstandings between nuclear nations, thereby increasing the likelihood of conflict escalation.[35] Such campaigns are often targeted at specific audiences and can be designed to exploit pre-existing political or social divisions, creating further instability in the already tense region.[36]

Opportunities to Stabilize Deterrence in Southern Asia

Although more attention is often given to how the introduction of emerging technologies has the potential to intensify security challenges, some of these technologies can also help overcome specific challenges and mitigate conflict risks. Some of these cases are initially explored in the following paragraphs.

Emerging technologies can also help mitigate conflict risks

Secure Communication Channels

In crisis-prone regions like Southern Asia, the presence of effective communication systems is of the utmost importance. Emerging technologies can help by ensuring the continuous availability of communication, even in times of crisis, and providing the confidence of authenticity. One of the challenges cited by India and Pakistan is that of spoofing, or disguising false communication to make it appear from a known trusted source.

For example, during the aftermath of the Mumbai crisis in November 2008, at the height of tensions between India and Pakistan, a hoax phone call was supposedly made from India's foreign minister Pranab Mukherjee to the Pakistani president, Asif Ali Zardari. Despite occurring late on November 28, the call was surprisingly connected by Zardari's staff without adequate verification of its authenticity. The call purportedly issued a war threat to Pakistan unless it took action against those responsible for the Mumbai attacks. If better encryption using emerging technologies can secure networks against jamming, spoofing, and cyber attacks to ensure rapid and secure transmission of information that is believed to be dependable, it could help manage a crisis.

Enhanced ISR Capabilities

A significant challenge in the region is the potential for miscalculation and accidental conflict owing to misperceptions or lack of information on developments related to the adversary. Emerging technologies in the field of ISR—including those which can enable advanced analytics and predictive modeling—can enhance situational awareness, thereby reducing the likelihood of misinterpretation or miscommunication. An increase in transparency and faith in the accuracy of information generated through advanced ISR technologies can reduce the risk of tactical errors and minimize the likelihood of pre-emptive actions.

For example, in the current Russia-Ukraine conflict, Russia has repeatedly issued nuclear threats, claiming that its nuclear forces are on high alert. However, the United States has not felt the need to reciprocate because its

ISR has not detected ground movements in Russia.[37] The ability to look across the border has been a way of keeping the situation stable despite the conflict. Similar use of ISR technology in Southern Asia could enhance crisis stability. Better information could lead to better informed decisions.

Of course, some also worry that better ISR could lead to the possibility of targeting nuclear assets. However, this is overplayed because despite ISR-obtained information, no nation can be sure that it can conduct a disarming or decapitating strike against the adversary. Therefore, the basics of nuclear deterrence would not change with better ISR, though its benefits in terms of verifying through national technical means could be better utilized, including for supporting existing military and nuclear CBMs. In fact, given that the three countries in the region face common climate change concerns as evident in severe natural disasters, space-based capabilities can also be collectively utilized for disaster management.

The Road Ahead

Deterrence instability may arise from various factors, including technological capabilities. To mitigate potential destabilization in the region caused by emerging technologies, confidence-building measures and diplomatic initiatives which promote responsible behavior could serve as crucial starting points. In fact, the benefits of these measures are universal. Given the current tense state of affairs in all nuclear dyads, it looks unrealistic to expect arms control frameworks to develop. Nevertheless, dialogues between countries, including in Southern Asia, can provide an avenue for expressing and understanding each other's threat perceptions. This, in turn, can help effectively address the implications of emerging technologies on strategic stability. In fact, it would be beneficial for Southern Asian states to explore collaborative utilization of emerging technologies in dealing with shared non-traditional security challenges like climate change, food security, and public health. By leveraging their collective expertise and resources, they can effectively address shared challenges.

Dialogues can help effectively address emerging technologies impact on strategic stability

In the current state of affairs, however, the three nuclear armed states in Southern Asia are less inclined to explore the opportunities that emerging technologies offer for collaborative problem solving and are more keen to develop and deploy them for their presumed military benefits. But adoption of emerging technologies can also introduce unfamiliar challenges that could inflame tensions and

heighten escalation risks. This occurred during the nuclear weapons race of the 1950s and 1960s between the United States and the Soviet Union. During that era, political tensions ran high, coinciding with the maturation of new technologies in missile systems, early warning systems, and defense capabilities. Each of these advancements was perceived as a potential disruptor to nuclear deterrence. Remarkably, echoes from this period are evident in today's environment.

The purpose of recalling this fact is to prevent being overwhelmed by a feeling of powerlessness in light of contemporary technological shifts. Disruption of deterrence stability can arise from technological advancements as much as from political dynamics, leaders, and underlying animosities. In fact, even the mere perceptions of enhanced speed, stealth, maneuverability, early warning systems, detection capabilities, and interception capabilities promised by emerging technologies can threaten regional nuclear deterrence. However, it is important to acknowledge that even with all factors considered, there can be no certainty that a first strike can prove to be effectively disarming or incapacitating for an adversary. The inability to rule out the possibility of retaliation despite the enhanced efficacy of a first strike even with emerging technological advancements is the very foundation of nuclear deterrence. Emerging technologies will have an impact on deterrence relations, but they are not the sole factors influencing stability. In order to correctly understand their implications for deterrence, one must juxtapose them with other factors that also impact the overall state of equilibrium between states.

