CENTER FOR INTERNATIONAL STRATEGIC STUDIES
43-Orchard Boulevard, Orchard Scheme
Islamabad Pakistan
Ph: +92-51- 8315410-423, **Fax:** +92-51-6132518

NUCLEAR DETERRENCE IN THE AGE OF EMERGING TECHNOLOGIES

REPORT

CISS INTERNATIONAL CONFERENCE ON

NUCLEAR DETERRENCE IN THE AGE OF EMERGING TECHNOLOGIES

CENTER FOR INTERNATIONAL STRATEGIC STUDIES
ISLAMABAD PAKISTAN

Edited by
Dr Bilal Zubiar, Director Research, CISS
Anum A. Khan, Associate Director Research, CISS

Supervised and Reviewed by
Dr Bilal Zubair, Director Research, CISS

Prepared by
Anum A Khan, Associate Director Research, CISS

Compiled and Transcribed by
Dr Anum Riaz (Associate Director Research), Dr Rahat Iqbal (Associate Director Research), Abdul Moiz Khan, Maryyum Masood, Amna Saqib, Murad Ali, Mobeen Jafar Mir, Fakhar Alam, Muhammad Ali Baig, Syed Ali Abbass, Shawana Sohail, Anum Murad Khan, Nawal Nawaz, Areesha Manzoor, ZamZam Channa, Malik Muhammad Kashif, Muhammad Kumail

Design Incharge
Shahid Waseem Malik, IT Administrator, CISS

The Center for International Strategic Studies (CISS) Islamabad conducts original policy research, analysis, and strategic outreach, aiming to highlight evolving regional and global strategic issues and promote peace and stability.

www.ciss.org.pk

REPORT

CISS INTERNATIONAL CONFERENCE

ON

NUCLEAR DETERRENCE IN THE AGE OF EMERGING TECHNOLOGIES

CENTER FOR INTERNATIONAL STRATEGIC STUDIES
ISLAMABAD PAKISTAN

Table of Contents

Acronyms

ABM Treaty	Anti-Ballistic Missile Treaty
ADR	Active Debris Removal
AGI	Artificial General Intelligence
AI	Artificial Intelligence
ANI	Artificial Narrow Intelligence
ARS	Acute Radiation Syndrome
ASAT	Anti-Satellite Weapons
ASAT	Anti-Satellite Weapons
ASI	Artificial Superintelligence
AUKUS	Australia, United Kingdom and United States
BECA	Basic Exchange and Cooperation Agreement
BJP	The Bharatiya Janata Party
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIA	Central Intelligence Agency
CMD	Credible Minimum Deterrence
COMCASA	Communications Compatibility and Security Agreement
CRP	Coordinated Research Project

CSD	Cold Strat Doctrine
DBT	Design Basis Threat
DEW	Directed Energy Weapons
ETs	Emerging Technologies
EDTs	Emerging Disruptive Technologies
EPA	Environmental Protection Agency
EPA	Environmental Protection Agency
eV	Electron Volt
EW	Electronic Warfare
FSD	Full-Spectrum Deterrence
GDP	Gross Domestic Product
GNSS	Global Navigation Satellite Systems
HALEU	High-Assay Low-Enriched Uranium
HEU	Highly Enriched Uranium
HMI	Human-Machine Interaction
IAEA	International Atomic Energy Agency
ICBMs	Intercontinental Ballistic Missiles
iCET	Initiative on Critical and Emerging Technologies
IIOJ&K	Indian Illegally Occupied Jammu and Kashmir
IMU	Islamic Movement of Uzbekistan

INDOPACOM	Indo-Pacific Command
IoT	Internet of Things
IRA	Irish Republican Army
ISIS-K	Islamic State – Khorasan Province
ISOP	Innovation to Support Operating Nuclear Power Plants
JADC2	Joint All-Domain Command and Control
LAWS	Lethal Autonomous Weapons Systems
LEO	Low Earth Orbit
LLM	Large Language Models
LNT	Linear No-Threshold Model
MDOs	Multi-Domain Operations
MeV	Million Electron Volts
MIRVs	Multiple Independently Targetable Reentry Vehicles
ML	Machine Learning
NASA	National Aeronautics and Space Administration
NC3	Nuclear Command, Control and Communications
NFU	No First Use Policy
NRC	Nuclear Regulatory Commission

NSG	Nuclear Suppliers Group
OODA Loop	Observe, Orient, Decide, Act
OSI	Open-Source Information
PAEC	Pakistan Atomic Energy Commission
PNT	Positioning, Navigation, and Timing
PPWT	Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects
QA	Quality Assurance
QBITS	Quantum Bits
QKD	Quantum Key Distribution
Quad	Quadrilateral Security Dialogue (Australia, India, Japan, and the United States
RMA	Revolution in Military Affairs
RPO	Rendezvous and Proximity Operations
RPO	Rendezvous and Proximity Operations
RSS	Rashtriya Swayamsevak Sangh
SCADA	Supervisory Control and Data Acquisition Systems
SMRs	Small Modular Reactors
SPD	Strategic Plans Division

SUPARCO	Space and Upper Atmosphere Research Commission
TRISO	Tri-structural ISOtropic
TRLs	Technology Readiness Levels
TTP	Tehrik-i-Taliban Pakistan
UAV	Unmanned Aerial Vehicle
UN SDGs	United Nations Sustainable Development Goals
UN	United Nations
UNSC	United Nations Security Council
VUCA	Volatile, Uncertain, Complex, and Ambiguous
WHO	World Health Organization
WMDs	Weapons of Mass Destruction

Introduction

The Center for Strategic Studies (CISS), Islamabad, organized a two-day International Conference, "Nuclear Deterrence in the Age of Emerging Technologies" on April 22-23, 2024, bringing together policy makers, practitioners, and eminent scholars from Pakistan and abroad. The conference highlighted Pakistan's commitment to continued dialogue and collaboration in addressing the challenges posed by emerging technologies to international security and regional stability.

The event brought together esteemed speakers from Australia, Canada, China, Russia, Switzerland, Italy, Spain, Austria, Nigeria, the United Kingdom (UK) and the United States of America (USA) on a dialogue discussing emerging technologies. The event was also attended by scholars, notable statesmen, think tank professionals, academics, foreign policy experts, and diplomats.

The speakers for the first day included Dr Han Hua from Peking University (China), Dr Xia Liping, Center for Polar and Oceanic Studies (China), Dr Naeem Salik from Strategic Vision Institute (Islamabad), Mr Anton Khlopkov from Center for Energy and Security Studies (CENESS) (Russia), Dmitry Stefanovich from Institute of World Economy and International Relations of the Russian Academy of Sciences (IMEMO RAS), Dr Alexander Evans OBE from LSE School of Public Policy (the United Kingdom), Dr Petr Topychkanov from Lomonosov Moscow State University (Russia), Ms Alice Saltini from James Martin Center for Nonproliferation Studies and Institute for Security and Technology (Italy), Dr Jean-Marc Rickli from Geneva Center for Security Policy (Switzerland), Dr Zafar Khan from Baluchistan Think Tank Network (Quetta), Dr Robert B. Hayes from North Carolina State University, (USA) and Dr Tariq Rauf from Austria.

The speakers for the second day included Dr Laetitia Cesari from the United Nations Institute for Disarmament Research (UNIDIR) (online), Ms Almudena Azcárate Ortega from UNIDIR, Dr Christine M Leah from the National Institute for Deterrence Studies (Australia), Dr Olamide Samuel from Open Nuclear Network (Austria), Dr Jessica West from Project Ploughshare (Canada), Mr HE Miao from China Arms Control and Disarmament Association CACDA (China), Brigadier (R) Dr Zahir Kazmi, Advisor, Strategic Plans Division, Pakistan, Dr Rizwana Abbasi (Non-Resident Fellow, CISS Islamabad) based in Vienna, Austria, Prof. Dr Zafar Nawaz Jaspal from Quaid-e-Azam University (Islamabad), Prof. Dr Andrey Pavlov from Saint Petersburg State University (Russia), and Mr Vladislav Chernavskikh from Stockholm International Peace Research Institute (SIPRI).

The conference commenced with Welcome Remarks by Ambassador Ali Sarwar Naqvi, Executive Director of CISS, highlighting the impact of the unregulated development of emerging technologies (ETs) on the nuclear security architecture and crisis stability in South Asia. General Sahir Shamshad Mirza, NI (M), Chairman Joint Chiefs of Staff Committee (CJCSC), delivered the Keynote Address, contextualizing the global transformation toward a "fluid multipolarity" recognizing power contestation, technological innovation and the erosion of traditional deterrence architecture as driving forces behind the fluid multipolarity. He reinforced Pakistan's commitment to Full-spectrum Deterrence (FSD) within Credible Minimum Deterrence (CMD), showcasing Pakistan's responsible nuclear stewardship and its advocacy for a Strategic Restraint Regime in South Asia.

Air Commodore (R) Khalid Banuri moderated Session I, "Emerging Technologies and the Concept of Deterrence in the Contemporary World Order," to explore the evolving dimensions of deterrence in the face of emerging and disruptive technologies (EDTs). Dr. Han Hua discussed trilateral nuclear dynamics among China, Russia and the US in her discussion on "Nuclear Deterrence, Emerging Technologies and Great Power Competition." Dr. Xia Liping presented an analysis on

Reshaping Strategic stability by Emerging and Disruptive Technologies, highlighting the impact of hypersonic weapons, AI and cyber warfare on conflict paradigms. He advocated global AI arms control and a No-First-Use pledge to maintain deterrence equilibrium. Dr Naeem Salik examined the influence of "Emerging and disruptive technologies on Nuclear deterrence," explaining the risks of inadvertent escalation and miscalculation on the conventional-nuclear threshold due to hypersonic systems and dual-use technologies. Mr. Dmitry Stefanovich offered a perspective on "influence of Emerging Technologies on the Changing Character of War," cautioning the world regarding erosion of the arms control regime due to space, cyber, and hypersonic capabilities. Dr. Alexander Evans provided insights into the human dimension of deterrence in his presentation on "Strategic Alliances in the Age of Emerging and Disruptive Technologies, stressing the need for maintaining transparency in managing technological surprises."

Dr. Anum Riaz, chaired Session II, Impact of Militarization of Artificial Intelligence, discussing the impact of AI on strategic stability. Dr Petr Topychkanov cautioned about the integration of AI into the nuclear decision-making process. Ms. Alice Saltini discussed the vulnerabilities of automated nuclear command systems in her presentation on the Impact of AI on NC3. Dr. Jean- Marc Rickli stressed the moral hazards of lethal autonomous weapons in his discussion on Militarization of AI: Security, Legal and Ethical Perspectives. Dr. Zafar offered a perspective on South Asia's Nuclear deterrence. Session II concluded by highlighting the importance of "human-in-the-loop" mechanisms for responsible use of AI in security domains.

Session III titled "Emerging Technologies and peaceful use of Nuclear Technology," chaired by Dr Rahat, articulated the positive aspects of technology integration. Mr. Anton V. Khlopkov highlighted the role of emerging technologies in expanding the scope of peaceful nuclear application. Dr Robert B. Hayes linked technological innovation with clean energy. Dr Tariq Rauf stressed the importance of nuclear safety and security in the digital era.

A Special Session titled 'A Conversation with General Zubair Mahmood Hayat' was moderated by Dr Bilal Zubair, Director Research, CISS. The session featured Gen. Zubair Mahmood Hayat, Former CJCSC, who contextualized South Asia's deterrence challenges within an increasingly volatile global environment shaped by the erosion of arms-control regimes, normalization of force, and the rise of multi-domain deterrence encompassing AI, space, and cyber domains. He cautioned that India's unchecked military expansion and ideological trajectory risk destabilizing the region's fragile strategic equilibrium.

Session IV, on Quantum, Cyber Technologies, and Autonomous Weapon Systems, chaired by Ms. Anum A. Khan, explored the influence of quantum technologies on deterrence. Mr. Vladislav Chernavskikh, Dr. Jessica West, Dr. Laetitia Cesari, and Dr. Rizwana Abbasi unanimously agreed that quantum and cyber disruptions affect strategic opacity.

Session V, moderated by Dr. Adil Sultan, focused on the weaponization of Space and advancements in Missile Technology, discussing the militarization of outer space. Speakers, including Ms. Almudena Ortega, Ms. Anna Belolipetskaia, Dr Christine Leah, and Prof. Dr Zafar Nawaz Jaspal, characterized space as the "new battlefield". Session highlighted the role of unchecked competition in outer space, transforming the modus operandi of warfare.

Session VI, moderated by Dr. Asma Khwaja, explored Emerging Technologies and Arms Control, examining the prospects of arms control in the era of technological disruption. Speakers, including Prof. Dr. Andrey Pavlov, Mr. He Miao, Brig. (R) Dr. Zahir Kazmi, and Dr. Olamide Samuel, unanimously advocated for a review of international law in the era of emerging and disruptive technologies.

Executive Summary

The key points of the two-day CISS International Conference on Nuclear Deterrence in the Age of Emerging Technologies are as follows:

- Traditional ideas of strategic stability, based on mutual vulnerability and the logic of assured retaliation, are increasingly strained by rapid technological progress. The speed and range of new technologies have created fresh uncertainties in crisis situations, challenging the predictability that supported the nuclear deterrence framework for many years.
- AI-enabled surveillance, precision strike systems, and autonomous decision-making tools are shortening decision timelines during crises. This faster pace raises the risk of miscalculations or unintended escalation. Incorporating AI into early warning and targeting systems risks creating "use it or lose it" pressures during tense moments between nuclear-armed nations.
- The dual-use nature of emerging technologies—where civilian innovations can be used for military purposes—complicates global efforts to regulate their deployment. The growing accessibility of these technologies also raises concerns about non-state actors gaining capabilities that could trigger or worsen crises.
- AI is increasingly integrated into Nuclear Command, Control, and Communications (NC3) systems, missile defense architectures, and unmanned platforms. While these upgrades may enhance efficiency and accuracy, experts warn that excessive automation could impair human judgment in critical decisions, potentially undermining the "human-in-the-loop" principle, which is crucial for nuclear stability.
- The ethical, legal, and operational frameworks for military AI applications are still underdeveloped. Without globally

accepted norms and guidelines, there is a significant risk of an AI-driven arms race. International cooperation and confidence-building measures (CBMs) are emphasized as crucial for ensuring transparency and accountability.

- Quantum technologies, especially in computing, sensing, and secure communication, are viewed as having both stabilizing and destabilizing potential. While quantum encryption can improve the security of communication systems, advances in quantum computing may also threaten existing encryption methods, creating new vulnerabilities in critical systems.
- Cyber vulnerabilities in nuclear command and control systems are increasingly critical. A cyberattack on strategic networks could easily be misinterpreted as an act of war, leading to unintended escalation. Strengthening cyber defenses and developing crisis communication channels among nuclear powers were highlighted as urgent priorities.
- The evolution of Lethal Autonomous Weapons Systems (LAWS) is blurring the distinction between conventional and strategic warfare. Delegating lethal decision-making to machines raises profound moral and operational challenges that could destabilize deterrence dynamics if left unregulated.
- Participants expressed concern over the accelerating weaponization of outer space, warning that it threatens the foundational principles of the Outer Space Treaty (OST). The conference emphasized the importance of inclusive space governance mechanisms, particularly in light of the growing role of private actors and parallel frameworks such as the Artemis Accords.
- Ongoing missile modernization efforts, including the development of hypersonic delivery systems, are fueling new arms races both regionally and globally. The capability of these systems to evade existing defenses and deliver strikes at unprecedented speeds increases strategic instability.
- While much of the focus was on risks, the conference also highlighted the positive applications of emerging technologies

in enhancing nuclear safety, improving energy efficiency, and supporting the UN Sustainable Development Goals (SDGs). However, participants warned that disparities in access and restrictive export controls might increase the technological gap between developed and developing countries.

- Existing arms control treaties and mechanisms are increasingly outdated in addressing new threats emerging from AI, cyber warfare, and space militarization. There was consensus that traditional non-proliferation frameworks urgently need modernization to reflect the realities of the 21st century.
- Speakers emphasized the need to establish new multilateral frameworks focusing on transparency, confidence-building, and legally binding mechanisms for the responsible development and deployment of emerging technologies. Such frameworks should ensure equitable participation and avoid discriminatory restrictions that marginalize developing states.
- In the South Asian context, the integration of AI into India's defense modernization — supported by advanced cooperation with the United States — was identified as a serious challenge to Pakistan's strategic balance. Participants stressed that this evolving asymmetry could destabilize regional deterrence if not addressed through dialogue and mutual restraint.
- The conference concluded with a strong call for sustained regional dialogue on the implications of emerging technologies. Scholars and policymakers agreed that cooperative frameworks, transparency measures, and joint research initiatives could help prevent crisis escalation and maintain credible deterrence in South Asia.

Welcome Remarks

Amb Ali Sarwar Naqvi
Executive Director, Center for International Strategic Studies, Islamabad

Assalam o Alaikum and a very Good Morning!

I welcome all worthy participants, distinguished guests, and eminent speakers from around the world to the International Conference on "Nuclear Deterrence in the Age of Emerging Technologies," organized by the Center for International Strategic Studies in Islamabad. Emerging technologies are among the factors transforming nuclear deterrence, posing a challenge to global stability. This conference will examine how emerging technologies such as AI, cyber capabilities, and autonomous weapons are transforming nuclear deterrence.

We will assess the militarization of AI and its security implications, particularly for South Asia. Subsequent sessions will examine quantum computing, cyber threats, and autonomous systems; space weaponization, missile advancements; peaceful nuclear applications, and their role in achieving the United Nations' Sustainable Development Goals. Finally, discussions will focus on the present and future of arms control in this era of technological disruption.

Today, we gather here at a pivotal moment in global history. Emerging technologies are the backbone of our modern world. The global nuclear security architecture is going through a transformation due to rapid technological advancements in the military domain. In particular, the interplay of technological dynamics serves as a catalyst in exacerbating geopolitical rifts and impacting nuclear deterrence. In the absence of comprehensive legal instruments, we are facing critical challenges posed by the unregulated development of AI, autonomous weapon systems, weaponization of outer space and cyber warfare.

These challenges are altering the characteristics of modern warfare, igniting new conflicts and reigniting old rivalries. A new approach to counterforce targeting is evolving with an increasing role of non-nuclear strategic weapons in the strategy of nuclear powers. The integration of these emerging technologies into strategic doctrines without consensus-based regulatory frameworks poses serious risks to crisis stability and arms control efforts.

What's important right now is understanding the bigger picture. Advanced technologies such as AI, cyber and autonomous systems have the potential to destabilize the global order. More specifically, their integration into military systems risks eroding the delicate balance that has prevented nuclear conflict for decades. The conflicts in Europe and the Middle East show how autonomous systems, real-time satellite intelligence, cyber warfare, and precision-guided munitions are changing the dynamics of warfare. Also, in the Middle East, Israel's war against Palestine has highlighted the growing use of cutting-edge technology for warfare. Moreover, the increasing use of unmanned vehicles and AI-enhanced surveillance in asymmetric warfare is raising new ethical, legal, and strategic challenges for international peace and security. These global events indicate how emerging technologies are not only transforming conflict at the tactical level but are also eroding present deterrence frameworks.

Meanwhile, the U.S.-led minilateral security arrangements, such as AUKUS (Australia, UK, U.S.) and QUAD (U.S., India, Japan, Australia), are accelerating the integration of advanced military technologies in the Asia-Pacific. The AUKUS pact, which includes the deal for nuclear-powered submarines and other advanced defense technologies, raises legitimate concerns about regional stability. This shift in military balance could potentially undermine not just the established deterrence between major powers but also regional deterrence stability. Similarly, QUAD's growing security cooperation is leveraging India's military growth in the region. India's military strength is reshaping regional power balances, threatening its

neighbors, particularly Pakistan, through the acquisition and integration of enhanced military systems through defence deals with major powers. These developments increase the risks of strategic instability and miscalculation among littoral states in the whole Asia-Pacific region.

The challenges are stark, yet they need a balanced approach. Emerging technologies present both opportunities and threats. On the one hand, they are strengthening safety, security, and peaceful applications of nuclear technology. On the other hand, they are raising serious concerns about strategic stability. The promising role of AI-driven technologies, quantum computing, space technologies and other emerging technologies must align with the sustainable development goals for the peaceful applications of nuclear science. In this regard, the path forward demands inclusive multilateralism, where emerging technologies serve sustainability rather than strategic rivalries.

Over these two days, the esteemed experts, scholars, policymakers and practitioners from different parts of the world will engage in enlightening discussions with a collective call for action. We must facilitate open dialogue and exchange ideas to strengthen deterrence stability and aim for conflict resolution in South Asia as the end goal. Together, we can explore new frontiers, confront emerging challenges, and develop a course that fosters a future-oriented approach to ensure strategic stability in the region and beyond.

On behalf of CISS, I again welcome you to this vital exchange. I wish all our guests from abroad a pleasant stay in Pakistan. Thank you all for your valuable time and worthy presence.

Keynote Address

General Sahir Shamshad Mirza, NI (M)

Chairman Joint Chiefs of Staff Committee

We are witnessing the emergence of a multipolar world, with the newly coined notion of "fluid multipolarity" gaining currency. New power centers and rising regional players are challenging the traditional dominance of the West and its institutions, making the global landscape increasingly contested. Secondly, there are notable changes and a resurgence in the geopolitical discourse. The primacy of geoeconomics, which once dominated international relations, is under stress. Today, we observe a multifaceted approach to global affairs, wherein energy posturing, ideological battles, and economic leverage are gaining prominence, and security now often takes precedence over trade.

Thirdly, there is great power contestation. We are observing a recalibration of the balance of power, with an emphasis on issue-based partnerships rather than traditional alliances. Emerging technologies, such as AI, cyber capabilities, electronic warfare (EW), space, and other niche domains, are becoming principal constituents of power contestation. The world is witnessing an intensifying U.S.-China competition, which is significantly driving this recalibration of global power structures. Fourthly, rising hyper-nationalism and populism are colliding with the erstwhile concepts of globalization. The shockwaves from intensified trade wars have accelerated this trend, with the potential for severe socio-economic impacts, leading to increasingly polarized internal dynamics. The post-World War II international order, built upon multilateral collaboration, is now under considerable stress. This is reshaping domestic politics while undermining international institutions such as the United Nations (UN), the World Health Organization (WHO), among others, and threatening the essential pillars of the existing global order.

Finally, the revolutionary power of emerging technologies is rapidly transforming societies, economies, instruments of warfare, and security paradigms at an unprecedented pace. These technologies are not merely enablers or force multipliers; they are catalysts for profound shifts, redefining the contours of power and the geostrategic balance.

In geopolitics, the notions of the "return of the right", the "rise of the rest" and "Global North versus Global South" are echoing with greater resonance. Developing nations are demanding greater representation and influence in global decision-making processes. We observe an increasing trend toward middle power activism, regionalism, and exceptionalism, as manifested in the emergence of frameworks such as AUKUS and the Quadrilateral Security Dialogue. However, these frameworks are being extensively criticized for complicating non-proliferation regimes, arms control consensus, and cooperation on non-traditional security challenges.

There is also an unchecked and imprudent policy of providing free rein to certain ambitious countries, which increases confrontation in various forms and categories. Smaller states are being forced into making constrained alignment choices, thereby limiting their policy and strategic options.

On the geo-economic front, we see a reshaping of global trade. The world is bracing for a full-blown escalation in tariff wars, with national interests, protectionist tendencies, and great power rivalries at the forefront. The intensification of competition for control over critical resources, even among long-standing allies, is driving a resurgence of economic nationalism and casting a deep shadow over global economic interdependence. Moreover, there is a weaponization of economic influence, where trade policies and export controls are increasingly serving as tools of strategic coercion.

In the Volatile, Uncertain, Complex, and Ambiguous (VUCA) domain of geostrategy, we observe that all states, developed powers, developing countries, and regional drivers alike, are competing not

only in traditional domains but also in cutting-edge defense technologies. There is an evident erosion of traditional security guarantees and defense architectures. Natural products and emerging cracks in past normative frameworks, particularly concerning sovereignty and territorial integrity, are compelling nations to pursue enhanced military and strategic defense capabilities.

This trend is fueling a surge in global military spending at the expense of social development, thus heightening the risks of armed conflicts. Modern conflict has evolved far beyond traditional battlefield confrontations. Today, adversarial power is increasingly projected through proxy networks, private militias, and hybrid campaigns targeting national centers of gravity. Interestingly, these methods allow states to circumvent traditional deterrence architectures and achieve their underlying strategic objectives.

The defining elements of state power are undergoing fundamental transformations, challenging traditional notions of balance and deterrence in interstate relationships. The pursuit of military domination is creating new and niche areas of strategic competition with profound implications for both regional and global environments. Amidst this sharper competition, non-traditional security challenges, such as climate change, pandemics, piracy, population management, food security, and cybersecurity, seem to have taken a back seat.

The world has shielded itself from chronic conflict hotbeds, including Palestine and Indian Illegally Occupied Jammu and Kashmir (IIOJ&K). This neglect has undermined global confidence in the international system's ability to limit socio-economic and ideological discontent.

If I were to summarize the global environment today, I would confidently say: The global order is in a state of disorder. The discounting of international security architectures, coupled with an increasing resort to the use of force with impunity to resolve disputes, has more traction today than ever before. Conflicts have become too many and too complex. The ideational values of a rule-based world

order, fundamental human rights, state sovereignty, territorial integrity, and international justice seem to have been somewhat lost.