Notes

1. Ashley Tellis, "Striking Asymmetries: Nuclear Transitions in Southern Asia," Carnegie Endowment for International Peace, July 18, 2022, 303, https://carnegieendowment.org/2022/07/18/striking-asymmetries-nuclear-transitions-in-southern-asia-pub-87394.
2. Rabia Akhtar, "First-Strike Stability and Credibility of Pakistan's Nuclear Deterrence," *Pakistan Journal of International Affairs* 5, no. 2 (2022), https://pjia.com.pk/index.php/pjia/article/view/677.
3. For more, see Manpreet Sethi, "Nuclear Risks in Southern Asia: The Chain Conundrum," in *Nuclear Risk Reduction: Closing Pathways to Use*, ed. Wilfred Wan (Geneva: United Nations Institute for Disarmament Research, 2020).
4. For a recent discussion on the technological disparities between China and India and their impact on Pakistan, see Walter Ladwig III et al., "India-China Security Competition on Land, at Sea, in Space, and Beyond," *Brookings Global India* (podcast), October 4, 2023, https://www.brookings.edu/articles/india-china-security-competition-on-land-at-sea-in-space-and-beyond/.
5. Zafar Khan, "India's Ballistic Missile Defense: Implications for South Asian Deterrence Stability," *The Washington Quarterly* 40, no. 3 (2017): 187–202, https://www.tandfonline.com/doi/abs/10.1080/0163660X.2017.1370339.

6. Sadia Tasleem, "No Indian BMD for No Pakistani MIRVS," Stimson Center, October 2, 2017, https://www.stimson.org/2017/no-indian-bmd-no-pakistani-mirvs/.
7. Shaza Arif, "Emerging Trends of Artificial Intelligence in South Asia and its Implications for Pakistan," *NUST Journal of International Peace & Stability* 2, no. 2 (2019): 55–66, https://njips.nust.edu.pk/index.php/njips/article/view/31.
8. Manpreet Sethi, "Understanding the Nuclear Landscape in Southern Asia: Complexities and Possibilities," *Journal for Peace and Nuclear Disarmament* 5, no. 2 (2022): 224–242, https://www.tandfonline.com/doi/pdf/10.1080/25751654.2022.2156253.
9. Ayesha Abbasi, "Indian Quest for Hypersonic Missiles in South Asia and Disruption of Strategic Stability in the Indo-Pak Dyad," *IPRI Journal* 23, no. 2 (2023): 23–52, https://journal.ipripak.org/wp-content/uploads/2023/06/Article-2-IPRI-Journal-XXIII-I-Ayesha-Abbasi-FINAL-JUNE-27.pdf.
10. "Hypersonic Weapons and Strategic Stability," *Strategic Comments* 26, no. 1 (2020), https://doi.org/10.1080/13567888.2020.1739872.
11. Beyza Unal et al., "Uncertainty and Complexity in Nuclear Decision-Making: Case Studies," Chatham House, March 2022, https://www.chathamhouse.org/sites/default/files/2022-03/2022-03-07-nuclear-decision-making-unal-et-al_1.pdf.
12. Congressional Budget Office, "U.S. Hypersonic Weapons and Alternatives," January 31, 2023, https://www.cbo.gov/publication/58255.
13. Dmitry Stefanovich, "Nuclear Posture and Technology Trends in South Asia and Ways Ahead," *National Security Journal* 3, no. 4 (2022), https://nationalsecurityjournal.nz/wp-content/uploads/sites/13/2022/02/NSJ-2022-March-Stefanovich.pdf.
14. Feroz Hassan Khan, "Strategic Risk Management in Southern Asia," *Journal for Peace and Nuclear Disarmament* 5, no. 2 (2022): 369–393, https://www.tandfonline.com/doi/full/10.1080/25751654.2022.2136878.
15. David Vergun, "General Says Countering Hypersonic Weapons Is Imperative," US Department of Defense, May 10, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3391322/general-says-countering-hypersonic-weapons-is-imperative/.
16. Rajeswari Pillai Rajagopalan, "India's Space Priorities Are Shifting Toward National Security," Carnegie Endowment for International Peace, September 1, 2022, https://carnegieendowment.org/2022/09/01/india-s-space-priorities-are-shifting-toward-national-security-pub-87809.
17. Ajey Lele, "Indian Space Force: A Strategic Inevitability," *Space Policy* 65 (2023), https://www.sciencedirect.com/science/article/abs/pii/S0265964622000522.
18. Stephen J. Cimbala, *Getting Nuclear Weapons Right: Managing Danger and Avoiding Disaster* (London: Lynne Rienner Publishers, 2018), 210.
19. Kartik Bommakanti, "A Conceptual Analysis of Sino-Indian Space Deterrence and Space Warfighting," Observer Research Foundation, April 24, 2017, https://www.orfonline.org/research/a-conceptual-analysis-of-sino-indian-space-deterrence-and-space-warfighting.
20. Tong Zhao, "China and the International Debate on No First Use of Nuclear Weapons," *Asian Security* 18, no. 3 (2022): 205–213, https://www.tandfonline.com/doi/abs/10.1080/14799855.2021.2015654.
21. Hammaad Salik and Rao Ibrahim Zahid, "From Cold to Code War: Dissecting Security Strategies for the Cyberspace Strategic Environment and Identifying Cyber Risks to the Nuclear Strategic Environment," *Cyberpolitik Journal* 7, no. 13 (2022), http://cyberpolitikjournal.org/index.php/main/article/view/156.