How the world transitions into a new global order will largely depend upon the approaches taken by world powers: will it be through decoupling or delisting, accommodation and cooperation, contestation, or open kinetic rivalries leading to catastrophic showdowns? Or will it be a specific combination of these pathways? Ladies and gentlemen, that remains to be seen.

In Europe, economic growth is slowing, migration pressures are increasing, and there is a visible rise of the right. The protracted nature of the Russia-Ukraine conflict has stressed transatlantic partnerships and exacerbated economic and other vulnerabilities. Consequently, Europe is shifting its focus from soft power to hard power to address these vulnerabilities. The ongoing reshaping through the notion of a "rearmed Europe" will likely undermine and stress international norms related to non-proliferation, disarmament, and the transfer of critical technologies.

In the Asia-Pacific and Indian Ocean Region, we observe intense strategic alignments, with increased militarization and strategic competition. Strategic patronization of certain states has significant implications not only for the region but also for contiguous regions, especially South Asia. With the presence of five out of the nine nuclear powers, the involvement of resident and non-resident states, and an increased military build-up, the region – instead of expanding partnerships and prosperity – is on the course of becoming the next frontier of military competition.

The Middle East continues to grapple with complex security challenges, ranging from ideological divergences to civil wars. The unprecedented Israeli atrocities committed in Palestine, especially during the Israel-Hamas conflict, have not only weakened the Palestinian cause but also testified that lasting peace in the Middle East is not possible without a just resolution of the Palestinian issue.

Inadequate action in response to over 50,000 deaths and the displacement of millions in Palestinian territories because of Israeli genocide remains an ugly blemish on the professed global values of liberty, freedom, fairness, and equality.

Pakistan has been one of the most consistent proponents of a two-state solution. We firmly believe that an enduring solution to the conflict resides in the creation of a viable, independent, and contiguous State of Palestine, based on the pre-June 1967 borders, with Al-Quds Al-Sharif as its capital, in accordance with relevant United Nations resolutions. Encouragingly, much of the world seems to be coming around to that conclusion today.

Turning to Afghanistan, the country is grappling with an unsettled government, a lack of critical social infrastructure, and incomplete control by the Taliban-led government. The resulting ungoverned spaces are occupied by Al-Qaeda and other international terrorist organizations, such as Islamic State – Khorasan Province (ISIS-K), Tehrik-i-Taliban Pakistan (TTP), and Islamic Movement of Uzbekistan (IMU). These ungoverned spaces, coupled with the absence of effective state control, present serious concerns, particularly regarding the use of Afghan soil for conducting terrorist activities inside Pakistan. Given the capabilities that currently reside inside Afghanistan, it should not surprise us if these figures lead to a situation even graver than 9/11 in the future.

Firstly, the global nuclear landscape remains intricate, challenging, and far more imperiled by strategic competition, nuclear multipolarity, and regional and extra-regional rivalries, particularly between nuclear-armed nations. While progress has been made in arms reduction and restricting the number of nuclear-armed nations to nine, contrary to President Reagan's fears of this number reaching 25, the world still faces the reality of thousands of nuclear weapons.

Another important point is that the deterrence architectures, which were designed in a bilateral context and marked by delicate diplomacy,

close talks, and strong-minded persistence, find limited applicability in today's complex geopolitical environment. The resurgence of nuclear rearmament as a byproduct of geostrategic contestation has led to the near collapse of bilateral arms control frameworks, while there remains little hope for any trilateral arms control arrangement between states.

Fifth, great powers are modernizing their nuclear arsenals and diversifying their nuclear triads, revisiting and even changing their nuclear doctrines and strategies. The transfer of nuclear-powered submarines outside of traditional frameworks is likely to set a dangerous precedent, encouraging similar ambitions among others and thereby challenging the spirit of the global non-proliferation regime.

Furthermore, the integration of emerging technologies into the strategic domain poses significant risks to the delicate equilibrium, especially among nuclear-armed states that already have underlying political disputes and geographical contiguity. The emergence of AI-powered tools for nuclear research, uranium enrichment, and warhead design could lower technical barriers for aspiring nuclear states, posing additional challenges to non-proliferation and strategic stability. AI-enabled nuclear systems may strengthen command and control systems but simultaneously affect strategic stability, especially if actors in an unmanaged arms race gain any level of autonomy in these systems.

Autonomous and even automated nuclear capabilities risk rendering domains of human prudence, such as deterrence, escalation control, nuclear diplomacy, and globally agreed conflict management norms, meaningless.

Technologies today are vastly different from those of the past. They have relatively minimal state control, are widely available off the shelf, have huge disruptive capabilities, and are easy to proliferate. Emerging Disruptive Technologies (EDTs) have challenged the fundamentals of the global balance of power, conflict management mechanisms,

strategic stability, deterrence regimes, and the character of future conflicts.

Techniques and strategies associated with most emerging technologies are inherently dual-use, particularly AI, cyber, biotechnology, and quantum computing – serving both civilian and military purposes. This dual-use character complicates arms control and verification regimes, erodes transparency, and undermines strategic balance and deterrence.

Rapid innovation outpaces the development of global norms, legal frameworks, and ethical guidelines, creating gaps in politico-military oversight. International regimes struggle to adapt, particularly in regulating possible militarization of AI and lethal autonomous weapons systems (LAWS) and ensuring data governance.

Non-kinetic capabilities like cyber-attacks, information warfare, and AI-driven systems have emerged as powerful tools to circumvent traditional security architectures. Rapid technological advancements are democratizing access to destructive capabilities, enabling non-state and private entities to wield unprecedented power while weakening traditional deterrence postures.

The weaponization of space and advancements in missile technologies present new challenges. Developments like space-based missile defenses and hypersonic glide vehicles open new pathways for arms races and inadvertent miscalculations. Moreover, breakthroughs in surveillance and reconnaissance are eroding the traditional secrecy surrounding nuclear force postures, infrastructures, and movements, increasing the risk of preemptive strikes and undermining second-strike assurances.

The integrity and stability of nuclear command, control, and communication systems face unprecedented risks from the integration of AI, quantum computing, and cyber warfare into offensive strategies. The potential influence of EDTs could catastrophically impact national, regional, and global security architectures. These technologies have

already started to dilute the traditional hegemony of nuclear arsenals as instruments of deterrence. Forecasting the synergistic capacities of emerging technologies with nuclear capabilities to reconstruct deterrence theories is a daunting challenge. Recent concepts like integrated deterrence devised by the West testify to this emerging reality.

Let me now connect how broader geopolitics undermines strategic stability in South Asia and perpetuates security dilemmas for a country like Pakistan.

Within the overall geostrategic context, the outlook of South Asia is being shaped by geopolitical rivalries. The technical character of the China-India-Pakistan equation, complicated Iran-West relations, instability in Afghanistan, strategic patronization of India, and unresolved India-Pakistan disputes, with Kashmir at the center stage, complicate matters significantly.

Kashmir remains a major settlement issue critical for enduring peace in South Asia. India today is gaining leverage as a so-called "net security provider," a misplaced notion that defies principles of power equilibrium and disregards geopolitical rationality.

India's bid for NSG membership, significant Western support, and its de jure status as a nuclear weapons state raise serious questions about the neutrality and spirit of non-proliferation regime, given India's deficient nuclear safety record and recurrent incidents involving illicit nuclear material trade and the BrahMos missile misfire. These issues warrant strict international scrutiny. Over the past decade, India has persistently escalated its nuclear rhetoric. Its pursuit of ballistic missile defense capabilities, deployment and expansion of SSBN fleets, and continuous testing of intercontinental ballistic missiles are inconsistent with the principles of minimum deterrence. These capabilities hint at ambitions beyond South Asia and into the extended region.

The 2019 Balakot episode demonstrated the dangerous potential for uncontrolled escalation and the blurring of conventional and nuclear thresholds. Pakistan responded firmly, exhibiting its resolve to protect national sovereignty while also displaying maturity by returning the captured Indian pilot as a goodwill gesture. However, the crisis underscored the fragility of strategic balance and the perpetual danger of inadvertent escalation.

The cumulative effect of these destabilizing developments is twofold. We have a neighbor emboldened by geopolitical relevance and willing to undertake military misadventures without taking cognizance of unaffordable nuclear escalation. The strategic enabling of India, coupled with commitments denied to Pakistan, creates an iconic conventional asymmetry gap, thus narrowing our strategic choices.

Pakistan's reliance on nuclear weapons is for deterrence against external aggression and defense of the nation. Contrary to Indian assumptions, Pakistan believes there is no space for limited war under the nuclear overhang. Without engaging in an arms race, we have demonstrated our resolve, capability, and will counter any military misadventure by India. The international community must consider Pakistan's perspective on its nuclear capability.

Firstly, our strategic program was and continues to be undeniably need-driven, not prestige-driven. Pakistan's difficult security circumstances compelled the pursuit of a nuclear program. Secondly, given our zero expansionist designs, the program remains purely defensive. Pakistan's strategic perception emanates solely from what India does – and does not do – to maintain a strategic equilibrium.

Thirdly, our program is aimed at deterring war and escalating unintended conflicts. Repeated crisis management experiences show that this objective has been achieved – there has been no full-scale war between Pakistan and India for over a quarter-century, reinforcing the notion that nuclear deterrence works. Thus, Pakistan's strategic capability has proven the skeptics wrong. We fully understand that this

capability must continue to play a positive role. In addition to statecraft, robust bilateral warning and communication mechanisms, and shared understandings of the consequences of nuclear exchanges are critical.

Pakistan is a responsible nuclear state. We have consistently played an active role in issues of arms control, disarmament, non-proliferation, and the peaceful use of nuclear technology. We believe that principles of equal and undiminished security for all, and non-discriminatory behavior will strengthen strategic stability, complement arms control, and reduce nuclear risks.

Pakistan is fully aligned with UN initiatives promoting international cooperation in peaceful nuclear technology use. We have consistently called for Pakistan's inclusion in relevant international forums, including the Nuclear Suppliers Group (NSG), based on non-discriminatory criteria. Our strong nuclear safety and security record demonstrates responsible stewardship. We oppose the militarization and weaponization of outer space and cyberspace. These global commons should be used for socioeconomic development rather than conflict.

Pakistan reaffirms its support for nuclear disarmament and responsible acquisition of emerging technologies under international security frameworks. We denounce discriminatory nuclear policies and urge legally binding assurances for non-nuclear states. We believe the UN must adopt multilateral approaches to mitigate the destabilization risks posed by military AI.

In conclusion, the unattended weaknesses of the global system have ushered in a new geopolitical competition. This competition feeds not only on longstanding security concerns but also on new threats arising from technological advancements. Multilateral, trilateral, and bilateral arms control architectures are under significant stress across the globe, giving way to a new "rules-based" order marked by reformed particularism and a return to selective globalization.

Emerging technologies, especially in niche areas, are fast becoming principal sources of competition. A cooperative approach must be adopted to harness their potential while ensuring strategic stability.

Selective access to civilian and military technologies, driven by geopolitical preferences, will continue to stress global stability. Humanity cannot afford divisive approaches at this critical juncture.

The integration of emerging technologies into the strategic domain poses profound risks, especially among nuclear-armed states. A nuanced approach is required – one that accounts for diverse strategic cultures, postures, alliance dynamics, and historical experiences.

This emerging challenge necessitates a reimagining of strategic stability and confidence-building frameworks to address the realities of a multipolar nuclear world.

Peace and stability in South Asia can only be achieved through the resolution of outstanding disputes, especially Kashmir. The reciprocal measures for nuclear risk reduction institute balance in the wider geostrategic context. Pakistan's proposal for establishing a Strategic Restraint Regime in South Asia is geared towards achieving these objectives. However, this initiative needs committed partners.

Durable peace in South Asia is not possible without a just resolution of the Kashmir dispute, based on UN resolutions and the aspirations of the Kashmiri people. Pakistan remains committed to providing political, moral, and diplomatic support to the Kashmiri cause. Pakistan desires the normalization of relations with India based on peaceful coexistence, sovereign equality, dignity, and honor. This is fully aligned with the UN Charter, international law, and International Humanitarian Law.

However, Pakistan's persistence in pursuing peace must never be misconstrued as weakness. Pakistan remains committed to maintaining Full-Spectrum Deterrence (FSD) within the bounds of

Credible Minimum Deterrence (CSD), conscious of the consequences for the region and the wider world. Pakistan is a natural balance center – a bridge point – with a vibrant, forward-looking society, a vital geostrategic location, a rich demographic profile, a robust system of armed forces, and a responsible strategic capability. Harnessing our potential and ensuring our stability are common interests for all.

Session-I

Emerging Technologies and Concept of Deterrence in Contemporary World Order

Moderator: Air Cdr Khalid Banuri (R)
Senior Advisor Training, Air Force Headquarters, Pakistan

Nuclear Deterrence, Emerging Technologies and Great Power Competition

Dr Han Hua
Director of Arms Control and Disarmament at the School of International Studies, Peking University, China

The U.S. increasingly frames China as both a strategic competitor and an adversary. This lens shapes a broader debate about the global balance of power: some analysts see an emerging U.S.–China–Russia trilateral, others a predominantly U.S.–China bipolarity, and still others the persistence of U.S.-led unipolarity. Regardless of the interpretation, the central dynamic remains the evolving dynamics among great-powers.

A new wave of strategic competition has emerged across conventional, nuclear, and technological domains. Deterrence, once defined by the bipolar U.S.-Soviet rivalry of the Cold War, has evolved into a more complex and integrated framework. The growing interlinkage between nuclear and conventional forces and the emergence of disruptive technologies have transformed traditional nuclear deterrence into a multi-domain concept, especially in a multipolar world.
A 'two-peer' nuclear problem is emerging, where the U.S. must simultaneously contend with two nuclear-armed rivals: Russia and China. This trilateral configuration introduces complexities far beyond the Cold War-era bilateral model. Increasing China-Russia cooperation further complicates deterrence calculations, particularly in the two main theaters of concern: Europe and the Asia-Pacific.

There is a notable shift in U.S. nuclear policy discourse, from a narrow focus on deterrence towards potential warfighting roles and cross-domain integration. Although early signals from the President Biden's administration initially raised expectations for adopting a 'sole purpose' doctrine in its 2022 Nuclear Posture Review, this did not

materialize. The recent U.S. Department of Defense guidance emphasizes more focus on the integration of nuclear forces with conventional, cyber, and space-enabled operations by framing nuclear capabilities within broader campaigns in contested multi-domain environments including space warfighting.

The concept of deterrence has expanded further with technological advancement. Under President George W. Bush, the idea of a 'new nuclear triad' reframed U.S. deterrence around three pillars: offensive strike like nuclear and advanced conventional, active and passive defenses including missile defense, and a responsive defense infrastructure. The Biden administration has formalized 'integrated deterrence,' which now includes space and cyber capabilities. Correspondingly, force structures have adapted: China elevated the PLA Rocket Force in 2015, and the U.S. established the Space Force in 2019, both institutional signals of deterrence shifting into space, cyber, and precision-strike domains.

Artificial intelligence (AI) and cyber technologies are increasingly embedded into Nuclear Command, Control, and Communications (NC3) systems, fundamentally reshaping escalation dynamics, decision timelines, and attack-surface risk. This technological shift is unfolding alongside a more forward-leaning posture in U.S. extended deterrence. In Europe, U.S. is reportedly restoring nuclear infrastructure in the UK, plans a rotational presence of intermediate-range fires in Germany. Thus, tightening integration with allied air and missile defenses. In the Asia-Pacific, the U.S. Declaration has increased the visibility and tempo of U.S. strategic assets on the Korean Peninsula, including bomber task forces and SSBN port calls. Moreover, new land-based systems such as the Typhon and other anti-ship capabilities are being fielded in the Philippines. Together, NC3 digitization and these theatre deployments signal a move toward tighter cross-domain integration of nuclear, conventional, cyber, and space enablers in support of extended deterrence.

The emerging deterrence architecture carries substantial risk. First, investments in advanced nuclear, missile-defense, and space enablers could catalyze a renewed arms race among major powers. Second, escalation dangers including deliberate or inadvertent, both are rising across key flashpoints (South China Sea, Taiwan Strait, the Middle East, Eastern Europe), where dense mixes of nuclear, conventional, cyber, and space capabilities compress decision times and blur thresholds. Added vulnerabilities to nuclear facilities and early-warning systems increase incentives for pre-emption and raise the risks of miscalculation.

The international arms-control architecture is fraying. Beyond New START which is set to expire in February 2026 with no agreed successor, these key arrangements have weakened or collapsed, including the U.S. withdrawal from the ABM Treaty, the demise of the INF Treaty, erosion of Open Skies, and the non-entry of CTBT into force. Meanwhile, verification norms and crisis-management channels are diminishing just as emerging technologies expand strike options and compress decision times. Navigating this environment will require pragmatic, issue-specific cooperation among nuclear-armed states and the wider international community. By prioritizing risk-reduction measures including hotlines, incident-prevention agreements, notification regimes, transparency and verification initiatives, and renewed dialogue on strategic stability.

Reshaping of Strategic Stability by Emerging and Disruptive Technologies

Dr Xia Liping
Director of the Center for Polar and Oceanic Studies, Tongii University, China

The rapid advancement in science and technology are reshaping both warfare and strategic deterrence. The diffusion of unmanned systems, AI-enabled command and decision support, and advanced weapons based on physical principles like high-energy lasers and electromagnetic pulses, has sparked a significant military shift. These capabilities compress timelines, widen attack surfaces, and blur domain boundaries, with consequential implications for global and regional strategic stability.

The rise of high-end technologies poses complex challenges to strategic stability. AI, increasingly described as a "new killer," is fundamentally reshaping the rules of war and deterrence. Rather than simply enhancing existing platforms, it is causing a qualitative transformation in warfare. The Russia–Ukraine war is widely assessed as the first major conflict to employ AI-enabled systems at scale for sensing, targeting, EW, and autonomy, and it has coincided with the most acute nuclear rhetoric and signaling since the Cold War, at times elevating concerns about potential battlefield nuclear use.

The large-scale deployment of AI-enabled conventional weapons has direct consequences for strategic stability. Like, Precision-strike systems that fuse AI targeting with deep-penetration munitions could threaten hardened or underground nuclear command nodes, raise decapitation fears and incentivize pre-delegation, launch-on-warning, or early nuclear use. An even greater risk is the creep of algorithmic decision-making into nuclear command and control. If machines are allowed to shape or substitute for human judgment under time pressure, model error, adversarial spoofing, or data bias could drive

actions leaders would normally avoid. These dynamics argue for strict "human-in-the-loop" safeguards, red-teaming of AI models, and clear firebreaks between conventional AI systems and nuclear decision chains.

AI is reshaping warfare across space and cyber domains, with future deterrence architectures expected to accelerate and reconfigure the command-and-control by fusing automated sensing, decision support, and effects. Hypersonic weapons have emerged as a new class of strategic deterrents with superior speed, manoeuvrability, and penetration; nascent counter-hypersonic defences lag, introducing fresh instability risks. Air dominance now extends across sea control and the electromagnetic spectrum, while orbital assets have become indispensable for ISR, navigation, and resilient communications, as illustrated by commercial constellations employed in Ukraine. Looking ahead, conflict is likely to be defined by seamless, multi-domain integration across land, sea, air, space, and cyber which are bind together by power grids and digital command networks, thereby reframing the speed, thresholds, and logic of deterrence.

Cyber deterrence has become integral to strategic stability. Cyberspace is now a primary domain of military competition, where states develop tools to disrupt important infrastructure and assert control across other domains. The militarization of cyberspace which is paired with new doctrines for offensive cyber operations and on-going efforts to draft cyber rules of engagement have significantly increased the risk of strategic miscalculation, especially given challenges of attribution, proportionality, and escalation control. Meanwhile, the growing scale and sophistication of state-linked intrusions, criminal hacking, and cyberterrorism present serious threats to international security and critical infrastructure. Furthermore, biosecurity has also gained prominence. The COVID-19 pandemic highlighted how biological threats, whether naturally occurring, accidental, or deliberate, can impact national and global security. Thus, as dual-use biotechnology (e.g., rapid sequencing, gene editing, synthetic biology) proliferates,

states must treat bio surveillance, laboratory security, attribution mechanisms, and consequence management as core elements of deterrence and crisis stability, not public-health add-ons.

AI is increasingly integrated into U.S. military systems with direct implications for China-U.S. strategic stability. It is being extended beyond conventional capabilities into nuclear domains to preserve American military superiority. This militarized application of AI not only enhances weapon systems but also accelerates decision-making and execution, collectively known as the "kill chain" from detection to efforts. As AI becomes more embedded across military systems, future warfare will be characterized by faster sensing, rapid decision cycles, and high-speed engagement, what is now being described as "intelligent warfare", that raise both effectiveness and escalation risks.

The US has extensively integrated AI into its military operations. In practice, commanders rely on AI systems to process large volumes of data in real time, generating insights that guide strategic decisions. This cycle of observation, judgment, and action is increasingly supported by AI. Notably, the U.S. military's nuclear intelligence, surveillance, and reconnaissance systems now use AI to identify and classify targets, including missile silos and nuclear facilities. These systems can also predict missile launches. The 2022 introduction of the Joint All-Domain Command and Control (JADC2) concept marked a significant shift in military integration. JADC2 connects combat systems and sensors across land, sea, air, space, and cyber domains. AI provides commanders with real-time situational awareness and analytics, enabling faster and more precise decisions. The parallel rise of autonomous weapon systems, backed by AI, has raised global concerns about the temptation of launching pre-emptive nuclear strikes.

AI-enabled strategic strike capabilities which are degrading China's second-strike capability, thus strengthening U.S. deterrence and shifting the offensive-defensive balance. This increases the risk of crisis instability. While U.S. officials assert that nuclear decisions remain

under human control, the rapid pace of operations may prompt partial delegation to machines, especially during high-stakes scenarios. If normalized, such practices would blur firebreaks between conventional AI applications and nuclear command-and-control functions, raising the probability of misperception, inadvertent escalation, and pressure for launch-on-warning postures.

Strategic stability must be recast for the post–Cold War environment of multiple actors, diverse technologies, and overlapping domains. Stability today is inherently multilayered, linking nuclear and conventional forces with space, cyber, and AI-enabled C2, and must be adaptable to shifting balances of power and rapidly evolving capabilities. Legacy deterrence frameworks rooted in unlimited military buildup are no longer viable. As a baseline restraint, all nuclear-armed states should adopt a no-first-use (NFU) policy and align force postures accordingly. China already upholds NFU and encourages other major powers to reciprocate.

A global governance system for AI armaments is urgently needed. In the absence of international regulation, concerns about AI's strategic risks have amplified. States must collectively establish legal, humanitarian, and security norms that set restrictive principles, mandate transparency and incident-reporting, and establish operational guidelines (testing, validation, auditability, and meaningful human control) through consultation. Implementation should include tiered risk management that conditions development and deployment on safety milestones, red-teaming, and certification, thus, preventing premature fielding of high-risk systems. Private industry and research institutions must be integrated into norm-setting through standards bodies and public–private partnerships, helping define ethics, compliance, and assurance regimes for AI design, data governance, and use in command-and-control and weapons applications.

There is practical scope for U.S.-China cooperation on managing AI armaments. Both states should institute reciprocal testing and validation protocols, stand up AI/NC3 hotlines, exchange notifications on high-risk exercises, and launch a technical working group on arms-race stability and incident reporting. Along with that, both U.S. and Russia must play a leading role in restoring nuclear stability by negotiating verifiable reductions and a successor to New START. Meanwhile, the India-Pakistan strategic balance remains critical for regional peace. The crisis stability requires sustained risk-reduction measures including reliable hotlines, advance-notification regimes, and incident-prevention agreements, while preserving full human control over nuclear decision-making.

Preventing the militarization of outer space and promoting responsible cyber behavior are equally vital. China and Pakistan can contribute by shaping norms for orbital "sky-grid" constellations and AI-enabled warfare—through confidence-building measures, targeted treaties, and robust crisis-management frameworks that keep pace with intelligent warfare's speed and complexity.

Impact of Emerging and Disruptive Technologies on the Concept of Nuclear Deterrence

Dr Naeem Salik
Executive Director, Strategic Vision Institute, Pakistan

Emerging and disruptive technologies must be understood within the broader context of deterrence. The term 'emerging technologies' can be misleading, as such innovations typically undergo development phases spanning 15 to 25 years or more before becoming operational. Artificial intelligence (AI), for example, was first coined as a term at Dartmouth College in 1955. It remained largely theoretical until IBM's Deep Blue defeated chess champion Garry Kasparov in 1997, marking a public milestone. Nearly two decades later, Google DeepMind's AlphaGo defeated world champion Lee Sedol in a five-game Go match. These examples demonstrate the time lag between conceptualization and full operationalization of advanced technologies.

One major obstacle to the widespread adoption of emerging technologies is their prohibitive cost. Even after successful research and development, financial barriers often make mass deployment impractical. Furthermore, there is often a discrepancy between the advertised potential of these technologies and their actual performance in conflict settings. Technologies that appear effective in demonstrations may falter under the unpredictable conditions of war. Compounding this issue, counter-technologies are often developed simultaneously, with adversaries deploying measures to neutralize new systems almost as soon as they are introduced.

AI has already entered military domains, notably enabling the coordination of autonomous systems such as aerial and underwater drone swarms. These swarms can operate cohesively toward a shared objective, a task unmanageable by human operators alone. When human oversight is removed, the AI-driven decision-making cycle, commonly referred to as the OODA loop (Observe, Orient, Decide, Act), shortens dramatically. This allows forces supported by AI to

outpace adversaries using traditional systems. However, this speed advantage may intensify the competition to deploy AI-enabled capabilities, accelerating the automation of decision-making processes.

Autonomous weapons empowered by AI offer capabilities beyond those of manned platforms, including indefinite loitering over battlefields. This enhances continuous surveillance and allows real-time engagement, effectively turning modern warfare into a 24-hour combat environment. AI also boosts the ability to process and analyze massive volumes of data, a task that has become increasingly unmanageable for humans following the information explosion of recent decades. These capabilities, however, come with serious risks. Speed can undermine deliberation, and removing humans from the loop eliminates ethical and moral considerations in decision-making.

AI systems are only as effective as the data on which they are trained. Currently, the United States and China possess the largest and most sophisticated datasets, and they are unlikely to share this data. This results in an imbalance in AI development and operational capabilities. Furthermore, even when datasets are made available, they often reflect the biases of those who created them, potentially leading to asymmetries and inaccuracies in application. There is also the danger of data corruption or hacking, which could severely compromise decision-making processes and the integrity of military operations.

AI supported weapons and command systems may lack the sensitivity required to interpret the subtle political signals critical to deterrence during crisis situations. While human decision-makers can evaluate adversaries' intentions and strategic signals, machines operate strictly on predetermined algorithms. Deterrence is a psychological state reliant on signaling and perception, something AI cannot comprehend. Machines cannot read an adversary’s shifting intent in real time. As a result, automated systems may overlook or misinterpret deterrent cues, increasing the likelihood of escalation.

Emerging and disruptive technologies are often labeled 'disruptive' precisely because of their impact on the foundational elements of deterrence: capability, credibility, and communication. Deterrence depends on the concealment and survivability of weapons systems, including deployment in silos, on mobile platforms, or aboard submarines to ensure second-strike capabilities. Submarine-based deterrence is particularly valued for its stealth. However, technologies such as drones, microsatellites, and unmanned underwater vehicles threaten to compromise the stealth and survivability of these platforms, undermining second-strike assurance.

The communication pillar of deterrence is also under growing threat. Cyber capabilities now make it possible to target and disrupt Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems. A successful cyberattack could cut communication lines between national leadership and deployed forces, delaying or even disabling crucial decisions during a crisis.

The emergence of non-nuclear strategic weapon systems, particularly hypersonic weapons, adds another layer of complexity. These weapons are fast, maneuverable, and difficult to detect, making them ideal for first-strike scenarios. Unlike nuclear arms, hypersonic systems do not carry the same political stigma, increasing the probability of their early use in a conflict. During a crisis, the mere suspicion that an adversary possesses hypersonic strike capabilities may prompt both sides to consider pre-emptive strikes, escalating tensions and increasing the risk of miscalculation.

The entanglement of conventional and nuclear forces further exacerbates the threat to deterrence stability. Many advanced weapon systems today are dual-use, capable of carrying either nuclear or conventional warheads. If a dual-use system is used in a first strike, the adversary might not be able to determine the warhead type, potentially prompting a catastrophic miscalculation. This risk is particularly acute

in countries like Pakistan, where conventional and nuclear assets are often co-located. An attack on a conventional site may unintentionally impact strategic systems, leading to an unintended or disproportionate response.

Emerging technologies promise enhanced operational capabilities, but they also present significant strategic risks. The potential for miscommunication, inadvertent escalation, and premature delegation of lethal authority to automated systems poses urgent challenges. As these technologies continue to evolve, their impact on global deterrence frameworks must be carefully examined and addressed.

Influence of Emerging Technologies on Changing Character of War

Mr Dmitry Stefanovich
Research Associate, Center for International Security at the Primakov National Research Institute of World Economy and International Relations (IMEMO), Russian Academy of Sciences

Emerging and disruptive technologies can be systematically analyzed by categorizing them into three functional baskets: support technologies, combat technologies, and universal technologies, each shaping deterrence and warfighting in distinct ways. The Support technologies include advanced computing capabilities such as supercomputing and quantum technologies. These technologies facilitate simulations for advanced weapons development, including nuclear weapons maintenance and the design of other weapon systems. Additionally, they support global-scale capabilities such as weather forecasting and contribute to the planning of complex military operations. Contemporary military space assets like ISR, PNT, early warning, and SATCOM, are predominantly support-oriented, furnishing the data, timing, and connectivity that make higher-end combat effects possible.

The Combat technologies are those employed for direct strikes and lethal effect. Scramjets, or supersonic combustion ramjets, are prominent examples as they will likely enable future hypersonic cruise missiles, advanced rocket engines, novel propellants, and next-generation warheads and explosives. These capabilities depend heavily on the support technologies mentioned earlier. Meanwhile, universal technologies contain cross-cutting technologies with AI as a key example. AI can be applied in both support and combat functions: It enables logistics, predictive maintenance, sensor fusion, and command-and-control, while also being embedded in guidance and autonomy suites for lethal systems.

The impact of these emerging technologies, especially hypersonic weapons, is particularly significant. They reduce the time to target, improve speed and maneuverability, and make missile systems harder to intercept. This could allow for smaller arsenals while maintaining the same level of deterrence. Yet persistent geopolitical distrust limits prospects for reciprocal reductions. Meanwhile, autonomous combat systems with AI-enabled guidance introduce new challenges for control and stability in warfare. These technologies can be deployed across all operational environments including air, sea, land, and outer space. Notably, their use may reduce both combat and non-combat casualties. Smart guidance systems increase the efficiency and lethality of various long-range weapons, from hypersonic missiles to loitering munitions, and uncrewed aircraft systems, even as their escalation and governance challenges grow.

AI and ML optimize and accelerate data analysis, thus enhancing situational awareness and compressing military decision-making. The sheer volume of data available to modern military planners has rendered traditional analysis methods insufficient. Notably, Russian scholars have recognized the potential of AI in decision-making support, highlighting the potential of AI in decision-making support well before such challenges became widespread.

Outer space has become central to military operations, with AI tools now processing vast satellite and reconnaissance data. A key advance is cross-constellation data fusion by combining raw streams from different commercial and national providers which, once mature, will markedly enhance space-based intelligence. Further, advancements in microelectronics are enabling smaller, more autonomous spacecraft capable of on-orbit servicing and engagement. Technologies such as directed energy weapons and electronic warfare systems are maturing but are yet to be widely fielded. These capabilities are expected to become operational within our lifetimes. Alongside cyber capabilities, these systems can hold satellite infrastructure at risk, not just physically

but also by disrupting telemetry, tracking, and command links through uplinks and downlinks.

A concerning trend is the pursuit of space superiority by some states. When one state seeks dominance in outer space, it compels others to follow suit, undermining the principle of peaceful use. More broadly, the strategic impact of emerging and disruptive technologies is mediated by perception: advanced capabilities either nuclear or non-nuclear, offensive or defensive, are likely to be perceived as an attempt to gain unilateral advantage. This perception can erode mutual trust and threaten international security.

Evidence from the past two decades points to an action–reaction cycle in which expansive U.S. missile-defense efforts spurred Russia to pursue novel nuclear delivery systems leveraging emerging technologies. These Russian advancements were subsequently cited by the U.S. to justify its own modernization efforts, involving both nuclear and non-nuclear capabilities.

The updated Russian state policy on nuclear deterrence explicitly identifies technological threats such as aerial drones, hypersonic weapons, directed energy weapons, and space-based anti-satellite systems, as requiring a deterrent response. Of particular concern is the integration of disruptive technologies, including AI into NC3. The highly sensitive nature of NC3 makes meaningful transparency or regulatory mechanisms nearly impossible. Mere declarations of responsible conduct lack credibility without concrete disclosure of actual practices.

There is skepticism that international consensus on transparency in NC3 can be achieved. Additionally, emerging technologies become destabilizing when states seek superiority across all domains while selectively pursuing control in others. This was evident during the previous U.S. administration, which expressed willingness to negotiate arms control while simultaneously advancing non-nuclear, hypersonic, space, and cyber capabilities. The current administration

appears to be continuing this approach, aiming for all-domain superiority while also seeking to curb defense spending. This contradiction may present openings for technological arms control. The proliferation of lethal non-nuclear weapons does not inherently enhance global security. One proposal to address this is to increase the publication of strategic planning documents, especially in areas such as aerospace defense, AI, and hypersonic systems. Such documents promote transparency, reduce the risk of misperception, and provide a means of self-assessment of a state's own capabilities and intentions.

Emerging technologies can yield either catastrophic or stabilizing outcomes. While some developments have already led to destructive consequences in various regions, proper integration of these technologies could reinforce deterrence. The scientific and expert communities must critically assess the implications of specific technologies and ensure proper training for future operators and decision-makers. Ultimately, the challenge lies not in the technology itself but in how it is applied by its users.

Strategic Alliances in the Age of Emerging and Disruptive Technologies

Dr Alexander Evans OBE
Associate Dean for Strategic Development at the LSE School of Public Policy, UK

A declassified 1982 CIA memo raised the challenge of preparing analysts for strategic surprise. That imperative endures. In today's renewed great-power competition—far removed from the optimism of the immediate post–Cold War era—strategic planning, doctrine, and training for military and civilian cadres must explicitly incorporate the dynamics of surprise. This also argues for including disciplined imagination into procurement and force-design processes: stress-testing assumptions, gaming low-probability/high-impact scenarios, and building adaptive capabilities that can pivot quickly when the unexpected arrives.

The reliability of nuclear deterrence is under renewed scrutiny. As noted historically by Mao Zedong, "an atom bomb goes off when it's told." However, current concerns revolve around whether such command and control can still be guaranteed amidst technological change. Hence, debates about emerging and disruptive technologies add complexity to this challenge.

The law of proliferating unintended consequences, as articulated by diplomat Ricardo Luna, underlines the unpredictable outcomes that new technologies may produce. Emerging technologies can disable or disrupt command and control systems, alter strategic balances, and deliver strategic effects through non-kinetic means. Areas of particular concern include cyber and cognitive warfare, the latter applying behavioral science to influence decision-making at scale. Strategic misperception remains a constant throughout history, from Zeppelin competitions to misread intentions during the China–USSR border crisis in 1968–69. The integration of artificial intelligence further

accelerates decision-making, increasing both risk and uncertainty in deterrence dynamics.

It has happened in South Asia as well, underlining the enduring reality of strategic misperception and misreading. The introduction of AI, combined with the rapid pace and compression of decision-making timelines, exacerbates this challenge. One example of how technology has already disrupted strategic environments is the 2018 release of Strava's GPS map data. Strava, a fitness tracking app, inadvertently revealed the locations of secret military bases when users often special forces personnel, ran laps around secured installations. The dataset exposed global black sites, illustrating how big data and open-source intelligence (OSINT) can impact strategic stability.

This case demonstrates how new and old forms of warfare converge, particularly in hybrid operations. Cyberattacks, targeted assassinations, disinformation, and subversion remain age-old tactics, but the delivery mechanisms have evolved. A humorous yet serious Danish poster warns against "becoming employee of the year at the Russian Intelligence Service," highlighting modern threats to cyber and national security.

Beyond cyber tools, economic statecraft is gaining prominence. 'Chip War' by Chris Miller explores the geopolitical ramifications of semiconductor dominance, while historian Adam Tooze focuses on machine tool engineering and industrial production as critical components of national power. It's not just about AI or chips; traditional industrial capacity matters too.

The industrial landscape is also changing rapidly. Visuals depicting drone production capabilities are already outdated, given real-time lessons emerging from the Russia-Ukraine war. Drones, AI, and even cognitive warfare applications are shifting the tactical and strategic calculations on the battlefield. The evolving debate around AI Large Language Models (LLMs), whether widely distributed or monopolized

by leading states such as the U.S., adds to global uncertainty around emerging technologies.

Recent instances illustrate how innovation is shaping strategic outcomes, for example, an attack on Hezbollah's communications infrastructure using detonating pages. A historical parallel is found in World War II during the Battle of the Atlantic. While breaking Enigma codes received much attention, centimetric radar proved equally pivotal. Unlike codebreaking, which merely indicated a submarine's presence in a general area (e.g., F-7 or F-6 in Islamabad), centimetric radar pinpointed precise locations such as "House 45, Street 7," facilitating effective countermeasures.

Paul Kennedy's historical work underlines a persistent bias in how we approach technological advancements, favoring flashy innovations over integrated strategic thinking. This bias hinders a comprehensive understanding of the full technological spectrum. The need to accelerate the decision-making "kill chain," as previously discussed by Mr. Stevanovich, is vital. Archival accounts, such as those documenting the USSR's decision to invade Afghanistan in 1979, reveal how strategic missteps are often made in times of crisis. Today, the risk is amplified by the speed of algorithmic and behavioral decision-making, producing an environment with high data fidelity but potentially lower-quality outcomes.

Ironically, the sheer volume of data may lead to poorer decisions. This highlights the pressing human capital challenge. Who truly understands AI, scramjets, swarm drones, nuclear deterrence, cyber, and space all at once? Anyone claiming expertise in all these domains is likely a unicorn, rare and fictional. Instead, building human capacity in expert communities and among apex leadership is essential. As emphasized earlier, we must rethink how we train both our general staff and strategic leadership.

Effective grand strategy requires both imagination and persistent doubt; qualities often underappreciated in bureaucratic promotion

systems. The challenge lies in embedding these qualities into structured decision environments that prize certainty and procedure. Consider the metaphor of a medieval castle under cyberattack: "Bad news, Your Majesty. It's a cyberattack." Such scenarios challenge conventional assumptions about deterrence and capability. Apex decision-makers must move from a "what for" mindset to a "what if" posture in an era shaped by emerging technologies.

Strategic planning must evolve from reactive "what for" capabilities to anticipatory "what if" approaches. This mirrors the shift from just-in-time logistics to just-in-case resilience models. In this context, international partnerships are best viewed as strategic insurance policies. They reduce critical dependencies, enhance situational insight, and foster interoperability without imposing binding pre-commitments. This preserves autonomy for states while improving their crisis readiness and support options.

Emerging research in neuroscience warns against the cognitive toll of constant operational demands like continuous digital connectivity and back-to-back meetings on decision-making. This hinders long-term planning and diminishes creativity, emphasizing the need to build time for reflection into leadership routines.

Drawing on Isaiah Berlin's distinction between foxes (generalists) and hedgehogs (specialists), modern strategic environments demand a fusion of both. "Neo-generalists", individuals capable of bridging multiple domains such as nuclear deterrence, cyber operations, and space security—are essential. These connectors are vital to improving decision-making quality in an era defined by complexity and technological convergence.

Question Answer Session

Q: How does India's rapid militarization of AI and its pursuit of AI-enabled ISR platforms, autonomous weapons, systems, and early warning systems affect the strategic calculus of South Asia?

A: On AI-enabled military integration, South Asia is far behind. The leading two states in this domain are the US and China which are driven by capital intensity, data scale, testing infrastructure, and industrial depth. India is investing, but meaningful, system-wide integration of AI across C2, ISR, and fires remains a work in progress; regional discourse often overstates its maturity. As these capabilities develop, counter-capabilities also evolve and they are usually much cheaper to develop. If India is advancing in this field, rest assured Pakistan will either develop matching capabilities or effective counters. Moreover, if India truly had such command-and-control mechanisms, its BrahMos missile would not have accidentally entered Pakistani airspace.

Q: How can we regulate the application of emerging technologies like Starlink, particularly when private enterprises are increasingly influential in both civilian and military domains?

A: Contemporary governance operates in a post-privacy environment, where the central task is to distinguish mission-critical national-security data from the broader universe of civilian information. Segments of critical national infrastructure can be hardened, yet pervasive dependence on commercial platforms and open networks makes comprehensive protection impracticable. Regulation of space-based communications constellations, such as Starlink, compounds the challenge through cross-border jurisdiction, dual-use functionality, and private ownership. Historical precedents, most notably 19th-century telegraph regimes that embedded national-security carve-outs, offer useful templates. A modern framework should codify narrowly scoped national-security exemptions within risk-based regulation, ensuring resilience and disclosure standards for providers while

avoiding blanket controls that would erode openness, innovation, and trust.

Q: Given India's pursuit of EDTs and its current political ideology what will be the future of strategic stability in South Asia?

A: India is investing in EDTs, with regional stability will depend on realistic threat assessments and continued deterrence. Confidence-building measures remain thin and dated, and dialogue has largely stalled; absent reciprocal engagement, substantive progress is unlikely. Pakistan will continue to develop counters to Indian initiatives, and the strategic balance will likely be maintained despite shifting political ideologies.

Q: Could the U.S. and China formalize a mutual understanding on maintaining human control over nuclear command and control systems, and is there potential to expand such an agreement to the broader P5 framework?

A: Given current political volatility, a formal bilateral agreement is unlikely; even limited understandings are vulnerable to leadership changes, as illustrated by prior reversals in U.S. policy. While leaders have periodically signaled interest—most notably around the San Francisco summit, no formal framework has emerged. China has indicated openness to bilateral or P5 discussions, and despite U.S.–China tensions, both sides affirm that nuclear weapons should remain under human control. Expanded communication and technical dialogue are needed, but the shared interest in avoiding automation of nuclear command and control endures.

Q: Would there ever be a need for China to place its second-strike capability in Pakistan?

A: The claim is speculative and baseless part of a recurring narrative that seeks to malign Pakistan, echoing false 1990s allegations that misattributed a Chinese nuclear test to Pakistan. Such assertions lack

credibility and reflect poor analytic rigor. China and Pakistan continue to develop their second-strike capabilities independently, and there is no indication in Chinese expert discourse of any intent to place Chinese second-strike assets on Pakistani soil. Expanded expert-level dialogue would help dispel these misunderstandings.

Q: The process of Human-Machine Interaction (HMI) tends to make human beings over reliant on the use of machines. Thus, the decision-making outcome machines offer would be reliant on the quality of the data. Would there be an increasing emphasis on building trust - not just in terms of enhancement of communication channels among countries - but also in terms of building interpersonal trust and communication skills among leaders of different countries? It is important because during a crisis-situation, like during the Cuban missile crisis, it was communication between leaders of both sides, the U.S. and former U.S.S.R, which helped end the crisis.

A: Communication is very important, especially in the current, very complicated and fast-changing geostrategic situation. It is vital to prevent miscalculation and misoperation. For example, even though there are many problems between China and the U.S., yet both share the understanding that nuclear weapons must remain under human control and not be governed by AI. Last year, both states reached an agreement reaffirming this. Going forward, China and other countries should promote more communication and understanding to prevent unintended escalation.

Q: Many EDTs have the potential to undermine the second-strike capability. Keeping this aspect of EDTs into consideration, can there be any possibility in future that a non-nuclear weapon state launches an attack on a nuclear weapon state to dismantle the latter's nuclear capability?

A: The idea of a non-nuclear weapon state attacking a nuclear weapon state with strategic non-nuclear capabilities is highly risky. Even with

nuclear weapons, there is no guarantee of a 100% successful first strike. During the Cuban Missile Crisis, when an advisor suggested a preemptive strike due to ICBM superiority, President Kennedy rejected the idea, emphasizing that even two surviving missiles could destroy major cities like Washington or New York. Non-nuclear weapons, especially hypersonic or kinetic strike systems, are not as destructive or reliable. Their precision may be high, but their warhead lethality is low. These technologies offer some capabilities to smaller states, but they cannot replace the deterrent effect of nuclear weapons. Moreover, attempting to disarm a nuclear state with non-nuclear means would be a high-risk endeavor. Such a move would require absolute confidence in the ability to fully neutralize the target without retaliation, which is nearly impossible especially in the era of tactical nuclear weapons and unpredictable escalation.

Q: On AI with a major focus on the responsible use of AI, what would be the definition of a 'responsible use'?

A: A responsible use of AI, particularly in national security contexts, would mean embedding human control, ensuring transparency in AI systems, and building regulations that factor in both ethical and operational safeguards. It also implies understanding the limits of AI, avoiding over-reliance, and building systems that serve to enhance, not replace the accountable decision-making processes.

Q: In recent times, Emerging and Disruptive Technologies (EDTs) have reshaped the concept of deterrence. In the context of South Asia, what measures should Pakistan and India take to maintain deterrence stability?

A: In the South Asian context of emerging technologies and deterrence, priority should be given to Track-1.5 diplomacy, greater transparency through public doctrinal statements, and sustained crisis-communication channels. Revitalizing Cold War–style confidence-building measures like advance test notifications, nuclear facility non-attack understandings, incident-at-sea agreements, and hotline

protocols, would help reduce misperception and manage escalation risks amid rapid technological change. Both states, India and Pakistan have indeed previously taken commendable steps like advance missile test notifications and non-attack agreements on nuclear facilities. These models can be updated to account for EDTs and could serve as a confidence-building baseline in the future. Unfortunately, India has disengaged from dialogue, stalling new CBMs. Without mutual willingness to engage, further regulation or mechanisms to preserve strategic stability are difficult. However, if dialogue resumes, these measures can be considered and expanded.

Q: Can there be another view of looking at the question of war and peace other than the dominant secular, contemporary view—perhaps from a civilizational or ideational perspective?

A: Values remain central to strategy. Technology and data can sharpen choices, but exclusive reliance on either human intuition or machine inference is misguided. Civilizational and ideational perspectives can enrich assessments, helping reintroduce imagination and constructive doubt into bureaucratic and military decision-making. Embedding such perspectives through red-teaming, ethical review, and diverse advisory inputs, guards against model myopia and institutional groupthink, improving judgment under uncertainty.

Q: Given the ambiguity of military objectives in Afghanistan, wouldn't the U.S. use of nuclear weapons on Hiroshima and Nagasaki serve as a more illustrative example—highlighting how strategic decisions made amid uncertainty can produce decisive yet irreversible outcomes and expose the tension between military necessity, technological capability, and moral responsibility in warfare?

A: No state holds a monopoly on poor decisions; every government carries a record of strategic errors, often obscured by secrecy. The aim is to learn from these mistakes, whether Soviet, American, or

otherwise; not to deflect criticism but to promote reflective analysis of past and present decision-making processes.

Session-II

Impact of Militarization of Artificial Intelligence

Moderator: Dr Anum Riaz
Associate Director, CISS

Artificial Intelligence and the Future of Nuclear Deterrence

Dr Petr Topychkanov
Head of Section for New Challenges in South and Southeast Asia, IMEMO, and Co-Chair of the Master Program 'Regional Issues of World Politics', Lomonosov Moscow State University

The intersection of artificial intelligence (AI) and nuclear deterrence remains a considerable challenge. Numerous publications from prominent institutions and think tanks across the globe including SIPRI, as well as organizations in Russia, Europe, the United States, Pakistan, India, and China, have explored this issue in depth, offering extensive analyses of potential future developments. However, many such publications often lack a crucial element: a bridge connecting the current state of affairs with both the future trajectory and the historical experience in this domain.

The term AI has existed since the 1960s, and even during that early period, experts had already begun to examine issues that remain relevant today. The ability to draw from historical insight while anticipating future challenges serves as a valuable approach to understanding the evolution of AI in military and strategic contexts.

The complexity of the topic is further amplified by the subject matter itself, the future of nuclear deterrence. While substantial literature exists in this area, it also reveals significant gaps, particularly in answering foundational questions regarding the connection between conventional and nuclear capabilities, the interaction between emerging and traditional technologies, and the evolving relationship between human operators and machines. Moreover, discussions on these themes are taking place in a dynamic and often tense geopolitical environment, characterized by limited dialogue between major powers such as Russia, the United States, European states, and China. Deep-rooted mistrust continues to pose a significant barrier to constructive engagement.

Against this backdrop, opportunities for multilateral exchange, such as those provided by this conference, are especially valuable. They allow for cross-national conversation and reflection on shared strategic challenges.

Historical perspectives on future warfare also offer critical insights. Soviet military thinkers in the 1960s predicted that future conflicts would entail the simultaneous defeat of enemy forces, destruction of infrastructure, and disruption of logistical networks. This conceptualization integrated three distinct arenas: the frontlines of combat, the adversary's domestic territory, and logistical pathways by land, sea, and air.

Recent conflicts, including the ongoing Russia-Ukraine war, have borne out some of these predictions. For instance, unmanned aerial vehicles (UAVs) have been used to target locations deep within Russian territory, raising strategic alarm and recurring references in Moscow's security discourse with the West.

The Soviet vision of future war also emphasized the role of highly mobile strike groups, capable of rapid maneuvers in multiple directions. In this context, warfare was expected to be particularly intense during its early stages. Analysts from that era noted that stockpiles of rockets and missiles, amassed during peacetime, could be expended within the first minutes or hours of a major conflict. Even following such an initial exchange of strikes, military operations would likely continue, with objectives such as securing or neutralizing critical command-and-control nodes and economic facilities.

Marshal Vasily Sokolovsky, a prominent strategic thinker in the post-World War II period, underscored the importance of automation in air and missile defense. He advocated that improvements in anti-aircraft and anti-missile operations would increasingly rely on automated systems—a view that proved prescient. From the 1960s onward, rapid advances in computer technology were driven by military needs, particularly to support strategic air and missile defense.