22. Rabia Akhtar, "Technological Determinism and Challenges to Deterrence in Southern Asia," Policy Brief No. 83, Asia-Pacific Leadership Network for Nuclear Non-proliferation and Disarmament (APLN) and the Norwegian Institute of International Affairs (NUPI), September 5, 2022, https://cms.apln.network/wp-content/uploads/2022/09/PB-83-Rabia-PB.pdf.
23. Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington D.C.: Georgetown University Press, 2018).
24. Binayak Dasgupta, "Chinese Hackers Targeted 7 Indian Power Hubs, Govt Says Ops Failed," *Hindustan Times*, April 8, 2022, https://www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html.
25. "Pakistan-based Hackers Target Indian Power Sector, Govt Organization," *Business Today*, July 13, 2021, https://www.businesstoday.in/technology/news/story/pakistan-based-hackers-target-indian-power-sector-govt-organisation-301224-2021-07-13.
26. Arvind Ojha and Bidisha Saha, "Decoding Pak-based Cyber Attacks that Targeted Govt Sites Ahead of G-20," *India Today*, September 10, 2023, https://www.indiatoday.in/india/story/behind-cyberattacks-pakistan-based-groups-indian-government-websites-before-g20-2433530-2023-09-09.
27. "Hackers from Delhi Reportedly Launching Cyberattacks against China, Pakistan," *The New Indian Express*, November 20, 2021, https://www.newindianexpress.com/nation/2021/Nov/20/hackers-from-delhi-reportedly-launching-cyberattacks-against-china-pakistan-2386047.html.
28. For a detailed discussion on cyber arms control and the challenges therein, see Thomas Reinhold and Christian Reuter, "Cyber Weapons and Artificial Intelligence: Impact, Influence and the Challenges for Arms Control" in Thomas Reinhold and Niklas Schörnig eds., *Armament, Arms Control and Artificial Intelligence: The Janus-faced Nature of Machine Learning in the Military Realm* (Cham, Switzerland: Springer International Publishing, 2022).
29. Edward Geist and Andrew J. Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" RAND Corporation, April 24, 2018, 15, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE296/RAND_PE296.pdf. Emphasis added.
30. Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St Martin's Press, 1981).
31. Paige Gasser, Rafael Loss, and Andrew Reddie, "Workshop Summary Report – Assessing the Strategic Effects of Artifical Intelligence," Centre for Global Security Research, Lawrence Livermore National Laboratory, November 12, 2018, 6, https://www.osti.gov/servlets/purl/1544928.
32. Zachary Davis, "Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability and Strategic Surprise," Centre for Global Security Research, Lawrence Livermore National Laboratory, March 2019, 10, https://cgsr.llnl.gov/sites/cgsr/files/2024-08/cgsr-ai_battlefieldweb.pdf.
33. Anushka Saxena, "China's Approach to Military Unmanned Aerial Vehicles and Drone Autonomy," Takshashila Institution, September 2023, https://takshashila.org.in/research/takshashila-slidedoc-chinas-approach-to-military-unmanned-aerial-vehicles-and-drone-autonomy.
34. Nicolas Ayala Arboleda, "How Fear of Future Quantum Hacks Could Expose Sensitive Data Now," Bulletin of the Atomic Scientists, March 30, 2023, https://thebulletin.org/2023/03/how-fear-of-future-quantum-hacks-could-expose-sensitive-data-now/.

35. Rabia Akhtar, "Deepfakes, AI & Digital Soldiers: Challenges of Cross-Domain Coercion for Pakistan," *Pakistan Politico*, October 7, 2020, https://pakistanpolitico.com/deepfakes-ai-digital-soldiers-challenges-of-cross-domain-coercion-for-pakistan/.
36. Syed Ali Zia Jaffery, "Non-Linear, Unpredictable, and Dangerous Crisis-Escalation in South Asia," CSIS Next Generation Nuclear Network, January 7, 2022, https://nuclearnetwork.csis.org/non-linear-unpredictable-and-dangerous-crisis-escalation-in-south-asia/.
37. Jim Sciutto, "Explained: US prepared 'Rigorously' for Potential Russian Nuclear Strike in Ukraine in Late 2022, Officials Say," CNN, March 9, 2024, https://edition.cnn.com/2024/03/09/politics/us-prepared-rigorously-potential-russian-nuclear-strike-ukraine/index.html.