This imperative led to significant investment in computational systems by the Soviet Union and other nations. The signing of the Anti-Ballistic Missile (ABM) Treaty in 1972 further shaped the strategic landscape and highlighted the foundational role of automation in military defense systems, rather than in offensive operations.

This early investment in automation also facilitated the redirection of financial resources to other strategic areas. Nevertheless, the foundational emphasis on automation proved critical for understanding its role in defense, particularly in contrast to offensive operations.

Progressing to the present, recent expert assessments such as those by Dr. Naeem Salik, have underscored the continuing relevance of this trajectory. As Dr. Salik noted, the vast volume of information collected through various sensors related to surveillance, intelligence, missile defense, and early warning is so immense that timely analysis and its conversion into actionable insights for military commanders is only feasible through modern computational systems.

From the 1960s to the present, the fundamental objective for both computers and AI has remained consistent: to enhance defense capabilities and manage data collected from sensors and early warning infrastructure. A significant evolution, however, is evident in the shift from primarily static sensors and radar systems to mobile, reconfigurable platforms. These modern systems, including anti-submarine platforms, can now operate autonomously or with minimal human intervention, particularly in maritime warfare contexts.

This evolution signifies a growing reliance on layered surveillance, early warning, and reconnaissance systems, supported by advanced computing technologies. Returning to concepts from the 1980s, Soviet military theorists of that era already envisioned many of the AI-driven military functions seen today. These included:

- Reconnaissance and early warning systems,

- Automated battlefield command and control systems,
- Expert systems, and
- The continued role of human decision-making in military operations.

Currently, reconnaissance and early warning functions are fully operational and integrated into the defense infrastructures of advanced militaries. Command and control automation has also progressed significantly, with the Russia-Ukraine conflict demonstrating the rapid deployment and adaptation of such systems in real-time conflict environments.

Human input remains essential in forecasting scenarios and strategic decision-making. However, emerging concerns persist regarding overreliance on AI-generated data. When decision-making is based solely on screen-displayed information, derived from AI-processed datasets, it may introduce vulnerabilities. Historical precedents have shown that flawed data could have led to catastrophic outcomes had it not been for human operators overriding AI-generated conclusions.

There have been past instances where operators received incorrect information from early warning systems, but chose not to act on it, thereby preventing potentially catastrophic retaliatory actions. Such examples underscore the continued importance of human oversight in decision-making, even when automated systems are involved.

Currently, fully integrated expert systems capable of comprehensive data interpretation, alternative action generation, and independent decision-making do not exist. The development of such systems is constrained by two major factors: conservative military leadership and the still-maturing nature of artificial intelligence technologies.

According to earlier Soviet literature on artificial intelligence, AI systems lack the capacity to process vague concepts or employ human reasoning methods. These systems operate strictly under the logic of pre-programmed algorithms. Two fundamental conditions govern the

effectiveness of such systems. First, the intelligence requirements imposed on an AI system must align with the capacities of its sensing mechanisms; and second, the outputs of AI systems are wholly determined by the instructions provided by human programmers.

Consequently, the capabilities of AI-driven platforms, such as unmanned aerial vehicles (UAVs) or autonomous sensors, are limited by both their programming and the technical specifications of their sensors. This understanding is essential to avoid overestimating the abilities of AI, especially as exaggerated portrayals often dominate public discourse.

In such discourse, three primary forms of AI are frequently discussed:

1. **Artificial Narrow Intelligence (ANI):** The only type presently relevant to military applications. ANI enables computers to process large volumes of data and detect patterns in tasks that are otherwise challenging for humans.

2. **Artificial General Intelligence (AGI):** A theoretical concept describing machines capable of learning and thinking like humans. While research is ongoing, AGI remains decades away from realization, particularly in military contexts.

3. **Artificial Superintelligence (ASI):** A fictional or highly speculative concept, not grounded in present capabilities.

In military applications, the principle of "human-in-the-loop" remains central. Any machine output is ultimately a reflection of human-designed inputs. Though contemporary AI can generate code and content autonomously (as in the case of gaming or software development), such applications are not acceptable when applied to sensitive functions like target identification in nuclear deterrence.

Military institutions are expected to maintain a conservative approach toward the adoption of AI in strategic roles for the foreseeable future.

AI-enabled systems may only be incorporated under extreme circumstances, such as total war scenarios, where all capabilities are mobilized without reservation.

To conceptualize the integration of AI into future military scenarios, it is helpful to consider its role within the framework of escalation ladders. For example:

- During periods of geopolitical tension, autonomous ISR (intelligence, surveillance, and reconnaissance) systems could provide decision-makers with accurate assessments of adversarial actions.

- Dual-capable systems equipped with AI functionalities might be deployed as signaling tools to communicate escalatory intent or readiness to adversaries.

Such uses demonstrate AI's growing significance in shaping both operational capabilities and strategic signaling in the evolving security environment.

The increasing reliance on AI-driven intelligence, surveillance, and reconnaissance (ISR) systems presents unique challenges. These systems process vast amounts of data, which can be subject to manipulation. An adversary could intentionally introduce misleading or corrupt data into the public domain to influence the decision-making of the opposing side. In such scenarios, ambiguity is exploited, prompting potentially destabilizing reactions based on false information.

During active hostilities, autonomous ISR systems would likely support covert operations, while AI-enabled combat platforms would be essential for offensive maneuvers. Throughout conventional conflict stages, the roles of ISR and offensive capabilities would remain largely consistent. However, both sides are expected to increasingly rely on

nuclear early warning systems and strategic command and control frameworks.

Recent developments indicate a trend toward integrated command-and-control systems. This convergence is blurring the lines between strategic and non-strategic operations, as well as between early warning mechanisms for strategic and conventional threats. In a nuclear conflict scenario, early warning systems, ballistic missile defense infrastructures, nuclear command and control, and autonomous components of the nuclear arsenal would be fully activated. For nuclear-armed states, the potential for autonomous command and control of nuclear weapons could emerge, not due to technical limitations, which were already explored during the Cold War, but as a matter of political decision-making.

This leads to a crucial question regarding the future of nuclear deterrence: should it be considered independently of conventional and emerging technologies? While a distinct focus on nuclear deterrence may benefit arms control and strategic predictability, current trends and the views of many strategic thinkers suggest otherwise. The development of emerging technologies is increasingly viewed as inseparable from nuclear deterrence.

During the Cold War, even minor escalation risks were treated as precursors to full-scale nuclear war. In contrast, the current discourse has normalized the notion of limited nuclear use whether in tactical deployments or within regional conflicts. As these ideas gain traction, AI, particularly in its ISR functions, becomes increasingly relevant.

If states move toward deploying tactical or battlefield nuclear weapons, these actions will likely occur in a complex operational environment heavily shaped by AI. Such integration would affect not only real-time data processing but also the interpretation of intent, thereby complicating strategic calculations and heightening the risks of escalation. The risks associated with ambiguity, rapid escalation, and

AI-generated recommendations could complicate efforts to maintain strategic stability.

The current global nuclear landscape is characterized by the presence of multiple nuclear-armed states, coupled with the proliferation of smaller arsenals and advances in counterforce technologies. This combination contributes to an increasingly unstable and unpredictable strategic environment.

In light of these conditions, the future of nuclear deterrence, particularly in relation to AI, remains uncertain. When asked to present on this topic, the most honest conclusion is that a definitive answer cannot yet be provided. The absence of robust nuclear arms control agreements, combined with weak political dialogue among nuclear weapon states, compounds this uncertainty.

A meaningful step forward would be the reestablishment of strategic dialogues between key actors: Russia and the United States, Russia and NATO, China and the United States, and India and Pakistan. Such a dialogue would create a constructive environment in which the evolving role of AI in nuclear deterrence could be examined and addressed.

Impact of Artificial Intelligence on NC3

Ms Alice Saltini
Research Fellow, James Martin Center for Non-Proliferation Studies (CNS)

This analysis encompasses the most advanced artificial intelligence (AI) models currently available, extending beyond the algorithms already integrated into nuclear decision-making components. The scope of the discussion remains naturally limited due to the relative capacities of nuclear command, control, and communications, commonly referred to as NC3 systems, which underpin the nuclear decision-making process. As such, this presentation is not exhaustive but rather aims to capture the most critical and salient applications within NC3.

While this assessment presents a generalization across all nuclear-armed states, it is important to note that each state exhibits significant distinctions, which merit deeper analysis beyond the scope of this presentation. Additionally, although the AI-nuclear conversation spans many dimensions including deterrence and broader implications for strategic stability, the current remarks are focused specifically on NC3 and the broader nuclear decision-making architecture.

Before examining the topic in detail, three preliminary points must be made. First, while AI demonstrates remarkable capabilities that are advancing rapidly, it is not a panacea. Technology possesses fundamental problems, including issues related to vulnerability, reliability, susceptibility to cyberattacks, the challenge of aligning AI models with human values and objectives, and the lack of transparency regarding how AI systems make decisions. Given these limitations, any integration of AI into the nuclear domain must be approached with the utmost caution. Nevertheless, as the presentation illustrates, there are clear indications that the integration of cutting-edge AI into nuclear systems is already underway. However, the exact roles and extent of such integration remain uncertain. Second, the capabilities and

limitations of AI, along with its implications, are not yet fully understood. As technology evolves, it may resolve some of its existing challenges but is also likely to introduce a new set of risks that are currently impossible to predict.

Third, when AI intersects with the nuclear domain, it offers potential benefits if integrated cautiously and with a deep understanding of the technology's nature. However, it also introduces a wide array of risks. These risks depend on three primary factors: (1) the type of AI technology under consideration for integration, (2) the specific area of integration whether within NC3 or among the multitude of systems and subsystems that support or influence NC3, or even in adjacent domains that indirectly impact nuclear decision-making, and (3) the level of human oversight and control maintained.

Due to these complex and interdependent variables, the implications of AI in high-stakes military domains are exceptionally nuanced. Consequently, it is imperative to enhance the understanding of these implications and establish clear thresholds for high-risk AI integrations to ensure that nuclear systems remain secure and that the likelihood of miscalculation is minimized.

Advanced AI models today such as large foundation models and reasoning models, have demonstrated extraordinary capacity to generalize across diverse tasks. These systems continuously improve when provided with larger datasets and increased computational power, leading to the emergence of significant new capabilities.

For example, significant advancements are being made with reasoning models. These models are designed to perform complex reasoning by generating and internally processing extended chains of thought before responding to a task—an innovation with transformative applications in scientific research and problem-solving.

At the same time, remarkable developments are emerging from China. One notable example is DeepSeek, a Chinese AI startup that recently

released an open-source model, R1, that reportedly matches the capabilities of OpenAI's systems, but at a significantly lower cost. This achievement has occurred despite United States' export controls on AI chips, which were specifically implemented to slow China's progress in artificial intelligence development.

While the capabilities of these advanced AI models offer substantial societal benefits, they also introduce potentially grave risks. These risks are inherent in both the nature of the technology and its modes of use. In an era of rising geopolitical competition, AI is increasingly perceived as a tool capable of delivering decisive strategic advantages in military contexts including within the nuclear domain. In fact, the strategic utility of AI may be so significant that nuclear-armed states may feel compelled to pursue its integration, fearing that failure to do so would place them at a disadvantage.

This dynamic was underscored in several of the opening remarks at this session. As a result of this perceived advantage, nuclear-armed states are seeking to integrate AI into functions that directly or indirectly influence nuclear decision-making. This integration may involve direct incorporation into NC3 systems or into adjacent systems that feed into NC3 operations and thereby shape outcomes indirectly.

The architecture of NC3 systems holds considerable significance across nuclear-armed states, as it reflects each country's unique nuclear doctrine and strategic posture. Broadly defined, NC3 encompasses the infrastructure, protocols, and systems that enable national leadership to control and manage nuclear forces. Rather than operating as isolated units, NC3 constitutes a complex, interconnected network of systems designed to monitor, coordinate, and implement nuclear operations.

This network supports five key functions: force management, situation monitoring, planning, decision-making, and force direction. Together, these functions constitute a continuous cycle of data collection, threat analysis, and command execution. Given the interdependent nature of this architecture, AI applications are not limited to a single function or

node. Rather, AI concurrently enhances multiple segments across the NC3 structure.

For instance, AI-enabled predictive analytics can assess a range of threats across different domains simultaneously. Such capabilities can support situation monitoring, enable adaptive planning, and provide real-time decision support, all of which help streamline force direction and execution processes within NC3 systems.

Equally important, the third "C" in NC3 refers to communications, emphasizing the necessity of moving information securely through multiple pathways to ensure that connectivity remains intact and reliable, even under adversarial interference or direct attack. However, as the majority of NC3 systems were developed during the Cold War, many of them are now outdated and ill-suited to address the complexities of today's evolving threat landscape. Consequently, modernization has become not only necessary but essential to enhance both the safety and operational efficiency of these systems.

Artificial intelligence integration is occurring within this broader context of nuclear modernization. The obsolescence of aging infrastructure incentivizes the incorporation of AI, either to maintain a technological edge, gain a strategic advantage, or simply avoid lagging behind adversaries. This dynamic is further intensified by ongoing geopolitical competition, as discussed extensively in earlier remarks.

Discussions around the role of AI in nuclear systems, however, remain speculative. When it comes to integrating AI and its implications for nuclear decision-making, current assessments often rely on informed conjectures. This uncertainty is largely due to the classified nature of NC3 systems, which restricts public access to comprehensive data. As a result, researchers are frequently left to infer and hypothesize AI's potential applications by analyzing available sources such as defense contractor briefings, subsystem modernization efforts, and open-source intelligence.

Work is currently underway at several institutions to better understand this issue. For example, the Institute for Security and Technology has recently concluded a series of workshops dedicated to exploring the integration of AI into nuclear systems. Preparatory material and project findings from this initiative are expected to be published shortly.

There are, nonetheless, certain assumptions that can be made based on public statements from high-level officials and ongoing technological developments. Notably, President Joe Biden and President Xi Jinping have both issued public commitments to maintain human control over the use of nuclear weapons—a position echoed by the United Kingdom and France. Additionally, the head of United States Strategic Command, General Anthony Cotton, has acknowledged that AI is expected to play a significant role in modernizing NC3 systems. This role includes automating data collection and processing, accelerating data sharing with allies, and broadly enhancing decision-making capabilities.

OpenAI has recently announced a partnership with U.S. national laboratories to deploy its reasoning models for scientific research across national labs, including those in the nuclear weapons industry. These deployments will be accessible to researchers holding security clearances. Similarly, Anthropic has declared a collaboration with U.S. national laboratories to evaluate frontier AI models, including its hybrid reasoning model. This builds on an ongoing partnership with the National Nuclear Security Administration and the Department of Energy's national laboratories.

Although further details about how OpenAI and Anthropic envision their models contributing to the nuclear weapons sector have not been disclosed, OpenAI has cited AI safety research and efforts to "reduce the risk of a nuclear war." Anthropic has emphasized research focused on how AI could support national security objectives. Given these official statements and the trajectory of current developments, it is

reasonable to conclude that the integration of advanced, state-of-the-art AI models into nuclear systems has already begun.

AI is generally viewed as a tool designed to assist human decision-makers in making more informed and timely decisions. Critically, such systems are intended to operate with human oversight – a human always remains in the loop. One of AI's most valuable contributions in this domain lies in accelerating threat detection and the analysis of real-time data.

Accordingly, AI is likely to be integrated into early warning systems and intelligence platforms, particularly for tasks such as analyzing data from space-based sensors or ground-based radars to verify missile launches. Additionally, AI can support decision-making processes by offering alternative courses of action and forecasting various potential scenarios.

For instance, centralized fusion hubs receive inputs from multiple information sources such as satellite imagery, radar, signals intelligence, and open-source data. AI enables multi-sensor fusion, which facilitates the rapid and efficient processing of disparate datasets. This can enhance warhead discrimination (e.g., identifying real warheads from decoys), support damage assessments, and detect behavioral changes in adversary military postures.

Another critical application is AI-enabled decision support. These systems can incorporate contingency planning and simulation tools, allowing commanders to model "what-if" scenarios. Ongoing modernization efforts are exploring how AI can suggest courses of action, enhance training through simulations, and aid in adaptive planning by generating new operational strategies.

Even when AI remains under strict human supervision, the central concern remains: is this enough to prevent unintended nuclear escalation? The answer is no. A core challenge lies in the fact that the full implications of integrating AI into the nuclear domain, especially

regarding nuclear escalation, are still not well understood. The complexity, unpredictability, and high stakes of nuclear operations mean that even marginal errors or miscalculations can have catastrophic consequences.

The complexity of AI's integration into nuclear decision-making is compounded by four key challenges.

First, AI can influence nuclear decision-making processes even without direct integration into nuclear command, control, and communications (NC3) systems. Functions external to traditional NC3 architectures can still indirectly affect outcomes by feeding into the broader decision-making ecosystem. This significantly complicates assessments, especially given the limited transparency surrounding both NC3 and adjacent systems.

Second, the trajectory of AI development remains highly unpredictable. Present-day advanced models possess attributes that render them unsuitable for critical military domains such as nuclear operations. These systems often exhibit unreliability, including the phenomenon of "hallucinations," which may range from generative language models fabricating historical facts to vision models detecting non-existent features.

Such models also operate as "black boxes," particularly in the case of large-scale architectures, meaning that their decision-making processes remain opaque. Although reasoning models employing chain-of-thought prompting are designed to enhance transparency by displaying intermediate reasoning steps, empirical studies indicate that these chains often fail to align with final outputs, leaving the underlying transparency challenge unresolved.

Additionally, AI systems remain highly vulnerable to cyberattacks and suffer from alignment issues, whereby model outputs may diverge from human goals or normative values. Notably, recent research from Anthropic has revealed concerning tendencies in some models toward

alignment faking and even deceptive behavior. These limitations persist even under human supervision.

It is critical to recognize that these deficiencies are not necessarily the result of malfeasance but arise from the fundamental architecture of these systems. For instance, large language models function as statistical approximations of language, based on observed correlations between words in training data. As such, they fail to capture the full complexity of the real world, which does not conform to the smooth probabilistic distributions learned during training. While the capabilities of these models are impressive, they are not yet suitable for high-stakes applications, particularly in domains where precision and reliability are non-negotiable.

Although future technological advances may address these shortcomings, they may simultaneously introduce new and unforeseen risks, especially in high-consequence sectors such as nuclear security.

Third, states may incorporate AI in diverse ways, shaped by their unique strategic doctrines, existing capabilities, and perceived threat environments. For instance, some may adopt AI to compensate for perceived vulnerabilities or to gain asymmetrical advantages in strategic stability.

Fourth and finally, there is currently no widely accepted framework or consensus for determining what constitutes a "safe" integration of AI in nuclear systems. Criteria for acceptable risk thresholds vary widely, and may be entirely absent, for different nuclear-armed states. This is particularly troubling given the catastrophic consequences that could result from a single failure in nuclear decision-making.

Moreover, it is conceivable that states perceiving themselves to be at a strategic disadvantage may accept greater risks in AI integration, especially if it offers opportunities for faster decision-making or perceived strategic parity. Such a calculus introduces significant

instability and should be regarded as a scenario that must be avoided at all costs.

In conclusion, current artificial intelligence models pose numerous risks, and existing mechanisms for mitigating these risks remain insufficient. Although substantial research is underway to address technological limitations such as improving model reliability under adversarial conditions and enhancing explainability, these efforts have not yet yielded comprehensive solutions.

As noted earlier, while technological maturation may eventually resolve certain issues, it is equally plausible that new and unanticipated risks will emerge as capabilities advance. At present, the field is marked by too many uncertainties— "ifs" and "when's"—to offer confident projections.

The implications and risks associated with AI integration in the nuclear domain depend on three interrelated factors:

1. The attributes of the AI models under consideration for integration.

2. The specific area of the system into which AI is being integrated.

3. The extent of human control and the redundancy mechanisms established to ensure system safety.

The interplay among these three variables ultimately determines AI's impact on the risk of nuclear escalation and helps identify points of high-risk integration. However, understanding how these factors interact remains a significant challenge.

The most logical path forward is to:

- Identify high-risk areas of integration;

- Develop robust risk assessment frameworks to quantify and evaluate those risks;
- Move beyond simplistic commitments to "human-in-the-loop" oversight;
- And establish thresholds for responsible integration.

These steps are essential to ensuring that AI integration does not inadvertently destabilize nuclear decision-making processes.

Autonomy, Machine Learning, Nuclear Weapons, and Strategic Stability

Dr Jean-Marc Rickli
Head of Global and Emerging Risks, Geneva Center for Security Policy

In 2019, a chapter was authored for a book published by the Stockholm International Peace Research Institute (SIPRI) addressing the implications of artificial intelligence (AI) for nuclear strategy. The present remarks revisit and update the analysis in that chapter, offering a perspective on the developments that have occurred over the subsequent six years.

Although six years may seem like a short time frame, in the realm of AI, it represents a substantial leap forward. Technological advancement in this field is accelerating at an extraordinary pace, particularly in terms of computational power and algorithmic efficiency.

This presentation examines how such advancements affect strategic stability. Strategic stability, in this context, refers not only to the absence of incentives to use nuclear weapons first or to engage in nuclear arms buildups, but also to the maintenance of assurance and reinsurance measures—factors closely tied to mutual trust, which AI is likely to influence in profound ways.

A comparative look at the evolution of computing power and algorithmic performance illustrates this transformation. On one hand, Moore's Law, depicted by the first line on the left, indicates that computing power roughly doubles every 18 to 24 months. As a result, computers in 2025 are approximately eight times more powerful than those available in 2019.

However, algorithmic improvements follow an even more dramatic trajectory. Represented on the right side of the graph (a logarithmic scale), the rate of improvement in AI algorithms occurs every 3–4

months. Over the same six-year period, this translates into a staggering 350 to 500,000-fold increase in algorithmic performance, demonstrating an exponential growth curve even on a log scale.

The key implication of this rapid advancement is the increasing speed at which AI systems can operate, particularly in processing vast amounts of information. This capability impacts foundational military concepts such as the OODA loop (Observe, Orient, Decide, Act) and the intelligence cycle.

In the nuclear domain, this acceleration of decision-making processes raises serious concerns. In a nuclear crisis, the last condition one would want is a compressed decision-making timeline. The pressure to act quickly, driven by AI-enabled systems, could reduce opportunities for deliberate judgment and crisis de-escalation, potentially destabilizing nuclear deterrence frameworks.

If one recalls the Cuban Missile Crisis, President John F. Kennedy had several days to deliberate and consider various options before making a decision. In the context of AI-enabled systems, such a luxury may no longer exist. The prospect of decision-makers having only seconds or a minute to respond, poses significant risks. This represents one of the key impacts of artificial intelligence on strategic stability.

Concrete demonstrations of AI's growing capabilities already exist. For example, in a U.S. military simulation, a former Top Gun instructor was placed in a dogfight against an AI algorithm. The pilot described the experience by stating that the AI "felt like it could preempt any of my moves." In subsequent, more realistic simulations, AI algorithms again consistently outperformed human adversaries.

Since then, the trend has expanded. AI-powered drones have begun to outperform those operated by human pilots. In another notable development, an AI algorithm successfully carried out eight distinct missions aboard a real jet aircraft, illustrating that legacy weapons

systems are increasingly being adapted to integrate autonomous capabilities, often outperforming human operators.

This evolution raises critical concerns about accuracy and second-strike capabilities, which are foundational to nuclear deterrence. The survivability of second-strike forces, particularly nuclear-armed submarines, has traditionally been seen as guaranteed due to the difficulty of detecting them underwater. However, advances in sensor technology and data processing are eroding that assumption.

Major powers such as France, the United States, and Australia are investing heavily in capabilities to detect submarines. In addition, autonomous underwater vehicles are emerging as tools that could monitor and potentially track submarine movements. Even more destabilizing is the perception, rather than the confirmed existence, of such capabilities. The mere belief that an adversary may possess these technologies is sufficient to undermine strategic confidence and escalate instability.

Another critical issue is the integration of AI into existing systems, including legacy platforms. This integration may compromise second-strike capabilities by enabling preemptive targeting or overwhelming conventional defenses. The perception of a technological gap where one side feels outpaced can lead to insecurity, arms racing, or reckless escalation.

Legacy systems are also increasingly vulnerable to swarms of sensors and low-tech, low-cost weapon platforms. Recent conflicts, such as those in Ukraine and Gaza, have highlighted this asymmetry: attackers can employ inexpensive systems to drain the far costlier defensive resources of their adversaries. This strategy, predicted by exhaustion rather than destruction, is likely to proliferate rapidly due to the ease with which such technologies spread.

Lastly, there are significant vulnerabilities associated with hacking and data poisoning. AI systems are fundamentally probabilistic. For

instance, when analyzing an image, an algorithm does not see the picture as a human does. Instead, it vectorizes every pixel and assigns it a classification value such as “2.5” for a sock or “2.7” for a dog. If an adversary can manipulate the classification process, it becomes possible to alter recognition outputs without visible changes to the image. These adversarial inputs may go undetected by the human eye, rendering the system brittle despite its technical sophistication.

One illustrative example concerns the manipulation of visual recognition through adversarial inputs. By placing stickers on a traffic sign, for instance, it is possible to alter how the sign is interpreted by an AI system. This issue is becoming increasingly concerning with the rise of generative AI, which produces synthetic data that, in turn, is used to train other algorithms. This creates a feedback loop that can lead to profound misrepresentations of reality, a trend that is accelerating.

Perceptions are central to nuclear deterrence, which relies heavily on the credibility of possessing and being willing to use retaliatory capabilities. If a state perceives that its adversary possesses advanced AI-enabled systems, especially given the extensive hype surrounding AI's potential, this perception alone can generate uncertainty and instability.

A separate but equally important issue is cyber deterrence, which contrasts starkly with nuclear deterrence in its logic. In the nuclear domain, states communicate their capabilities explicitly to deter adversaries. In the cyber domain, however, states do not disclose their capabilities because doing so would simultaneously reveal their vulnerabilities. Cyber weapons, particularly zero-day exploits, are often single-use tools. Once deployed, the target system is patched, and the exploit becomes obsolete. This conflicting approach to strategic signaling presents a dilemma when both nuclear and cyber deterrence operate in tandem.

Additionally, we are witnessing the emergence of machine-induced perceptions. These affect both human interpretations of machine outputs and machine-to-machine interactions, which fundamentally alter crisis dynamics. AI systems can learn from human cognitive biases and manipulate information flows to guide decisions in specific directions. This manipulation could take place without the target being aware of the influence.

Experiments have already shown how susceptible humans are to AI-generated misinformation. In 2022, tests revealed that participants were more likely to believe deepfakes than authentic images. In 2023, a study involving patients asked them to rate medical advice from both doctors and AI chatbots. Not only did the chatbots outperform doctors in perceived quality, but they also scored higher on empathy—a human attribute. This does not imply that machines have become empathetic; rather, they have become adept at mimicking empathy in ways that deceive human users.

If these trends are validated further, they open the door to mass manipulation through AI systems. Earlier today, this was referred to as a form of "weapon of mass destruction." The speaker has referred to it as “Weapons of Mass Disinformation,” a concept he developed in a publicly available piece in the *Geneva Policy Outlook*. The article argues that serious attention must now be given to subversion through disinformation as a strategic threat.

However, this challenge goes beyond AI alone. Increasingly, the world is seeing the convergence of AI with neurotechnology. In one experiment, a subject was placed in a functional MRI scanner while viewing images. The AI algorithm, within one hour, was able to reconstruct a close approximation of what the subject was seeing. This experiment demonstrated the beginning of mind-reading technologies.

The company Neuralink, for example, has conducted successful human trials in which a chip implanted in the brain allows individuals to communicate directly with machines. This represents the dawn of

cognitive warfare. Unlike, information warfare, which seeks to influence through the flow of data, cognitive warfare aims to control how and what people think, and thereby, how they act. This is increasingly feasible with the convergence of AI, invasive sensing, and neuro-technologies.

As highlighted earlier by Alice Saltini, the absence of oversight and accountability in this field is alarming. The strategic implications are profound, and the current regulatory vacuum demands urgent attention.

There is frequent discussion around the idea that no one would be reckless enough to call for the integration of an algorithm into autonomous nuclear weapons systems. However, when considering decision-making processes, particularly in the context of meaningful human control, the situation becomes more complex. As part of the Group of Governmental Experts (GGE) on Lethal Autonomous Weapon Systems (LAWS), the debate over a potential ban has been ongoing for over a decade. A key concept in this discourse is "meaningful human control."

The case of Lavender, the Israeli algorithm used to identify human targets, is instructive. While the operator is technically given a few seconds to confirm or cancel a strike, the entire decision-making chain has already been filtered and framed by the algorithm. This raises a critical question: to what extent is the final human decision actually meaningful, when the framing is entirely machine-generated?

The issue of proliferation is equally pressing. Driven by perceptions of technological inferiority and the fear of falling behind, states feel compelled to accelerate AI adoption—this is horizontal proliferation. In addition, there is vertical proliferation, where the technologies move from state control to non-state actors. This trend is accelerating as access to these capabilities becomes easier.

This brings us to the issue of swarms, which can have profound implications for nuclear strategy. The primary idea behind swarming tactics is to saturate an adversary's defense systems. Although Iran did not use swarms in its recent attacks on Israel, the strategy of overwhelming defenses through massed attacks bore similarities. These developments point to changing dynamics in both conventional and strategic deterrence.

Another challenge is traceability. As noted earlier, understanding how decisions are made within these complex systems is difficult. When failures occur, it is often nearly impossible to pinpoint the cause. The only real-world examples of machine-to-machine interaction and escalation are found in financial markets, through phenomena such as flash crashes. These incidents offer limited insight, and extrapolating from them to nuclear escalation scenarios is fraught with risk. Applying escalation models derived from human decision-making to machines may fail, as these systems behave very differently.

Cultural dynamics also play a role. While militaries are typically conservative in adopting force-related innovations, and may be reluctant to fully embrace AI, other actors, including non-state entities and rival states, may be more willing to take those risks. As argued in his recent book, technology itself must increasingly be treated as an actor or surrogate in strategic analysis. This fundamentally alters the strategic environment. When machines can learn and adapt their functions, they are not simply tools; they become functionally competitive agents. The more capabilities an algorithm is given, the more it begins to rival human roles.

To conclude, artificial intelligence has already evolved through three identifiable waves:

1. **Predictive AI**, prevalent a decade ago.

2. **Generative AI**, which includes technologies such as deepfakes.

3. **Agentic AI**, now emerging.

Agentic AI involves autonomous agents capable of understanding specific tasks, developing strategies, and executing those tasks independently. This transformation will have significant implications for military operations and nuclear strategy alike. The emergence of agents capable of autonomous action introduces a new class of destabilizing technologies.

The U.S. Department of Defense, for example, is already investing in this domain. The Fortune Initiative aims to provide field commanders with AI-generated courses of action, further embedding AI into real-time battlefield decision-making.

The key takeaway from this discussion is that, in the rapidly evolving landscape of Artificial Intelligence and strategic stability, it is imperative to think beyond conventional paradigms. The pace of technological change requires policymakers and strategists to remain agile and innovative. What may seem impossible today could become feasible tomorrow. As a result, strategic thinking must encompass not only weapon systems but also the broader operational environment, including dimensions of perception and cognition.

Addressing the emerging challenges necessitates the development of new skill sets among practitioners. These include foresight, the ability to conceptualize alternative futures, cognitive resilience, and interdisciplinary competence. Strategic actors must be trained to detect and interpret weak signals—early indicators of disruptive shifts that could impact stability.

From an industrial perspective, the emphasis must shift toward responsible innovation. Security considerations should be prioritized in the development of AI technologies. Failure to embed safety mechanisms into the design process could lead to catastrophic consequences. In this regard, proposals such as the implementation of

"kill switches"—emergency shut-off protocols for autonomous systems—deserve serious attention.

Artificial Intelligence: Impact on South Asian Nuclear Deterrence

Dr Zafar Khan
Executive Director, BTTN

The topic assigned for this session requires a conceptual and scholarly analysis, presented within approximately twenty minutes. The remarks are grounded in existing academic literature and conceptual frameworks, with specific application to the South Asian context.

With the return of great power politics in the age of Artificial Intelligence (AI), the world has entered a phase of increasing strategic uncertainty. States are engaged in struggles to ensure their survival and territorial integrity. Within this evolving environment, emerging technologies such as AI, quantum computing, hypersonic glide vehicles, remote sensing, lethal autonomous weapons systems (LAWS), drone swarms, and anti-drone technologies are perceived as potential game-changers in warfare, enabling states to pursue swift and decisive military victories.

This evolving technological landscape has been described as the advent of a "Third Nuclear Age," and its implications are increasingly visible in the South Asian region. The core question becomes: how will these augmented technologies shape the policies of India and Pakistan, and what are the broader consequences for strategic stability in South Asia?

Proponents of AI-driven military innovations argue that this new revolution in military affairs (RMA) is imminent. An expanding body of literature suggests that AI integration across land, air, and sea domains could fundamentally alter the dynamics of warfare. These shifts may undermine the survivability of retaliatory capabilities, transform doctrinal and force postures, and intensify the offense-defense dilemma. Some scholars further suggest that AI-led command systems could marginalize human decision-making, potentially rendering traditional notions of nuclear deterrence obsolete.

Specifically, the development of lethal autonomous weapons systems, including autonomous drone swarms, is believed to enable operational autonomy: the ability to launch, navigate, identify targets, and strike without direct human involvement. In such a scenario, these AI-driven systems may not only revolutionize the tactical and operational landscape but also significantly challenge existing nuclear postures and strategies in the region.

This perspective assumes that AI-enhanced military systems will eventually replace traditional methods of tactical and operational planning. Such developments could erode second-strike capabilities, destabilize mutual deterrence frameworks, and blur the line between conventional and nuclear thresholds. In the South Asian context, where stability is already fragile, the rapid deployment of AI and machine learning in defense technologies may provoke arms racing behaviors, misperceptions, and crisis instability.

Hence, strategic thinkers and policymakers in South Asia must carefully evaluate the risks associated with the integration of AI into nuclear command, control, and communication (NC3) systems. Transparency, arms control measures, and the development of norms governing the use of autonomous systems are essential to mitigate escalatory dynamics and to preserve strategic stability in the region.

Many argue that traditional weapon systems, such as artillery, tanks, aircraft, bombers, and even nuclear weapons, could be undermined by AI-enabled autonomous platforms. Others contend that these systems may significantly affect nuclear strategies and related decision-making, particularly as the nature and character of warfare continue to evolve in light of AI technologies. For example, leading AI expert Danes Garcia has argued that the development and use of AI for lethal purposes in warfare fundamentally alters the nature of conflict. In a similar vein, Kenneth Payne asserts that AI introduces non-human decision-making that transforms the conduct of war.

These and other scholars argue that autonomous weapon systems, such as AI-linked warbots and robotic battlefield systems, could render adversaries increasingly vulnerable. Such technologies may impair a state's ability to conceal forces or movements on the battlefield, exposing them to barrages of lethal autonomous weapons. Scholars focusing on South Asia similarly warn that the integration of AI technologies could alter the military and nuclear strategies of regional rivals, thereby affecting the broader framework of strategic stability.

However, skeptics of AI-related technologies question the extent to which these innovations will dramatically transform warfare or enable rapid and decisive victories. Critics argue that AI may not entirely supplant traditional military tactics and strategic doctrines. They caution against overestimating the revolutionary potential of AI-driven platforms, suggesting that these systems may not fully replace the deterrent value of nuclear weapons in preventing large-scale war and ensuring mutually assured destruction.

For instance, Anthony King has argued in the *Journal of Strategic Studies* that while autonomous weapons may become more common, their transformative potential remains uncertain. He concludes that robotic warfare may not materialize in the manner often predicted. This skepticism extends to the broader critique that AI-enhanced military systems may not significantly alter the foundational logic of nuclear deterrence. Drawing upon the growing literature and embedding conceptual analysis within the South Asian context, this paper explores the applicability, adaptability, and implications of AI technologies for regional strategic stability. A central conceptual proposition is that in a conflict scenario, possession of AI capabilities may tip the balance in favor of offense. That is, the state armed with superior AI technologies could gain a decisive edge, undermining adversary's defensive or retaliatory capacity and potentially enabling preemptive strategies.

Thus, this analysis seeks to understand how AI-driven capabilities, if integrated into military planning and nuclear strategy, might influence

the offense-defense balance in South Asia and what this portends for long-term regional stability.

States in possession of AI-led technologies vis-à-vis their rivals often opt for offensive strategies aimed at achieving quick and decisive victories. Whether this perception reflects a genuine capability or a delusion associated with AI-led technological superiority remains a contested issue, giving rise to ongoing debates between proponents and opponents of such technologies. Historical examples include the United States–Iraq conflict, the Russia–Ukraine war, and the Second Nagorno-Karabakh conflict between Armenia and Azerbaijan.

South Asia presents a similar offense-defense dilemma. India's aspiration to acquire and integrate AI-led technologies, alongside other advanced military systems, vis-à-vis Pakistan encourages the potential for offensive posturing. Unlike the aforementioned examples, where conflict involved either two conventional powers or an asymmetry between nuclear and conventional forces, the South Asian context involves two nuclear-armed states. It remains uncertain how a presumed offensive by India against a nuclear-capable Pakistan might unfold. Given the heightened risk of escalation into a large-scale military conflict with unintended consequences, it is important to note that AI-led offensive capabilities may be more applicable when deployed by a nuclear power against a weaker conventional force, or by a strong conventional power against a smaller or exhausted adversary. However, it remains unclear how AI-led technologies might function or be advantageous in conflicts between two nuclear powers.

With regard to the transformation of warfare, proponents of AI-led technologies conceptually argue that such systems may fundamentally alter battlefield dynamics. Traditional tactics, at both the tactical and operational levels, could be increasingly replaced by autonomous systems, thereby reducing the relevance of conventional methods and materiel. It remains to be determined whether an "AI general" could render warfare more "nasty, brutish, and short." Proponents often cite

the aforementioned conflicts – such as the United States–Iraq war, the Russia–Ukraine war, and the Second Nagorno-Karabakh conflict—as case studies where AI-related technologies contributed to rapid and decisive military outcomes.

The more critical question, however, is whether these episodes reflect a fundamental change in the character of warfare. Existing literature suggests that while AI-augmented technologies played a significant role, the decisive factors in each case remained the human commanders, disciplined ground forces, traditional armored units, and artillery deployed on the battlefield.

From an empirical and conceptual standpoint, it remains uncertain whether India's acquisition of AI-led technologies can successfully transform the dynamics of warfare in South Asia. Despite its conventional superiority, India failed in its attempted preemptive strikes against Pakistan during the 2019 Balakot incident. Whether future operations bolstered by AI technologies would yield different results remains speculative. As every technology invites a counter-technology, Pakistan's effective countermeasures could render any Indian bid for a quick and decisive victory both difficult and complex.

Contrary to the assertions of AI technology proponents who presume that the dynamics of warfare, both operationally and tactically, are as straightforward as chess, the Clausewitzian universe emphasizes the inherent complexity of war. As Clausewitz noted, "everything in war is simple, but the simplest thing is difficult." Conceptually, it may be presumed that states acquiring AI-related technologies could modify their doctrinal force postures against potential rivals, adopting offensive strategies while sidelining traditional defensive mechanisms in pursuit of swift and decisive victories.

Empirical evidence from historical and contemporary strategic competition among rival powers supports this trajectory. In South Asia, for example, the acquisition and gradual integration of such technologies appear to be influencing India’s doctrinal evolution.

Several Indian security analysts, many of whom have served in senior strategic positions, argue for the reconsideration of India's declared No First Use (NFU) nuclear policy. For instance, Subrahmanyam Jaishankar and Shivshankar Menon have both indicated that circumstances may arise in which a first strike could be deemed necessary. Such views suggest that India, in possession of AI-led capabilities, may lean toward offensive strategies to achieve military and political objectives.

This transformation in India's force posture, driven by actual or perceived AI-enabled advancements, may have several consequences:

1. It could enhance India's confidence in pursuing offensive strategies;

2. It may increase temptations for preemptive strikes aimed at decisive victories;

3. It could support India's pursuit of regional dominance.

However, such offensive inclinations, particularly toward nuclear-armed adversaries such as Pakistan and China, risk exacerbating the regional security dilemma. This, in turn, could accelerate an arms race, heighten crisis instability, and increase the likelihood of escalation toward large-scale or even nuclear conflict.

The notion of replacing human commanders with autonomous systems is another prominent theme in existing literature. It remains uncertain whether the evolving and complex security environment of South Asia could accommodate the replacement of human battlefield commanders by AI-driven systems. The consequences of such a transformation, particularly between nuclear-armed states, are unclear and warrant careful scrutiny.

Proponents argue that lethal autonomous weapons systems and drone swarms operating without human oversight could revolutionize

warfare, enabling rapid decision-making and swift battlefield outcomes. These technologies are believed to outperform human decision-makers in speed and precision. However, historical evidence demonstrates that expectations of quick victories often prove illusory.

In this context, AI scholar James Johnson has argued that militaries utilizing AI for remote sensing, situational awareness, battlefield maneuvering, and compressed decision-making loops will likely gain significant tactical advantages over those relying solely on human judgment. Nevertheless, in a Clausewitzian framework rooted in empathy, discernment, and prudence, the complexity and chaos of real-world conflict cannot be reduced to algorithmic calculations. If all variables and outcomes were knowable and war was governed purely by rational considerations, it might be subject to an "algebra of action," but such assumptions do not hold in the human domain of war.

Theorists have argued that with the advancement of autonomous technologies, the need for the physical presence of armies could be diminished, reducing warfare to a theoretical relationship between forces. While narrow AI may contribute to decision-making processes, there is limited evidence suggesting that AI technologies, particularly in the military domain, can adequately distinguish the diverse dynamics and complexities of warfare. For example, Hunter and Bowen argue that while narrow AI can perform specific tasks such as playing games like chess and Go, or simulating aircraft flight, these functions do not imply that such systems can be entrusted with the responsibilities of military command.

A recurring theme in conceptual analysis is the *illusion of preemptive strikes*. States with modernized conventional and nuclear forces, such as India, may be tempted to initiate preemptive action against potential rivals. India has previously exhibited such tendencies and may continue along this trajectory as it integrates AI-led technologies into both its conventional and nuclear domains. New Delhi has been exploring doctrinal shifts geared toward counterforce strategies,

particularly against Pakistan. This temptation for preemptive action, while inconsistent with India's originally stated nuclear posture, becomes more plausible in the presence of AI-augmented capabilities that may incentivize offensive behavior.

Such developments raise the risk of unintended escalation. Scholars like James Johnson caution that AI-enhanced capabilities could have serious implications for the survivability of second-strike forces. Writers such as Preston and Lieber further argue that the foundational principles of nuclear survivability, specifically concealment and hardening, could be undermined by advanced AI technologies. However, it is equally plausible that states will continue to develop and deploy effective counter-technologies, allowing for the continued dispersal and concealment of retaliatory assets, thereby preserving deterrence stability.

Some AI scholars argue that emerging technologies may render nuclear deterrence increasingly irrelevant. According to this view, rivals may no longer be able to effectively conceal deterrent capabilities, including nuclear-powered submarines associated with second-strike assurance. Frequently cited literature in this area suggests that even submerged platforms may become detectable with the maturation of AI-enabled surveillance. Nevertheless, vulnerable states may adapt by adopting innovative strategies and deploying effective countermeasures against AI-driven technologies.

In this evolving environment, nuclear-armed states are likely to retain their deterrent arsenals and delivery systems. However, second-strike capabilities may become increasingly vulnerable in an era marked by AI-facilitated counterforce targeting. With the development of counter-technologies, it remains possible to secure strategic assets. For every offensive technological innovation, there exists the potential for a corresponding countermeasure.

To conclude, three key observations emerge from this analysis:

1. It is unlikely that AI-related autonomous systems will possess limitless capacity to identify, strike, and destroy targets with absolute precision.

2. The significance of traditional military systems, particularly the role of human military commanders, cannot be entirely sidelined or rendered obsolete. The continued emphasis on retaining "human-in-the-loop" control reflects the enduring value of human judgment in warfare.

3. AI-enabled weapon systems may ultimately favor defensive strategies rather than offensive ones. However, it remains uncertain whether the conceptual assumptions underpinning these technologies can be fully applied to, or hold the same relevance in, the South Asian strategic context.

These conclusions underscore the need for a cautious and context-specific approach when evaluating the impact of AI on nuclear deterrence in South Asia.

Question Answer Session

Q: Even if AI integration into nuclear decision-making remains technically premature, some states might still pursue it for perceived strategic advantage. How can states avoid the classic dilemma, where mutual restraint on AI-enabled nuclear command, control, and communication is ideal for strategic stability, but mistrust and unilateral incentives undermine it? What realistic measures or mechanisms can build trust and preserve meaningful human control amid compressed timelines and autonomous escalation risks?

A: The integration of AI into nuclear command and control is no longer theoretical. Having worked on AI for over a decade, the topic has shifted from being fringe to becoming central in defense dialogues. For example, discussions at the REAIM Conference in South Korea highlighted increasing focus on integrating AI in nuclear command systems.

The key challenge is trust. The world is currently experiencing an epistemic crisis where facts are increasingly replaced by opinions, eroding the standards for determining truth. This has serious implications for nuclear stability. Modern AI technologies now manipulate emotional responses using tools like eye trackers and brain-monitoring earbuds, thus shaping individual reactions to information.

To build trust, interpersonal relations and consistent communication are vital. However, the ability of AI to tailor misinformation to manipulate perception presents unprecedented risks. Traditional methods such as critical thinking may no longer suffice. A broader regulatory framework, akin to arms control agreements of the Cold War era, such as "subversion control agreements," may become necessary to address the influence of AI on human cognition and strategic decision-making.

Q: What practical trust-building measures can states adopt?

A: Interpersonal relations and diplomatic engagements are essential. However, due to intense competition in AI development, particularly between the United States and China, establishing global governance is increasingly difficult. For example, the removal of ethical AI guidelines by the Trump administration illustrates how strategic interests often outweigh ethical considerations.

The rapid pace of AI development is far outpacing regulatory capabilities. Governments often lack the flexibility to think outside the box, making regulation unlikely in the near future. Therefore, continued technological advancement without sufficient oversight appears probable.

Q: Given the increasing interaction with empathetic AI, is it possible that in a future nuclear crisis, leadership might over-rely on AI-generated options, believing these takes into account human nuance, empathy, and destruction? Could such reliance dangerously influence the decision-making process?

A: Dialogue and confidence-building measures remain essential. Current discussions are heavily focused on the P5, but all nuclear-armed states must be involved. One step that can be taken unilaterally is the establishment of internal risk assessment frameworks to identify where AI might fail and cause escalation, especially within national NC3 systems.

In a recent *War on the Rocks* article, it was argued that instead of committing merely to maintaining human involvement in decision-making loops, states should adopt a broader commitment: that AI integration must not result in inadvertent escalation. This principle can guide both national policies and international dialogue. Inclusive multilateral discussions, coupled with concrete unilateral steps, represent the most logical path forward.

Q: In the absence of an international framework regulating AI-related technologies, especially one that includes all nuclear-armed states, those already possessing advanced capabilities are at an advantage. Is there any precedent from non-proliferation settings that could be adapted? Regionally, Pakistan faces a disadvantage compared to India. How can this imbalance be addressed?

A1: This question goes to the heart of the discussion on the future of nuclear deterrence. What exactly should be controlled through regulation? If the focus is on futuristic concerns like autonomous robots, it may seem less urgent. However, if the concern is about the current and increasing risk of nuclear escalation exacerbated by AI, the approach must return to traditional arms control frameworks.

Arms control is far from obsolete. It encompasses more than treaties—it includes transparency measures, consultations, technical tools, and trust-building mechanisms. These mechanisms already offer platforms to address AI's contribution to nuclear risk. For instance, U.S.-Russia bilateral talks and P5 nuclear consultations have begun addressing AI-related challenges. These should be expanded and intensified.

A2: The regulation of AI and associated trust-building measures are essential. However, formal regulatory mechanisms for AI remain absent. Historically, it took many years for the international community to arrive at agreements like the NPT. A similar timeline may be required for AI governance. The process will likely depend on whether leading and emerging powers possess or deploy these technologies before initiating formal regulatory discussions. Past nuclear arms control developments provide useful empirical parallels. Therefore, regulation of AI, both ethically and strategically, may eventually evolve, but only over time.

Session-III

Impact of Emerging Technologies on Peaceful Uses of Nuclear Technology

Moderator: Dr. Rahat Iqbal
Associate Director CISS

Role of Emerging Technologies in Expanding Peaceful Applications of Nuclear Technology

Mr Anton V. Khlopkov
Director, Center for Energy and Security Studies (CENESS)

Emerging technologies not only present new proliferation challenges but also offer notable opportunities and benefits. Several examples from the nuclear industry illustrate how emerging technologies, including artificial intelligence (AI), are already being utilized. For instance, AI can be used to analyze vast amounts of data from aerial surveys to identify areas rich in minerals such as uranium, a key component for nuclear fuel.

In the domain of centrifuge production, currently the central technology for uranium enrichment, AI can reduce costs associated with the design, testing, and production of centrifuges. It can also save time in the development of newer, more efficient centrifuge designs, thereby reducing overall associated expenses.

Similarly, in nuclear power plant design, emerging technologies can shorten the time required for developing new reactor types and testing prototypes. These technologies help identify necessary improvements and enhance the efficiency of nuclear power plant operations, increasing their economic competitiveness. This is especially critical for regions or countries where cost competitiveness is a major concern. Historically, certain nuclear plants in the United States were shut down due to economic reasons. If emerging technologies provide opportunities to reduce operational costs, the appeal of both large-scale and small modular reactors may increase.

Another area of importance is nuclear safety. Digital twin technology, for example, allows for the creation of a digital replica of a nuclear reactor. This can be used to forecast plant operations and enhance overall safety.

Examples from Russia's experience also demonstrate the integration of AI and other emerging technologies into the nuclear sector. These technologies are actively used in uranium mining. A notable case is at the Khiagda facility, where the use of emerging technologies led to increased mining efficiency. Such technologies also improve personnel safety at mining sites and can be applied to various nuclear facilities in Russia and beyond. Similarly, predictive models for components such as generators, turbines, and circulation pumps have been implemented in newly constructed nuclear power plants, including the sixth unit of the Novovoronezh Nuclear Power Plant. These models help operators anticipate equipment behavior, thereby enhancing operational safety. According to data from the Russian State Nuclear Corporation Rosatom, the predictive algorithms can forecast nuclear power unit parameters up to 30 minutes in advance—an essential feature for maintaining safe plant operations.

It is essential to emphasize that despite the advancements brought by emerging technologies—especially AI—humans must remain at the center of nuclear facility operations. The "human-in-the-loop" concept must continue to be central to the functioning of nuclear power plants. New technologies are best positioned as supportive tools that assist human operators in enhancing the safety and efficiency of nuclear facilities. There is a certain irony in the fact that new technologies are not only capable of supporting and enhancing the efficiency of the nuclear industry but also of making it significantly safer. However, at the same time, these technologies often require substantial amounts of electricity. This results in increased energy demand, including the construction of new power plants or the resumption of operations at previously shut-down facilities, even those once considered permanently closed. A notable example is the Three Mile Island Nuclear Power Plant, the site of one of the most significant nuclear accidents in history. The first unit of the plant was permanently shut down in 2019. However, due to a request from Microsoft, plans are now underway to restart the operation of this unit in the near future.

The Role of Emerging Technologies in the Achievement of UN SDGs

Dr Robert B. Hayes
Associate Professor, Department of Nuclear Energy, North Carolina State University

The focus of this presentation is on how Small Modular Reactors (SMRs) can play a transformative role in advancing the United Nations Sustainable Development Goals (UN SDGs). One often overlooked yet promising area in this regard is uranium extraction from seawater. The world's oceans contain an estimated 4.5 billion tons of uranium, naturally introduced through geological processes such as erosion and continually replenished by plate tectonic activity. This effectively makes it a renewable and virtually inexhaustible resource, offering humanity a sustainable pathway to secure nuclear fuel for generations to come. If breeder reactors were utilized, the amount of uranium deposited annually into the oceans by rivers alone could generate nearly nine times the United States' yearly electricity consumption. This underscores an immense yet largely untapped reservoir of energy potential. Although such topics rarely feature in mainstream energy discussions, they highlight the often-underappreciated advantages and long-term sustainability that nuclear energy offers in meeting global energy and climate goals.

A particularly striking observation is that – even when accounting for the Chernobyl disaster—nuclear power remains statistically safer than wind energy. This comparison not only reinforces nuclear energy's viability but also underscores the technological evolution within the field. Comparing Chernobyl to today's reactors is much like comparing the Hindenburg to modern aviation – a reminder that the lessons of the past have led to vastly improved, safer, and more efficient technologies.

One fundamental reason for nuclear energy's relative safety is its energy density. As a comparison, the combustion of fossil fuels yields

approximately 1 electron volt (eV) per atom. In contrast, the fission of a uranium-235 atom yields approximately 200 million electron volts (MeV). Energy density is directly proportional to environmental friendliness, which explains the interest in fusion and other high-density energy sources. Fission products—byproducts of nuclear reactions—are often viewed as problematic. However, they can potentially be converted into useful commercial products. This is already being done in the field of nuclear medicine, although not all fission products have found commercial applications yet. Continued research and development may unlock new uses.

Public concern often centers around the use and storage of nuclear fuel, particularly regarding small modular reactors. However, the high energy density of nuclear fuel significantly mitigates these concerns. For context, over the past 50 years, the United States—one of the largest energy consumers globally—has derived approximately 20 percent of its electricity from nuclear power. Despite this vast amount of energy production, the total volume of used nuclear fuel generated would not fill more than a single football field stacked 10 meters high. This demonstrates the extraordinary efficiency of nuclear energy.

While concerns such as terrorism targeting used nuclear fuel exist, the reality is that current technologies are well-equipped to manage these challenges. Public perception is often shaped by misleading narratives, but the technical community has effective solutions that ensure both safety and sustainability.

To obtain a license from the Nuclear Regulatory Commission (NRC) to store used nuclear fuel in specialized casks, the design must undergo rigorous safety testing. The cask must be dropped from a height of 30 feet (approximately 10 meters) onto an unyielding surface without leaking. Subsequently, it must be dropped again, this time from 40 inches onto a steel bar – targeting its weakest structural point – again without leakage.

Next, the cask must withstand a simulated tunnel fire at approximately 1,500°F (815°C) and still retain its structural integrity. Furthermore, it must be submerged under 50 feet of water for eight hours without leaking. All of these tests are sequential, and only upon successful completion of all these stages can a license be granted. These casks are virtually indestructible.

As a health physicist, radiation safety expert, nuclear engineer, and nuclear scientist, it is worth noting that, from a safety perspective, the threat posed by a terrorist attempting to detonate explosives near such a cask is minimal. While any malicious act is undesirable, these containers are designed to survive such scenarios. In that context, even an attempted attack might result in fear, but not fatalities. From a security standpoint, such resilience could potentially serve as a deterrent or diversion away from more vulnerable targets.

One of the critical contributions of nuclear energy to the United Nations Sustainable Development Goals (SDGs) lies in the field of medical isotopes (SDG 3: Good Health and Well-being). Radioactive isotopes—produced in the core of nuclear reactors – are used in diagnostic imaging and cancer treatments, saving millions of lives. This is a prime example of how something inherently dangerous can be safely controlled and used for beneficial purposes.

Additionally, nuclear energy supports food security through preservation. In many developing countries, sufficient food is produced, but preservation remains a challenge due to a lack of energy infrastructure. Without the ability to cook, freeze, or transport food, spoilage is inevitable. Reliable energy, particularly energy with high density like nuclear, enables preservation and supports higher living standards.

Much of the opposition to nuclear energy stems from fear of radiation. However, this fear often arises from misconceptions. For example, simply being present in a typical building can result in a radiation dose of approximately 10^-5 joules per kilogram. While such a number

might appear alarming when associated with electricity production, it becomes mundane when attributed to natural background sources such as radon gas from the ground, cosmic radiation from outer space, or internal sources like potassium in the human body.

That same radiation dose – 10^-5 joules per kilogram – equates to about 0.01 millisieverts, which is the average daily background dose in the United States. When properly contextualized, these numbers reveal that routine radiation exposure is not inherently dangerous and certainly not unique to nuclear energy.

After all that has been explained, such a dose would likely not appear alarming. However, without proper context, it easily could. Most people are neither health physicists nor nuclear scientists, and in the absence of accurate understanding, even scientifically correct figures can be misinterpreted or appear unduly frightening.

A radiation dose of 0.05 millisieverts is roughly equivalent to a round-trip flight from Los Angeles to New York – exposure from cosmic rays at altitude. Interestingly, that same number is also the U.S. Environmental Protection Agency's (EPA) drinking water standard. Over the course of a year, if one were to consume water with radioactive content at the regulatory limit, they would receive no more than 0.05 millisieverts annually, and that is the legal threshold.

Imagine being informed that 0.0501 millisieverts of radiation was received from drinking water, just above the permitted standard. Such a minute exceedance would likely provoke public concern, media attention, and regulatory action. Despite its negligible magnitude, it tends to be perceived as hazardous simply because it crosses a legal threshold. This illustrates how highly conservative and precautionary contemporary regulatory frameworks are, particularly in matters of nuclear safety.

Scaling this further, 0.1 millisieverts represents the regulatory limit for airborne, off-site radiation releases from a nuclear facility threshold

that, if exceeded, would constitute a legal violation. Yet few recognize that this same dose is roughly equivalent to the minimum internal radiation an individual receives from potassium, a naturally radioactive and essential element present in every human body. Most people remain unaware of potassium's radioactivity, even though it is vital for biological function and indispensable for survival.

For a small-framed woman or a child, the internal radiation dose from naturally occurring potassium amounts to roughly 0.1 millisieverts per year. In contrast, for a large or muscular individual, the dose may reach up to 0.4 millisieverts, as potassium is primarily stored in muscle tissue. Such exposure, however, is not dangerous—it is a normal and essential aspect of human physiology, reflecting the body's natural balance rather than any health risk.

Now consider a dose of 1 millisievert – the typical exposure from a standard medical X-ray, such as one taken for a dislocated hip. This value also represents the maximum legal annual radiation dose permitted for an individual residing at the boundary of a U.S. nuclear facility. In other words, even someone living year-round just outside the plant's perimeter could not, by law, receive more than 1 millisievert of radiation from that facility. In practice, however, operators maintain doses well below this threshold, as regulatory penalties – often exceeding $10,000 per day – strongly incentivize strict compliance with safety standards.

In the United States, the average annual radiation dose from all sources, including natural background radiation, is about 3.2 millisieverts. This average accounts for population distribution, with lower doses near coastal areas and higher levels inland – such as on the Colorado Plateau—where natural uranium deposits and increased cosmic radiation exposure occur.

Several orders of magnitude in radiation exposure have now been considered – from 0.05 to 3.2 millisieverts – encompassing examples from daily activities, medical procedures, and nuclear regulatory

limits. The question that naturally arises is: at what level does radiation truly become alarming? In reality, public fear tends to originate from misconception rather than actual hazard.

At higher levels, such as 10 millisieverts, exposure remains within the realm of ordinary medical practice. For example, a cardiac stress test – particularly for older individuals – typically involves the injection of radioactive thallium, followed by exercise on a treadmill to assess heart function. The average dose from this diagnostic procedure is approximately 10 millisieverts, well within the range of controlled and medically justified exposure.

In the United States, if a member of the public receives 10 millisieverts in a single year, the EPA can issue evacuation orders. Moreover, if an individual continues to receive 5 millisieverts annually thereafter, authorities are permitted to maintain those evacuation orders indefinitely – potentially forcing a permanent relocation from one's home.

This is where cognitive dissonance sets in: individuals are told to leave their homes permanently to receive a dose equivalent to that from a CT scan to the head, chest, or hip. Many people have undergone scans, which typically involve a dose around 10 millisieverts. That is approximately the same threshold that, in the regulatory context, may prompt a forced evacuation. While in practice, evacuation may occur at doses closer to 20 millisieverts, the 10 millisievert threshold remains the minimum legally required to justify permanent relocation in the U.S.

Such contradictions can undermine public confidence and breed skepticism. When a health physicist assures, "This is not a significant dose," yet regulatory authorities still order relocation, it's natural for people to question whether nuclear experts truly grasp the risks. In truth, they do – the regulations are deliberately and exceptionally conservative by design.

At 50 millisieverts, the annual legal dose limit for occupational radiation workers in the U.S. is reached. Even under the linear no-threshold (LNT) model, which assumes any amount of radiation carries some risk, this dose is still regarded as safe. The associated risk remains lower than many common industrial or workplace hazards.

Moving to 100 millisieverts, a few scientific studies, particularly those involving children undergoing radiotherapy, have indicated a measurable increase in cancer probability of approximately 0.5%. This is the first observed threshold where radiation exposure shows any clinically measurable medical effect. Before this level, no consistent or statistically significant health effects have been documented – not even minor symptoms.

To put that in perspective, the average lifetime cancer risk in the United States is around 40%. In simple terms, nearly half of all people will develop some form of cancer over their lifetime – be it melanoma, lung cancer, or another type. Against this backdrop, a 0.5% increase at 100 millisieverts represents only a small addition to the existing baseline risk.

At 1,000 millisieverts (or 1 sievert), the threshold for acute radiation syndrome (ARS) is reached. At this level, the estimated cancer risk increases by about 5%, similar to what was observed among atomic bomb survivors. Although this represents a significant dose, it does not pose an immediate threat to life; rather, it reflects a moderate rise in long-term cancer risk – from roughly 40% to 45%.

The Chernobyl liquidators were the individuals – mainly Soviet military and civilian personnel – who were deployed to clean up the aftermath of the 1986 Chernobyl nuclear disaster. Many of them became convinced that any kind of deleterious health effect they experienced—be it arthritis, memory loss, hearing impairment, hair loss, or anything else – must have been caused by Chernobyl. But how can anyone be certain? How did anyone know it was Chernobyl? And therein lies the issue: it becomes a self-fulfilling prophecy. Any later

health problem is often assumed to be proof of exposure. Look, I just had a health issue. It must have been Chernobyl. But how can that be known? Is the person a health physicist? Do they understand which symptoms radiation actually causes? That's the challenge. For most people, limited scientific understanding makes radiation seem frightening.

Now, to conclude, when harnessing high energy density – as with nuclear power – nations can effectively achieve the United Nations Sustainable Development Goals (SDGs). These goals are met one after another, starting with affordable and clean energy.

Nuclear power also performs extremely well in terms of environmental impact. Consider the quantity of materials required for mining, milling, manufacturing, and waste management. If one assesses only the infrastructure needed to build the plant – excluding the fuel – nuclear energy is dramatically superior to solar and wind in terms of resource efficiency. It simply does not require the same scale of raw material extraction and industrial processing.

Unless society would rather expand mines, tailing ponds, and large-scale manufacturing, nuclear energy offers a far more sustainable path forward. The difference in land use alone is staggering. On a logarithmic scale, the area required for nuclear power is only a fraction of that needed for renewables – several orders of magnitude smaller.

Beyond electricity generation, nuclear energy can also drive desalination, industrial heat production, hydrogen generation, and the manufacture of concrete and steel – processes that currently depend heavily on fossil fuels. In each of these areas, nuclear power provides a cleaner, more efficient alternative.

Furthermore, think about food preservation. In many developing countries, food is grown in abundance, but without sufficient energy for cooking, refrigeration, and transport, most of it perishes. Irradiation of food – which is safe and effective – could dramatically extend shelf

life. It's essentially a form of heating, but without the greenhouse gas emissions. Unfortunately, fear of the word "irradiation" still limits its adoption.

So, to summarize quickly: nuclear energy directly supports multiple Sustainable Development Goals. From clean energy and climate action to industrial innovation and health, it checks all the boxes. If the objective is truly sustainable development, then nuclear is the way forward. Yes, fusion may eventually become viable – but at present, it remains a technological dream, possibly 50 years away. In the meantime, nuclear fission – especially via small modular reactors – offers a proven, powerful, and scalable solution.

Emerging Technologies for Nuclear Safety/Security/Verification: Challenges and Opportunities

Dr Tariq Rauf
Former Head of Verification and Security Policy, IAEA, Austria

Artificial intelligence (AI), at its core, is machine learning (ML) that holds promising potential for utilization in various aspects of the nuclear fuel cycle, including nuclear verification, nuclear safety, and nuclear security. Machine learning, including large language models (LLMs), operates through internal processes that are generally incomprehensible to humans. As ML systems function, vast arrays of numerical values change as the system learns and processes data. All embedded knowledge in the ML system exists within these numerical arrays, making it difficult to derive or understand the underlying rules. AI proponents consider ML systems to mimic human logic, problem-solving, and decision-making. AI relies on transformers – a type of neural network architecture – that convert input sequences into output sequences by learning contextual relationships between elements in a sequence.

For example, given the input sequence, "What is the color of the sky?", the transformer model utilizes a mathematical representation to recognize the relevance and relationship between the words "color," "sky," and "blue." Drawing upon the training data provided by human operators, the model generates the output: "The sky is blue."

Skeptics of AI/ML argue that the human brain comprises more than 100 trillion synaptic transformers and that current global computing capacity remains insufficient to match human cognitive processing. Furthermore, AI and ML remain entirely dependent on human-generated training data and operational algorithms. These technologies do not enable the violation of physical laws and cannot create facts where none exist. They can enhance understanding of known phenomena within limits but cannot address unknown unknowns more effectively than humans.

Even quantum computing is subject to these limitations, as noted by the Alan Turing Institute at the Royal Institution in London. At its core, machine learning is rooted in statistical analysis. Correlation does not imply causation. The principle of "garbage in, garbage out" remains valid – bad or biased data will produce flawed outputs. This concern is particularly acute for LLMs trained on web-scraped data comprising approximately 500 billion words, which include both high-quality and biased content.

Serious concerns arise regarding the integrity of training data fed into AI, ML, and LLM systems, especially in the context of nuclear safeguards, safety, and security – the so-called "three S's."

This concern is underscored by the reality that training data in these domains primarily reflects value judgments from Western sources – predominantly from the United States – and includes government, industry, academic, media, and policy sectors. Such data can be deeply biased, particularly as countries in the Global South are often portrayed as proliferation threats to the nuclear order established by Western technology holders.

Key open-source information (OSI) providers for this AI enterprise include institutions such as Project Alpha, media entities like the Economist Intelligence Unit and Jane's, and databases such as Google and the CIA Factbook, alongside intelligence organizations. While OSI experts in many cases lack nuclear technical or linguistic expertise, they possess access to powerful big data platforms including Palantir, Oracle, Google, Meta, and Amazon, in addition to open-source satellite imagery from Airbus, Maxar, PlanetLabs, and others.

This OSI is then fed into AI- and ML-based proliferation trackers, and the output contributes to the formation of State Nuclear Profiles. These collection and assessment practices are applied differentially. To the best of current knowledge, such scrutiny is not conducted with equivalent rigor for countries such as India and Israel. In contrast, so-called "proliferation risk states" such as Algeria, Egypt, Morocco, Saudi

Arabia, and Turkey are subjected to more intensive surveillance. Conversely, "friendly proliferation" cases, including Japan, Poland, Germany, and South Korea, typically do not face similar levels of scrutiny.

The conclusion, therefore, is that in the realm of the three S's – nuclear safeguards, safety, and security – serious concerns persist regarding the quality of training data fed into AI and ML systems, along with the consequences that may ensue. Generative AI, a subset of deep learning neural networks, has captivated public attention by producing original texts, images, and videos. It is highly versatile and adaptable to a wide array of functions and activities. Most users encounter it on mobile devices in the form of predictive text, Google Translate, ChatGPT, DeepSeek, and related applications, which are often riddled with errors.

While generative AI may be helpful for administrative tasks across industries, its application in the operation of nuclear facilities and power plants presents significant challenges due to its lack of integrity and overall opacity. The internal workings of artificial neural networks and the logic by which they arrive at conclusions remain poorly understood. More transparent systems – referred to as explainable generative AI – could offer promise for broader use in repetitive tasks and data processing within the civilian nuclear fuel cycle.

It is important to distinguish between AI and ML systems and advanced robotics in the nuclear field. While these are often equated, they are fundamentally distinct. Advanced robotics, largely a product of biomechanics, involves machines programmed with algorithms to perform complex physical tasks in the real world. These systems rely on hardware, sensors, actuators, and mechanics, and are capable of repetitive motion tasks.

When AI and ML are combined with robotics, the result is intelligent robots – machines capable of interacting with their environment and

making programmed decisions. Examples include aviation autopilot systems, autonomous drones, and self-driving vehicles.

In the nuclear field, intelligent or "intelligentized" robots are already in use. These include nuclear fuel loading and unloading machines, robotized Cherenkov viewing devices (which float in spent fuel ponds to measure Cherenkov radiation and count submerged fuel assemblies), and laser curtains for containment tracking, installed at facilities in La Hague (France), Ezeiza (Argentina), and Olkiluoto (Finland). In Iran, online enrichment monitors have been deployed at the Natanz and Fordow enrichment plants. Additionally, "suicide robots" have been used to assess damage at nuclear accident sites such as Chernobyl Unit 4 and the Fukushima Daiichi reactors, allowing engineers to plan for remediation.

Despite earlier concerns, ML and robotics have proven beneficial in certain areas of the nuclear industry. ML algorithms are leveraged for real-time monitoring and predictive maintenance. By processing large volumes of sensor data, ML systems can identify anomalies, allowing human analysts to focus on potential irregularities rather than sifting through irrelevant information. One operator remarked: "We removed the haystack." However, such confidence may be misplaced. Data gaps or flawed data can result in critical system failures if key interactions are missed or misunderstood by AI systems. Therefore, the "human-in-the-loop" remains indispensable.

Potential applications of AI in nuclear power plants include improving operational efficiency and ensuring a consistent electricity supply by dynamically adjusting power generation based on real-time inputs, such as consumer demand, weather patterns, and equipment performance. Yet, AI, ML, and robotics do not replace human analysis and decision-making. Rather, they augment these processes, offering faster and potentially more accurate results while still requiring indispensable human oversight.

Although there is significant interest in adopting AI-based solutions in the nuclear industry, regulatory approval remains a prerequisite. Regulators must understand the relevant AI and ML technologies in detail to develop standards, guidelines, and licensing mechanisms for their deployment.

Future deployment of such technologies necessitates the establishment of robust regulatory frameworks, developed collaboratively by regulatory authorities and industry stakeholders. Since 2021, the IAEA has recognized the potential for AI in nuclear power operations. It has released reports and established working groups under the International Network on Innovation to Support Operating Nuclear Power Plants (ISOP) to explore the regulatory and technical dimensions of AI deployment.

The IAEA has designated the Center for Science of Information at Purdue University in the United States as an official IAEA Collaborating Centre. This collaboration aims to support the Agency's activities related to the application of AI in nuclear power, including reactor design, plant operations, and educational and training initiatives. Notably, Dr. Pervez Butt, former Chairman of the Pakistan Atomic Energy Commission (PAEC) and former Chair of the IAEA Board of Governors, who received training at Purdue University, would likely view this development with particular satisfaction.

In addition, the IAEA has designated the Plasma Science and Fusion Center at the Massachusetts Institute of Technology (MIT) as a Collaborating Centre, focusing on the acceleration of fusion research. This includes applying AI tools to support the IAEA’s initiative on artificial intelligence for fusion technologies.

As of now, a total of 73 IAEA Collaborating Centers are active worldwide. The Agency is also leading a Coordinated Research Project (CRP) that investigates how AI and other innovative technologies can expedite the development and deployment of small modular reactors (SMRs).

Furthermore, the IAEA will host its first-ever International Symposium on Artificial Intelligence and Nuclear Energy at its headquarters in Vienna, scheduled for 3–4 December this year. The symposium aims to explore how nuclear energy can meet the increasing electricity demand from AI-driven data centers and examine the growing convergence between AI and nuclear technologies. The event will focus on two major themes:

1. Powering data centers with nuclear energy; and

2. Opportunities and challenges for AI within the nuclear sector.

The timing of this symposium reflects the parallel rise of AI and the resurgence of nuclear power as mutually reinforcing global trends.

Leveraging Artificial Intelligence for Enhanced Nuclear Verification by the IAEA

AI and ML offer multiple potential applications for strengthening nuclear verification under the IAEA safeguards regime. It is important to note that the Agency applies the same safeguards, objectives and measures to similar nuclear technologies and facilities, regardless of the type of safeguards agreement in place. The comprehensive technical details of this framework can be found in the presentation submitted to the Conference on Disarmament (CD/PV.1037).

The overarching goal is to enhance the effectiveness, efficiency, and credibility of IAEA safeguards by integrating advanced technologies and improving data analytics capabilities. Several potential, though non-exhaustive, applications of AI/ML in nuclear safeguards include:

1. **Satellite Imagery Analysis:** AI can support near real-time detection of undeclared nuclear activities by analyzing satellite imagery. This includes monitoring for the construction of fuel fabrication, enrichment, or reprocessing facilities, detecting activity at nuclear reactors, and identifying the movement and

storage of spent nuclear fuel. AI tools can also assist in planning targeted inspector visits.

2. **Image and Video Surveillance Analysis:** AI can analyze large volumes of CCTV footage from safeguarded facilities to detect anomalies such as unusual patterns of movement, unauthorized access, or tampering with nuclear materials and instrumentation.

3. **Integration of Emerging Technologies**

    - **Internet of Things (IoT):** Tamper-proof sensors can be deployed to monitor real-time environmental conditions, facility operations, and material movements.

    - **Blockchain:** AI systems can be integrated with blockchain for the secure logging of verification data, thus enhancing transparency and preventing tampering.

4. **Environmental Sampling and Nuclear Forensics:** Advanced AI tools can support the detection of isotopic signatures in environmental samples—air, water, and soil—that may signal undeclared nuclear activity. There is also ongoing development toward the miniaturization and field deployment of portable detection systems for in-situ containment and surveillance operations.

In sum, while the promise of AI in nuclear safeguards and power applications is substantial, the implementation must proceed with rigorous regulatory oversight, robust data governance, and international cooperation to ensure that such technologies enhance rather than compromise the credibility of the nuclear non-proliferation regime.

There are additional uses of AI in the modernization of safeguards inspection protocols. These include the development of optimized inspection schedules and criteria as the global inventory of nuclear material under safeguards continues to expand. AI can also increase the use of unattended monitoring systems, thereby reducing the resource burden on inspectors and improving efficiency.

In the domain of predictive maintenance and equipment monitoring, AI could enhance the reliability of installed safeguards instruments – such as cameras, tamper-indicating seals, and radiation detectors – by predicting failures before they occur. This would help ensure uninterrupted verification operations.

Leveraging Artificial Intelligence for Enhanced Nuclear Safety and Security

Nuclear safety and security are core pillars of the IAEA's mission to ensure the peaceful use of nuclear energy. As threats evolve – ranging from sophisticated cyberattacks to insider threats – the tools to prevent, detect, and respond to these challenges must also advance. The objectives of AI deployment in this domain are threefold:

1. Strengthen real-time detection of unauthorized activities and threats;

2. Analyze complex data for early warning and effective response; and

3. Enhance both physical and cyber safety and security measures at nuclear facilities.

Several potential applications exist for integrating AI into nuclear safety and security frameworks:

- **Anomaly Detection in SCADA Systems:** AI-enhanced supervisory control and data acquisition (SCADA) systems can identify operational anomalies in real-time.

- **Cybersecurity Applications:** AI may support:
    - Intrusion detection;
    - Anomaly detection in network traffic;
    - Enhanced vulnerability scanning;
    - Automated patch management; and
    - Predictive threat intelligence using machine learning on cyberattack patterns.
- **Physical Protection Systems:** AI can improve perimeter surveillance through smart fencing and autonomous drones. These systems may integrate various sensor types – thermal, acoustic, visual, and pressure-based – to provide comprehensive 360-degree situational awareness.
- **Hybrid Threat Modeling:** AI-informed analyses could be used to update the nuclear security design basis threat (DBT), refine response protocols, and model complex cyber-nuclear hybrid threats.
- **Emergency Response Optimization:** AI simulations can model complex emergency scenarios, offering recommendations for optimal evacuation routes and containment measures. Furthermore, AI may dynamically update crisis response strategies based on changing inputs such as weather, infrastructure damage, or radiation dispersion. AI-assisted dashboards can also enhance decision-making and inter-agency coordination during emergencies.

Conclusions

Integrating AI and ML into the IAEA's nuclear verification, safety, and security (the "3S" framework) presents a potentially transformative

opportunity to address emerging threats more effectively. However, this integration also introduces significant risks to the operational integrity of the Agency.

With appropriate safeguards, transparency, and multilateral collaboration, AI and ML can serve as powerful enablers – indeed, as force multipliers – in support of the IAEA's global mission to enhance the security and safety of nuclear infrastructure and materials. However, these technologies cannot replace human expertise or judgment. Competent human oversight must remain an indispensable element in all critical operations and decision-making processes.

Significant risks accompany AI integration, including:

- The use of deepfakes and spoofed data, which are increasingly accessible to state and non-state actors, criminals, and malicious entities. These technologies have already been exploited to compromise sensitive nuclear infrastructure.

- False positives or misinterpretations of ambiguous events, which may undermine the credibility and integrity of nuclear governance frameworks.

Recommendations

It would be prudent for the IAEA, in collaboration with experts from the AI/ML and nuclear sectors, to develop risk-informed and performance-based regulatory frameworks for the safe and secure application of artificial intelligence across nuclear verification, safety, and security domains.

Finally, it must be acknowledged that IAEA Member States remain divided on the potential benefits and risks of AI and ML technologies. While some advocate for their expanded use, others express concern that unregulated or widespread integration could compromise the Agency's independence, technical integrity, and global credibility.

Question Answer Session

Q: How can AI play a role in the vigilance of nuclear security personnel?

A: AI could have both positive and negative implications in this context. Historical incidents have shown that nuclear scientists have been targeted in some countries using advanced technologies, including AI—a matter more aligned with nuclear insecurity than security. Regarding nuclear security, one example already discussed was the use of emerging technologies to prevent the illicit transportation of nuclear materials and technologies.

While specific applications of AI in personnel vigilance were not detailed, it is anticipated that companies engaged in nuclear security services will seek to integrate AI and other emerging technologies into the solutions they offer commercially. Further insights and real-world examples may be provided by colleagues, such as Rob and Tariq, during the panel, as they are likely aware of current AI applications that enhance nuclear security.

Q: The IAEA is providing a platform for the use of AI for peaceful purposes. Given the broad acceptance by Member States, could such a guiding framework or platform also be envisioned for non-peaceful nuclear technologies? Could this model be adopted by other institutions to regulate the use of AI in the non-peaceful nuclear domain?

A: While this is a valuable suggestion, even in the peaceful nuclear domain, the application of IAEA standards is subject to national sovereignty. The standards and guidance provided in areas such as nuclear safety and security are recommendations; it is the responsibility of governments to incorporate them into domestic legislation. Thus, the path from standard formulation to implementation is neither simple nor short.

As discussed in previous sessions, new technologies can introduce global risks. It is hoped that political leadership will be prudent enough to accept and negotiate certain restrictions and integrate them into national frameworks. However, the IAEA does not appear to be the appropriate platform for regulating AI in non-peaceful nuclear domains. Instead, this responsibility may more appropriately lie with international institutions such as the United Nations, particularly the United Nations Office for Disarmament Affairs, which could take a leading role in negotiating regulations in this area.

Q: The growing energy demands of AI processing are driving major companies – Microsoft, Google, Amazon, Meta – to invest in nuclear energy, including small modular reactors (SMRs) in Africa. Given the security challenges on the continent, how might this trend affect proliferation risks?

A: From a technical standpoint, there are no inherent objections to SMRs, provided they are proven to be safe and have undergone operational testing. One distinguishing feature of many SMR designs, compared to conventional large light water reactors, is their use of uranium enriched up to 20% higher than the typical 3–5% enrichment in standard reactors, but still well below weapons-grade levels.

Most countries interested in SMRs lack the infrastructure to further enrich uranium or extract it for weapons use. Therefore, if SMRs are deployed under IAEA safeguards, designed with safety in mind, and operated by adequately trained personnel, no significant proliferation risks are anticipated.

Many so-called newcomer states without existing nuclear power infrastructure are expressing interest in SMRs due to their lower costs and smaller scale. In such cases, foreign personnel may be involved in operational support, as seen with the UAE's nuclear program. The location of SMR deployment is less critical than the technology itself, the regulatory oversight provided by the IAEA, and the quality of training for operating staff.

Q: This may be a naïve question, but do you foresee a problem of standardization regarding the various AI tools being developed for the peaceful use of nuclear technology—such as running a power plant? Is this an issue that the IAEA guidelines might address or help regulate? Or could this become a problem in the future?

A: Yes, standardization of technologies used in nuclear applications, including AI tools, is indeed an important issue. The IAEA would be an appropriate platform to facilitate discussions on this matter. Such standardization would require close collaboration between nuclear experts, facility operators, and AI specialists.

Currently, there are relatively few experts worldwide with direct, practical experience in integrating AI at nuclear facilities. Therefore, cross-disciplinary collaboration would be valuable not only to share the benefits of AI integration but also to understand and address associated risks. Standardization efforts should aim to consolidate this emerging experience, though perhaps not too hastily, as the technology is still in the early stages of deployment.

While continuous updates to standards may not be immediately necessary, the issue should remain on the agenda. As with other areas of the nuclear industry, establishing consistent frameworks and guidelines for AI applications will be increasingly important over time.

Q: What are the factors contributing to the persistent negative perception of nuclear energy, beyond fears of nuclear accidents and detonation? In particular, what role does the economic dimension, such as the high upfront cost, play in the hesitation of developing countries to adopt nuclear energy as a viable source for power generation?

A: One significant factor contributing to the negative perception of nuclear energy is the disproportionate economic response to radiological events, even when actual risk is minimal. For example, in a previous role at the Waste Isolation Pilot Plant – a geological

repository for transuranic waste – a drum sent from Los Alamos National Laboratory experienced a deflagration event. While this event triggered an alarm, the safety systems performed exactly as designed, limiting the release to about 1% of what the license permitted. Technically, the release was well within safe regulatory limits.

However, the fear it provoked led to political and financial overreaction. The US Department of Energy spent approximately $2 billion to bring the facility to a state where it emitted nothing, despite it already complying with its license. This illustrates the political difficulty in managing even safe nuclear operations when public fear overrides scientific assessments.

Public narratives often frame nuclear energy in emotionally charged terms. For instance, harmless elements like water can be portrayed as lethal by emphasizing their potential to drown or serve as a medium for bacteria, despite being essential to life. Similarly, nuclear energy opponents frequently conflate technical information with moral arguments, suggesting that opposition to nuclear energy is synonymous with being a responsible or ethical person. Once this belief is embedded in personal identity, it becomes difficult to dislodge through facts alone, as contradictory information is often dismissed as biased or unreliable.

These intertwined economic and psychological dynamics play a major role in undermining rational discussions about nuclear energy, particularly in developing countries where resource constraints heighten sensitivity to public fear, perceived risk, and high startup costs.

Q: This is by far one of the best sets of speakers on the peaceful uses of nuclear energy and its nexus with emerging technologies. The question concerns SMRs. While being a strong proponent of SMRs, it remains difficult to convince the public about their safety and security particularly due to their smaller scale. In this context, could emerging technologies such as AI be used positively to address some

of the technical hurdles that delay SMR deployment? Specifically, can AI help speed up the approval of SMR designs or assist in testing them?

A1: AI can be valuable when trained effectively. AI essentially mimics human decision-making, but its reliability entirely depends on the quality and scope of the training data. Just as a well-trained human expert makes better decisions than a random individual, an AI system trained on robust and relevant data performs more effectively.

However, AI can only make decisions based on the data it has been trained on. For instance, testing materials for SMR safety – such as Tri-structural isotropic (TRISO) fuel pebbles or molten salt – requires actual experimental data under relevant conditions. AI cannot substitute for this physical testing. To train AI to predict outcomes with sufficient accuracy to satisfy regulatory bodies such as the US Nuclear Regulatory Commission (NRC), high-quality empirical data is essential.

Therefore, while AI can help guide decisions, streamline development, and optimize testing strategies, it cannot replace the rigorous physical testing required for licensing and safety validation. At best, AI serves as a decision-support tool once comprehensive testing data exists. Without such data, reliance on AI alone would not meet current nuclear safety quality assurance (QA) standards.

A2: Currently, around 80 SMR designs are under consideration globally, but only two or three are being actively developed. No SMR has yet been commissioned. A major challenge is the "First of a Kind" (FOAK) issue – these initial units are expected to cost approximately $1 billion, despite their smaller size. Moreover, they still require the same rigorous environmental assessments, licensing processes, and safety protocols as large-scale reactors.

Another critical concern relates to the use of High-Assay Low-Enriched Uranium (HALEU), which contains up to 19.95% uranium-235 – just

below the threshold for Highly Enriched Uranium (HEU). From both enrichment and verification perspectives, this raises new proliferation and security concerns.

Although there is significant interest in SMRs from technology firms (e.g., Amazon, Google, Meta) and the shipping industry, key questions remain unanswered – particularly regarding the sourcing of nuclear fuel, licensing, safety, and security measures. While the potential of SMRs should not be dismissed, their commercial viability, cost-effectiveness, and nonproliferation compliance must be critically assessed. Further research on SMRs is crucial, and it is encouraging that numerous institutions are engaged in advancing this discourse.

Q: My question concerns the capacity of the IAEA in applying AI to nuclear safety, security, and verification. While the IAEA is renowned for its professional competence across many areas, AI is a relatively new domain. How equipped is the IAEA to address this emerging technological challenge?

A: That is a highly relevant and timely question. The IAEA is currently facing significant personnel and resource constraints across its three core areas: verification, safety, and security. Presently, the Agency includes experts in AI and ML who have limited or no nuclear-specific expertise, and conversely, nuclear experts with limited understanding of AI/ML. This mismatch in expertise is one reason why a performance-based, risk-informed regulatory framework has been proposed – to bring together the IAEA, industry stakeholders, and technology holders to jointly develop common protocols for AI deployment in nuclear domains.

As you may be aware, the IAEA's Planning and Budget Committee is currently in session, and there are proposed budgetary lines for AI-related initiatives. However, these proposals have met with significant resistance from some Member States, particularly from the Global South, due to concerns regarding the use of AI-generated data for nuclear verification and nonproliferation purposes.

There remains a pressing need for increased engagement among Member States, the nuclear industry, and the IAEA Secretariat to develop robust and inclusive regulatory frameworks and governance protocols. This is a long-term challenge, and greater participation from institutions such as the Pakistan Atomic Energy Commission and the national nuclear regulatory authority in IAEA-led research initiatives would be welcome. It is important to ensure that the development and implementation of AI in nuclear applications are not driven solely by experts and interests from the Global North.

Emerging technologies, including AI and ML, offer immense potential to enhance the efficiency, safety, and security of peaceful nuclear applications. These tools are pivotal across sectors from power generation and healthcare to agriculture and environmental protection. However, for these technologies to be fully operationalized, countries must establish comprehensive regulatory frameworks tailored to their specific needs and contexts.

Special Session: A Conversation with General Zubair Mahmood Hayat

Moderator: Dr Bilal Zubair

Director Research, CISS

The moderator introduced Gen. Zubair Mehmood Hayat and invited him to frame the discussion on emerging challenges to nuclear deterrence in the India-Pakistan dyad, an environment marked by unresolved territorial disputes and persistent hostilities in the absence of conflict resolution. He requested that the speaker first outline the broader context and trends, then assess regional security and nuclear trajectories, and finally narrow the focus to bilateral dynamics between the two states.

General Zubair Mahmood Hayat, Former CJCSC

Nuclear issues cannot be confined to a single domain or region. Any assessment of the Pakistan–India dyad must be situated within the wider global nuclear environment. What broader global trends are shaping this environment?

The trend is unfortunately that there is an acceptability for use of force. Over the last five years, we have seen an increasing resort to the use of force. and I can give many examples if I wish to. There was an aversion to applying force, and that aversion is eroding; states are finding it an instrument of choice that they want to use to achieve an effect. Secondly, there is another troubling trend – the growing normalization of killing. We have witnessed genocide live on our televisions. It is shocking - who could have imagined sitting at home and seeing reports of 18,000 children killed in Gaza? This reflects a normalization of killing, as if such things can simply happen, whether in Gaza, in Kashmir, or elsewhere. This is a trend I have observed with deep concern. Secondly, we had thought, or we had been told, that there is a rules-based order; there are international laws. May I dare say that, over the last couple of years, the rules-based order and international law have evaporated; they no longer exist. Therefore, there is a growing realization that international treaties, which were so sacrosanct to us and which we thought were the gold standard, are not even the dust

standard. They can be put in any dust basket; any morning, anybody can get up and put an international treaty in a dust basket and move forward. Therefore, we have seen a gradual erosion or death of institutions like the WTO, the UN etc. This is all happening because I believe everybody wants to become great.

Greater Russia, Greater America, Greater Israel, Akhand Bharat - there is only one world, and if everybody wants to become "great," there are going to be problems. The global "pie" is only so large, and demographically, for example, far more people live in Asia than in other parts of the world. This trend toward greatness is important to examine because it is impacting South Asia. There is a shifting balance of power, and history, spanning eight to six thousand years of recorded experience, shows that whenever the balance of power shifts, great dangers arise. We are very much in that zone now. As the balance shifts, nations' political intentions are also shifting and changing, and that is a major warning sign.

When I see certain European nations changing their political intent, that is not a small development; it is significant. Because political intent is changing, the strategic postures of these countries or regions are also changing. Whatever strategic posture they held for X number of years is now no longer valid. Owing to this shift in political intent, they are beginning to realize that they need a different strategic posture and you can clearly see the signs.

Although I believe the comprehensive settlement of that posture has not occurred, the movement toward it and its general direction are very clear for anyone to see. Similarly, because of this changing strategic posture, alliances and partnerships are shifting. So, old alliances and partnerships that once seemed unbreakable have suddenly weakened. There are no "special relationships" as sometimes claimed. A significant shift in alliances is currently happening.

In the broader military domain, I can see clear signals; an across-the-board increase in defense expenditures. In Europe, people were not

prepared to spend even 2% of their GDP on defense; today, countries are spending 7%, and many others are moving beyond 2% toward 2.5%, 3%, and even 3.5%. This is unbelievable, and it is happening at a time when their economies are suffering but it reflects their own assessments of threats. This is important to understand because when we discuss India and Pakistan, it is essential to keep this context in mind.

Then force sizes are increasing. Notice the number of forces that are growing and people are starting to recruit. Observe the recruitment efforts by Russia; consider the recruitment debate in the United Kingdom; examine the discussions on increasing the military in Germany; and look at Japan's remilitarization. When Japan militarized, we saw what it meant for the world and for the "Indo-Pacific," as we now call it. Although I understand there was no term "Indo-Pacific" before 15 or 18 years ago, it is a phrase we created. If there can be an Indo-Pacific, why not an Indo-Atlantic? But that is a separate debate; let's set it aside.

So, force sizes are increasing, and in the nuclear domain, there is a heightened focus on nuclear forces – the strategic forces of states – whether through modernization, expansion, or other measures; that trend remains very much ongoing. All this is supported by a substantial military logistics buildup. In the First Gulf War, the US had a theater command for logistics; General Paganis, I believe, was in charge. He wrote a book called Moving Mountains. You understand that wars are not fought without those mountains, so when you see logistical "mountains" being shifted or expanded, I, as a humble military professional, recognize that serious issues are at stake for which those mountains are being moved. I hope I have provided some useful context.

Dr. Bilal Zubair

Building on your broader context, how are these trends manifesting in bilateral dynamics, particularly in South Asia, and where relevant, elsewhere?

General Zubair Mahmood Hayat

Before I turn to bilaterals, not only India–Pakistan but bilaterals in a broader context, let me first outline the global context and operating environment, because it is directly applicable to South Asia.

There is a clear erosion of arms control regimes. If I had spoken at this table ten years ago, my remarks on disarmament would likely have been very different. Today, however, it is evident that arms control and disarmament frameworks are weakening, even in the conventional domain. States are withdrawing from treaties governing issues such as landmines, and in the INF domain we have witnessed outright collapse, while START and related instruments are under increasing strain. Once such trends occur, strategic stability becomes fragile, it is under stress, and these are clear signs. This is not being driven by one nation; it is a domino effect: one country does one thing, another feels it must respond, and then a third reacts to the first two. Military history teaches, even in chapter one, how such cyclical reactions begin. Once they start to unfold in the strategic domain, and you begin to unravel the entire architecture of arms control and disarmament, you are effectively unhinging yourself from the constraints, parameters, and laws that have governed this capability.

Secondly, it's not only the arms control of legacy systems; it's also the multi-domain deterrence that has now emerged, something that did not exist before. This adds to the challenge because you have a legacy challenge that is both existing and existential, and yet you also have a new challenge: multi-domain deterrence, whether in AI, space, or cyber, among others.

Then, to me, there's a risk of proliferation in new regions. We already know there has been a strong focus on Iran, which has been ongoing for quite some time. In fact, every few years, it becomes a top priority; then it quiets down, only to resurface years later. But Iran isn't the only concern. North Korea has also been on the agenda for quite some time. Someone refers to it as the "little rocket man," but that "rocket man" has nuisance value, can create an impact, and has a card to play. I also believe this blurry friction risks are now more widespread. This isn't just about Iran and North Korea—there's some smoke in the Middle East, Southeast Asia, and even Europe.

So, this risk of proliferation in new regions is affecting the environment globally. In the multi-domain spectrum, there is also the weaponization of space. People deny that space has been weaponized; you can fool some people for a while, but not everyone all the time. Anyone with even basic knowledge of the topic will tell you that space has already been weaponized. Additionally, there are space commands—how can you have a space command if it isn't weaponized? Anti-satellite tests have been conducted not only by one nation but by many, including the country to our east. If that isn't the weaponization of space, then what is?

Then there is an emergence of AI and it has been already discussed in the context of global environment, and how it impacts the command-and-control (C2) sector of the nuclear domain. This is uncharted territory that we are all going through, and it is something to be reckoned with. We are not talking about nation-state control or organizational control over nuclear weapons; we are talking about human control over nuclear weapons coming into question. That is a far bigger debate and a far bigger question.

And, obviously, in the global environment, I see modernization of nuclear arsenals. Among the nine nuclear states, one will publish articles about another, "the other state is doing this, this, this, and this," while keeping a curtain over its own actions; and we know what they

are doing, everybody does. Modernization is occurring across the spectrum - weapon systems, warheads, and delivery systems- and it is clearly impacting the global strategic environment.

Before turning to the bilateral level, it's essential to consider the international context that shapes the strategic domain. Now, at the regional level, the most salient debate is Europe's "nuclear backstop": will Europe develop an independent nuclear umbrella outside the United States' cover? If so, what shape and form would it take, what strategic dimensions would it entail, and what posture would it adopt? The answers will be consequential, as such a move would amount to a significant breakout.

It is a sort of breakthrough because we believed there was an overarching safety net covering almost everything, and suddenly, there's a spirited debate. The new German chancellor says: I don't have to say it on live TV, but I must mention we should consider our own nuclear weapons system or an arrangement. Suddenly, talks are happening between France and Germany, and between France and the UK. Secondly, moving beyond Europe's nuclear backstop debate, there is AUKUS and the spread of nuclear propulsion in the Indo-Pacific. This cannot be dismissed with a small press release claiming it doesn't matter. It signifies a lot; it shifts the power balance in a specific region and gives certain countries advantages over others. How could it mean nothing? I don't want to take a sleeping pill, go to bed, and wake up to find the entire power structure of a region has changed because someone now has a nuclear propulsion mechanism at their disposal.

The third point I raised is the threshold or breakout states. I won't assign a specific number to it, but there are states on the brink and states ready to break out. It's like a 100-meter race: before the start, all the athletes are warming up, and it only takes one whistle to bring them to the line. This is exactly where we are in the strategic domain.

The world should stop focusing solely on the nine existing nuclear powers, as they are a fact, and start looking beyond what is coming. It's

a tsunami that will arrive, and once the alarm is sounded, there will be no stopping; no one will prevent it. We have seen the volatility in the Middle East and the Iran–Israel standoff; we know what it can imply, what it can do, and what it can unleash. I only hope this Pandora's box remains closed. This is a Pandora's box: once it opens, no one can shut it. Then, there is Russia's "tactical" nuclear posturing, along with "tactical" nuclear enhancements and deployments by other countries. For a long time, I was told I possessed "tactical" nuclear weapons, although I always said I don't have "tactical" nuclear weapons; I have short-range, low-yield nuclear weapons. But since you call your nuclear weapons, especially those with lower yields, "tactical," I will use that terminology for your benefit. I am uncomfortable with it; there is nothing tactical about a nuclear weapon. I strongly disagree with anyone who claims this. This so-called tactical nuclear posturing requires serious scrutiny.

Finally, in the regional sphere, extended deterrence remains a key issue. If nuclear weapons are deployed forward, such as Russia in Belarus and the US already having nuclear weapons in five allied countries, that is a current reality. Will these deployments grow? I don't know. If they do, where will they spread? What security guarantees will the Baltic states have? What assurances will frontline Eastern countries like Poland and others get? These are real and open questions.

Dr Bilal Zubair

You are talking about the proliferation and erosion of norms and agreements. This erosion of norms and the proliferation of threats are concerning. There is exceptional treatment of certain states vis-à-vis others, particularly in bilateral arrangements. This is indeed an alarming development. How do you see that, Sir?

General Zubair Mahmood Hayat

Bilal, you make a very relevant point. I am not here to play the victim; I will state the facts as they are, not the ones I read in mainstream newspapers or those written by people pursuing their own agendas. I need to be very honest about the facts as I see them. If I wear a shoe, only I know where it pinches; nobody else can tell me where my shoe pinches.

So, if I see a threat that is existential, real, and capability-based—one I must prepare for—then I need to be clear and upfront about it. And if there is exceptionalism, double standards, or duplicity, then please don't ask me to turn a blind eye. No nation can do that, and I certainly won't.

Now, let me discuss the broader aspect of nuclear dynamics. Bilaterally, the U.S.–Russia strategic rivalry has persisted for roughly the last 75 years. We are aware of the amounts of fissile material each side possesses. We know the levels of their nuclear arsenals. Additionally, various treaties have reduced those arsenals to much lower numbers—around 5,500 weapons. All this information is well known.

However, this strategic rivalry has not ended; it persists today in various forms. What is new is the increasing strategic cooperation between Russia and China, especially in the area of BMD. This information is now publicly available. I am not sharing any top-secret briefing or classified data.

I will only share information available in the public domain. When this kind of strategic cooperation occurs, it has important strategic implications and effects. At the same time, there is a gap in U.S.–China nuclear dialogue and crisis management. I'm not trying to blame either side; I am simply presenting the facts.

Now, there is also the issue of India–China escalation in the bilateral sphere. India aims to align itself with broader strategic partnerships, and I plan to explore India's role in more detail with you as we proceed. It's important to highlight that this escalation between India and China is not limited to the traditional military domain – it goes beyond that. To be clear, it is driven by India and influenced by India; China is not the one initiating this dynamic.

Then, of course, we have the India–Pakistan dimension, which we will discuss later. As the events of yesterday demonstrated, this subject is never truly off the table. Sometimes it recedes into the background, but it always comes back to the forefront. So, these represent the bilateral aspects.

Dr Bilal Zubair

Regarding strategic stability in South Asia, we often see the West call for greater restraint from both states. Additionally, how do you view a destabilizing factor in the India-Pakistan strategic dynamic, where India attempts to establish a new normal? Furthermore, I would like you to emphasize how the exceptional treatment given by the West is undermining strategic stability. On one hand, they call for stability, but on the other hand, their actions are directly contributing to instability in the region.

General Zubair Mahmood Hayat

You mentioned that people have been calling upon both India and Pakistan to exercise restraint. I would genuinely like to see a clear statement from someone specifically calling upon India to exercise restraint. If such a statement exists, please share it with me – who made it, and when it was made. In recent times, I have not encountered anything that substantiates that claim. What I do see is a one-sided pressure, and such pressure will never work. Nonetheless, it is evident that the pressure being applied is overwhelmingly one-sided.

Now, I will discuss the three aspects of India's strategic behavior: ideological, political, and technological. All three are risky and destabilizing. Let me explain why this is a key point from our discussion today.

First, India has the largest and fastest-growing nuclear program in the world. Independent studies, not only those conducted in Pakistan but also from around the globe, have confirmed this reality. I am confident that some honorable participants here, if they wish, can share those studies to further illustrate this point.

Have you heard any serious discussion about this? There is complete silence. We have a country that has been the top importer of conventional arms in the world for ten straight years, and at the same time, the same country is developing the fastest-growing nuclear program. These are two undeniable facts. I know some colleagues from SIPRI are here who can confirm these figures. The question is: what is the purpose of such a huge weapons import? Certainly not for celebrations like Diwali.

This unchecked drive – the urge to flex muscles and expand the chest from 36 inches to 54 inches – is being seen as strategic strength. But, instead of building strength through various forms of power, including soft power, India is trying to show its might only through the buildup of arms and nuclear weapon systems.

What makes this situation even more alarming is that India is the only country where such advanced nuclear weapon systems are effectively in the hands of an extremist political group. This reality represents not only a regional danger but a global concern.

You see, the Bharatiya Janata Party (BJP) is essentially the public face of the Rashtriya Swayamsevak Sangh (RSS) – its political representation. It also serves as the political front for groups like the Bajrang Dal. To put it differently, think of the Irish Republican Army

(IRA): the IRA was the militant wing, and Sinn Féin was the political branch. Similarly, the RSS functions as the ideological and militant core, with the BJP acting as its political wing. However, no one wants to discuss this openly because India is a large country, and due to the broader strategic goal of containing China, India must, in one way or another, be appeased at all costs. Let's not shy away from recognizing these double standards.

If this were only a matter of the Hindutva regime and the RSS, one might have thought it was a passing phenomenon. But the reach of the RSS has now deeply penetrated India's institutions, including its military and strategic community. Today, it is increasingly difficult to become a senior officer in the Indian military without conforming to the RSS philosophy. In fact, someone can even be called out of retirement and appointed Chief of Defence Staff precisely because of an ingrained RSS ideological alignment.

To illustrate this change, consider the Indian Army Chief's office. For a long time, it displayed a photo from the 1971 war – a symbol of what was once seen as India's greatest achievement. That photo has now been removed. In its place, a new painting featuring an ideological and religious theme, Dharma, has been put up. This is not a small change; it signals a broader shift in priorities and identity.

These facts are public knowledge. Anyone can verify them. Use Google, open-source platforms, or AI tools like ChatGPT or DeepSeek; they'll provide whatever data is available for you to explore. They're not human with personal judgments; they deliver information based on what they have access to.

This Hinduization and saffronization of the Indian military is a fact. Next, consider the scope of India's missile and weapons systems. Indian missile systems now extend well beyond South Asia or Southern Asia, if you prefer that term. They go beyond China. Today, Indian missile systems can reach Europe, and their advanced missiles

will soon be able to reach the mainland United States. That is the reality.

India's nuclear capability has extended far beyond South Asia. It doesn't directly concern me much, as my needs are limited. Their K-15 missile was sufficient for our situation; the K-4 and other systems, like the Surya and the Agni series, are not intended for Pakistan. Europe faces threats, and so does the United States.

Now, let us discuss India's doctrinal shift. Whether officially acknowledged at the top level or not, it has not been disowned either, and for me, that suffices. These are serious matters. If a state does not disavow such shifts, it implicitly endorses them. Those shaping these policies are not ordinary people sitting in a bazaar having tea; they are serious-minded individuals who know exactly what they are doing. This is why India's refusal to clearly reaffirm its 'No First Use' policy must be noted. By keeping its position ambiguous and vague, India is deliberately maintaining strategic uncertainty.

Throughout all of this, I observe that the West is either complacent or complicit. I can't definitively say which – and I prefer not to speculate – but the result is the same. This frames the overall context of what is happening globally, regionally, and bilaterally. However, it also underscores the importance of focusing on India and clearly acknowledging what India is doing. I have now brought that point into focus.

Dr Bilal Zubair

This is indeed a fascinating account of how you've explained this triangular issue involving India, centered around ideology, politics, and increasing military spending. As you've correctly noted, this is highly destabilizing for the region. Looking ahead, what do you see for the India–Pakistan relationship? In the absence of meaningful conflict

resolution, do you believe this situation will continue into the foreseeable future?

General Zubair Mahmood Hayat

You see, the very nature and character of the Indian state have changed. India is no longer the India it once was—It is now Bharat. And I am not merely speaking figuratively. When you see the Indian Prime Minister seated at international conferences, look at the nameplate in front of him: it no longer says 'India,' it says 'Bharat.'

For those interested in a deeper study, this is connected to the ideological triangle I mentioned earlier. India is shifting from a secular, liberal democracy to a Hindu Rashtra. We saw this ideology come to the forefront in Gujarat during the Muslim massacre—an event that resulted in Mr. Modi being barred from entering the United States. Not for just a year, but for ten years he was prohibited from stepping on U.S. soil. He was banned because of his role in that tragedy. However, just fourteen days after his election victory, the ban was quietly lifted in preparation for his visit.

Now, there's the spectacle of 'Howdy Modi.' The same man who was once banned is now celebrated. We have seen Howdy Modi 1.0, and we have seen Howdy Modi 2.0. My question to you is: will there be a Howdy Modi 3.0? Or will we instead see an 'Amit Shah 1.0' or a 'Yogi 1.0'? And what would that mean for the trajectory of the triangle I spoke about – the ideological, political, and technological dimensions of India's transformation? I believe that sets the context and answers your question.

Question Answer Session

Q: Considering the role of religious beliefs in shaping geopolitics, particularly as we see in the East with Hindu religious ideology and conflict, how do you view the situation in the Middle East? Specifically, in light of the U.S. withdrawal from the JCPOA in 2018, the relocation of the U.S. Embassy to Jerusalem with Evangelical involvement, the ongoing war in Gaza, and U.S. threats to Iran – to either negotiate or face bombing – how might the 'end of times' beliefs in Christianity, Judaism, and Islam influence the trajectory of the Middle East over the next five years?

A: Principally speaking, my own personality and my own study have taught me to keep religion out of nuclear weapons systems. In 1983, when this term was introduced for Pakistan, the BBC created a documentary called *'The Islamic Bomb.'* That was the point at which religion was introduced into the discourse – the so-called 'Islamic bomb.' I mean, you don't have a Christian bomb, you don't have a Jewish bomb, but you have an 'Islamic bomb.' This is the most dangerous thing one can do: to introduce religion into the nuclear domain. If anybody is doing it by design, they are doing no favor to humanity. And if anybody is doing it out of madness – well, there is no cure for madness.

Q: Last night, I came across a tweet by Shashank Joshi the Defense Editor of *The Economist*, in which he suggested that it is likely that we will see an Indian military strike against Pakistan in the coming weeks – probably as retaliation for the recent attack in Kashmir. Given that I am not very familiar with the Pakistan–India conflict, what is your perspective on this possibility?

A: I knew when I was coming here today there would be a question, and I thank you for making me think that I am still on the right lines. You see, I am amazed: when India comes and kills 22 persons on Pakistani soil, mainly in Punjab, I have not heard of Pakistan striking

back. When India kills a Canadian on Canadian soil, I have only seen it played out in the political domain; I have not seen Canada try to strike back. When India is alleged to have killed an American on American soil and the Washington Post has reported on it, I have not seen corresponding action. When I see India implicated in the deaths of two UK citizens or others on UK soil, nothing substantial follows.

Day in and day out, Pakistan is attacked. More recently we had the Jaffer Express incident: 400 people were hijacked on a train – the largest train hijacking in world history – and there was not a word on who had done it. It was carried out by proxies that are supported by India. This is the writing on the wall. In the last 25 years there have been over 89 incidents in Balochistan and KPK in which more than 20 people have been killed. People have been taken off buses, identified, and killed. This is mainland Pakistan not a disputed territory. Kashmir is a disputed territory; it is illegally occupied by India, and when Kashmiris struggle for their freedom and strike at India, somehow Pakistan is blamed and there is talk of a strike on Pakistan. This logic is absurd. If somebody still believes they can strike Pakistan, they should take a lesson from what happened after the attack on Balakot. And this time it will not be restricted to a Balakot-type response alone.

Q: My question is more of an academic nature regarding the future of strategic stability. Traditionally, strategic stability has meant the absence of incentives for adversaries to launch a first strike or attack. However, in today's era, with emerging technologies evolving, warfare becoming opaquer, and non-state actors increasingly capable of triggering crises as we witnessed recently, do you believe the traditional notion of strategic stability still holds? Or does it need to be redefined in this changing environment?

A: You see, strategic stability exists when there is a Balance of power. The first point I made during my discourse was that this balance of power is shifting. The inherent implication of this shift is that strategic stability will be diluted and will come under stress.

Q: Yesterday we discussed robots and the development of automated systems, and how they might contribute to nuclear deterrence. In the context of Pakistan and its regional environment, particularly in relation to India, how do you see the role of such technologies in the future? Do you believe robots and automated systems could play a stabilizing or destabilizing role, and is there any possibility of initiating consultations with your neighbors on this issue?

A: You see, once a technology is out there, it can never be put back into the genie's bottle. That is the lesson of history. So, if someone says that artificial intelligence is out there and we can contest it, put it back, or simply choose not to deal with it - no, that is not going to happen. This is now a reality, and it is here to stay.

What we are going to do with it is a much bigger debate than just us. As I mentioned, there are already nine nuclear states, as well as threshold states and breakout states. So, make your count – this is a broader, global debate. And if you feel that under the current great power competition someone is going to seriously address this issue, I will not fool myself on that account. That is not going to happen. Nobody is going to sit at the table and create a win-win situation for everyone. Power is being contested; states want domination and control. Ethics is not involved here.

What you are asking is more ethical in nature. If you want me to discuss theory and I see there are students from universities here, I can give you a theoretical answer in which I could argue, yes, it should happen that way. But I have been a practitioner, not just a theorist, and I understand what these things mean in reality.

So, yes in a utopian world, perhaps it should happen. But in the near future and when I say near, I mean 5, 10, even 15 years – I do not see a real chance of major movement in this direction. Only once the balance of power has shifted, one way or another, will such secondary debates come into play.

Session IV

Impact of Quantum, Cyber Technologies and Autonomous Weapon Systems on Deterrence

Moderator: Ms Anum A. Khan
Associate Director, CISS, Islamabad

Impact of Quantum Technologies on Nuclear Deterrence

Mr Vladislav Chernavskikh
Research Assistant, SIPRI Weapons of Mass Destruction Programme, Sweden

Quantum and artificial intelligence (AI) technologies, though fundamentally different in their operational mechanisms, share similarities in their potential military applications and their implications for strategic environments – particularly those involving nuclear decision-making. Both are considered potential force multipliers, with the capacity to significantly enhance existing strategic capabilities, particularly in domains such as data collection, processing, intelligence, surveillance, reconnaissance, targeting, and secure communications.

Consequently, both technologies are expected to influence strategic stability and deterrence practices by altering the capabilities upon which nuclear strategies rely. Furthermore, AI and quantum technologies are central to a new generation of arms competition, not just in terms of weapon platforms but also in the race for computing power, algorithmic superiority, and data dominance.

In terms of technological maturity, AI is currently far more advanced. Quantum technology remains nascent, with most of its proposed transformative applications still theoretical or in early experimental stages. Building practical quantum devices remains extremely complex, and timelines for operational deployment remain uncertain.

In contrast, AI has already demonstrated significant advances and is being actively integrated into multiple military and strategic systems. Looking ahead, quantum technology is expected to amplify the existing effects of AI, acting as a key enabler for military AI applications. In this context, AI represents the more mature and active element, while quantum technology is poised to support and enhance it over the long term.

AI has demonstrated notable progress in recent years, particularly in functions relevant to military and nuclear deterrence, such as:

- Signal recognition (acoustic and electromagnetic signatures);
- Object detection and classification in images and videos;
- Data management and analysis.

These capabilities are integral to NC3 systems, and AI is increasingly viewed as a tool to enhance these systems across the entire deterrence architecture.

Among the emerging application areas of AI in the nuclear domain, one of the most prominent is its integration with space-based systems, particularly in intelligence, surveillance, and reconnaissance (ISR). AI is increasingly used to:

- Analyze satellite imagery;
- Perform geospatial data fusion;
- Enhance real-time monitoring and interpretation.

These advancements are directly relevant to nuclear stability, as they may enhance a state's ability to detect, track, and target adversary nuclear delivery systems, including mobile missile launchers. Investments in this area are substantial:

- The United States has launched several projects aimed at integrating AI across its space-based ISR networks;

- India's space agency has announced plans to deploy AI-enabled surveillance satellites over the next five years to bolster its ISR capabilities.

This domain represents a clear and immediate use case for AI in support of nuclear strategy and deterrence. The growing reliance on these technologies signals a shift in how deterrence is conceived – away from platform-based parity and toward information dominance and computational superiority.

The second key application area is early warning and missile defense. The United States provides perhaps the most prominent example in this regard. Both the U.S. Space Force and the Missile Defense Agency are investing significantly in integrating AI capabilities across missile defense networks, including ground-based launch systems, radars, and space-based sensors. The objective is to develop an AI coordination layer that integrates these systems – sensors, interceptors, and command structures – into a more effective and adaptive missile defense architecture.

Other states are also exploring this domain. For instance, Russia has reportedly incorporated AI into its S-500 air and missile defense system, reflecting a broader trend of applying AI to bolster traditional defense platforms.

A related area is space domain awareness, which has gained urgency with the increasing proliferation of satellite constellations by state and commercial actors. AI is being leveraged for enhanced tracking, coordination, and anomaly detection in space operations, including the identification of potential threats to satellites and early warning systems. Such capabilities are especially relevant given the reliance of NC3 systems on space-based assets.

The third significant application is in cybersecurity—both in offensive and defensive capacities. AI is naturally suited for this domain and is already being used to strengthen cyber operations, including penetration testing, anomaly detection, and real-time response modeling. States are actively red teaming AI-enhanced cyber strategies to test vulnerabilities in nuclear-related digital infrastructure.

In the naval domain, AI is being applied to undersea surveillance, particularly in tracking nuclear-powered submarines, which are crucial elements of second-strike capabilities. For example, under the AUKUS agreement, Australia, the United Kingdom, and the United States are examining how AI can enhance acoustic signal analysis and sonar data processing to improve the speed and accuracy of submarine detection. Several other states are pursuing similar applications.

Another domain of concern is the integration of AI in conventional weapons systems with potential strategic consequences. A recent example includes Ukrainian drone attacks on Russian strategic bomber bases, which demonstrate how AI-enabled precision strike systems can target adversaries' nuclear-associated infrastructure—even by non-nuclear weapon states. In response, Russia's revised nuclear doctrine now includes attacks by drones as possible triggers for nuclear use, indicating how AI integration into conventional weapons can affect nuclear posture.

Further, there are cases where AI is being directly incorporated into nuclear weapons delivery platforms. The Russian Poseidon, a nuclear-armed autonomous underwater vehicle (AUV), is reportedly under development with reliance on advanced AI systems. In the United States, the B-21 Raider strategic bomber is designed for both crewed and uncrewed operations, capable of coordinating missions with other platforms, including unmanned drones.

Despite widespread agreement among states that human decision-making must remain central—the so-called "human-in-the-loop" requirement—there is nevertheless growing integration of AI into

nuclear delivery systems, raising concerns about inadvertent escalation or unintended delegation of authority.

In summary, these applications introduce strategic risks by accelerating arms races and undermining crisis stability. As nuclear-armed states perceive their nuclear assets as increasingly vulnerable—especially to AI-enhanced conventional systems—they may adopt more aggressive or preemptive postures, as illustrated by Russia's doctrinal changes.

In the nuclear field, one of the most significant limitations of AI remains the absence of quality data and the highly contested, ambiguous operational environment. These constraints reduce AI's effectiveness and increase the likelihood of technical failures or misuse.

Turning to quantum technologies, experts typically group their applications into three core categories:

1. **Quantum Computing** – Aimed at solving complex problems that are intractable for classical computers, including optimization and cryptographic challenges.

2. **Quantum Communications** – Offering theoretically unbreakable encryption through quantum key distribution.

3. **Quantum Sensing and Imaging** – Enhancing detection of weak signals or objects with extreme precision, which could be used for submarine detection or nuclear material tracking.

Each of these categories harnesses distinct quantum properties to overcome limitations in classical computing, communications, and sensing. When combined with AI, quantum technologies have the potential to significantly enhance military and nuclear capabilities, thereby compounding existing strategic risks.

To elaborate further, quantum computing fundamentally differs from classical computing by relying on *quantum bits (qubits)* instead of binary bits. This allows quantum systems to process information in non-linear and probabilistic ways, vastly increasing computational speed and processing power. One of the most significant implications of quantum computing is its ability to accelerate AI model training and real-time data processing, especially in high-stakes military contexts.

By enhancing speed, reliability, and scalability of machine learning, quantum computing could significantly reduce the time required for AI algorithms to learn from complex datasets—such as those generated through ISR operations. This can, in turn, improve identification, decision support, and targeting capabilities that rely on large-scale data fusion.

However, quantum computing also introduces new security threats. It has the theoretical potential to break many classical encryption schemes, which could compromise sensitive communication networks, including those critical to nuclear command and control systems. This risk places additional pressure on states to adapt their cybersecurity infrastructure in anticipation of a post-quantum world.

Moving to quantum communications, this domain leverages quantum properties to establish highly secure data transmission channels, often via quantum key distribution (QKD). These channels are resistant to eavesdropping and inherently secure due to quantum mechanical principles. Such technologies are applicable to both terrestrial networks and satellite-based communications, making them particularly relevant for command and control systems in military and nuclear domains.

In contested or degraded environments, quantum communication could enhance coordination, resilience, and secure information sharing, protecting critical nuclear decision-making infrastructure from cyber intrusion. When combined with AI-enabled cybersecurity

systems, the integration of quantum communication may result in a multi-layered defense against cyber threats targeting nuclear assets.

Finally, quantum sensing and imaging utilize quantum phenomena – such as entanglement and superposition – to achieve high-precision measurement and detection capabilities. Quantum sensors can collect faster, richer, and more accurate data than their classical counterparts, which AI systems can analyze for enhanced situational awareness and ISR operations.

In practical terms, this includes the development of quantum navigation systems that are resilient to jamming or spoofing, offering strategic benefits for operating in GPS-denied environments. These systems are particularly valuable in military operations or covert deployments. Additionally, quantum-enhanced radar and imaging techniques can assist in detecting obscured or concealed targets, further improving the efficacy of AI-driven detection and tracking capabilities.

In conclusion, the convergence of AI and quantum technologies poses both opportunities and risks for strategic stability. While these technologies promise unprecedented capabilities in terms of intelligence gathering, targeting, secure communications, and system resilience, they may also destabilize deterrence relationships by undermining existing assumptions about nuclear survivability and second-strike capabilities.

Cyber Threats to NC3 Infrastructure – Implications for Nuclear Deterrence

Dr Jessica West
Senior Researcher, Ploughshare Foundation, Canada

Cyber is the backbone of emerging technologies, serving as the conduit that connects and amplifies risks across domains such as AI, quantum computing, and space systems. The growing complexity and interdependence of digital infrastructure lead to cascading risks, making cyber dependencies critical to stability. Human judgment remains essential to prevention and deterrence, yet the space for human-centered decision-making is shrinking—both technologically and diplomatically.

Cyber refers to the systems and networks through which information is created, stored, transmitted, and manipulated. This digital infrastructure connects technical systems, communications, and the physical world. Virtually all systems today, from satellites and nuclear command-and-control networks to household appliances, are integrated into the cyber domain. While powerful, this interconnectivity introduces significant systemic vulnerabilities.

Historical cases underscore these risks. In the 1990s, backdoors were discovered in critical military software. In the 2010s, the Stuxnet cyberattack caused physical damage to Iran's nuclear infrastructure through a targeted line of code. At least one nuclear-armed state has since experienced communication breaches. Civilian nuclear facilities in India and air-gapped systems in Germany have also been compromised. These examples illustrate that no digital infrastructure is completely secure, including systems used in submarines and other critical platforms.

The current threat landscape is defined by the scale, scope, and speed of cyber vulnerabilities, which allow for cascading failures and fundamentally alter how deterrence and escalation are understood.

Previous conflicts were triggered by physical and visible events – a gunshot, a political assassination, or a missile launch. In contrast, the initial spark today could be silent and digital, such as a dormant line of malicious code or a software malfunction – a "normal accident."

The first strike in a future nuclear conflict may target space-based assets, likely through cyber means. During the war in Ukraine, for instance, a cyberattack disabled the Viasat satellite network by exploiting vulnerabilities in end-user modems, without interfering with satellites in orbit.

NC3 systems function as the nervous system of nuclear arsenals. These systems operate in a persistent fog of uncertainty, and cyber vulnerabilities significantly exacerbate that condition. Interference may include tampered early-warning data, spoofed or severed communications, disinformation, and social manipulation. Differentiating between deliberate attacks and malfunctions becomes increasingly difficult under these conditions.

NC3 infrastructure is closely interwoven with other emerging technologies such as AI, quantum computing, and space systems. While these technologies accelerate data collection and decision-making, they simultaneously increase the likelihood of false alarms, misinterpretation, and inadvertent escalation. While tools like AI and quantum can bolster cybersecurity, they also enable offensive cyber capabilities, reinforcing the dual-use dilemma. This feedback loop fosters strategic instability and complicates crisis management.

The current environment is collapsing the foundational logic of nuclear stability. Deterrence depends on the reliability of strike capabilities—now rendered uncertain by cyber threats. It relies on clear signaling, yet cyber operations obscure intent and attribution. It assumes time for assessment and response, but new technologies increasingly compress decision timelines. It depends on human control, even as systems are designed to bypass or overwhelm human decision-makers.

Two core beliefs underpin deterrence: that systems will function as intended when required, and that they will not be employed without proper authorization. Both assumptions are being undermined. Former commanders of U.S. Strategic Command (STRATCOM) have publicly expressed concerns about the reliability and integrity of nuclear systems. If confidence in these systems erodes, the credibility of deterrence erodes with it.

Addressing these challenges requires revitalizing Cold War-era mechanisms such as hotlines and crisis communication channels—updated for a more complex, multi-stakeholder environment. Beyond state actors, the private sector plays a pivotal role in digital infrastructure, and civil society remains essential for shaping public understanding and fostering accountability.

Strengthening the human layer (the decision-making layer) is imperative. This includes ensuring sufficient time for deliberation, establishing robust communication frameworks, validating information through reliable mechanisms, and reinforcing interpersonal and intergovernmental trust. The ultimate goal is not merely to safeguard systems but to protect people.

Emerging Applications and Impact of Directed Energy Weapons

Dr. Laetitia Cesari
Consultant, UNIDIR

The Directed Energy Weapons (DEWs) technologies have been under development for centuries, gaining particular momentum in the early 20th century through advancements in physics—specifically concerning light, photons, and particles. Key contributions were made by figures such as Max Planck and Albert Einstein, the latter introducing the concept of stimulated emission of radiation in a 1916 paper.

The first functional laser was constructed by researcher Theodore Maiman, who employed ruby—a gemstone—to amplify light, using specific lamps to support the process. The term "laser" stands for Light Amplification by Stimulated Emission of Radiation. Maiman published his findings in *Nature* in August 1960.

This technology, having evolved over decades and involving efforts from scientists around the world, was quickly recognized for its military potential. During the Cold War, both major blocs invested heavily in the research and development of DEWs, particularly lasers and particle beams. These became strategic components of defense programs, largely intended for intercepting ballistic missiles. Numerous experiments and developments were closely linked to broader tensions surrounding nuclear systems.

From the 1990s onward, additional states have increasingly invested in DEW technologies. Today, this field features prominently in initiatives such as missile-defense domes, as well as in discussions around orbital anti-satellite technologies.

While DEWs were originally conceived for military purposes, they now have important civilian applications – including in healthcare, industry, and space communications. These technologies are valued

for their precision. In the medical field, for instance, lasers are commonly preferred over scalpels for eye surgery due to their accuracy. Similarly, they are used in industrial processes, such as surface treatment in manufacturing.

Concentrated light is also being utilized for space-based optical communication. Concepts related to quantum technologies – such as quantum key distribution—can likewise be transmitted via light. As such, the civilian utility of lasers and DEWs continues to expand.

However, the disruptive potential of these technologies remains a key concern. The 2021 United Nations Secretary-General's report '*Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts*' identified three categories of disruptive electromagnetic technologies: (1) directed energy weapons, (2) electronic warfare capabilities, and (3) electromagnetically propelled weapons.

Directed energy weapons serve as a "catch-all" term encompassing a range of technologies. Their levels of maturity vary significantly, depending on national investment in research and development. DEWs may be deployed via ground-, sea-, or air-based systems – and potentially, in the future, from space-based platforms.

Several technical limitations persist, particularly in relation to power supply and energy output. Ground-based systems have a relative advantage in energy availability, enabling them to support laser, particle, or microwave applications more effectively. A core challenge remains the covert deployment of these capabilities. To this end, mobile platforms—such as sea- and air-based systems—have seen greater development. This has also driven research into space-based systems.

DEWs comprise a broad category. A more formal definition is found in a 2022 commentary by Sarah Grand-Clement for UNIDIR, describing DEWs as systems using concentrated electromagnetic energy or charged particles—such as lasers, microwaves, or particle beams—to

disable or destroy targets without the use of physical projectiles. These are also referred to as "non-kinetic" systems. Mastery of the relevant physics is essential for their effective use – something not all states have achieved, particularly when considering long-range targeting, including in airspace or outer space.

The potential effects of DEWs are diverse. Lasers, whether high or low power, are capable of disrupting or destroying equipment, especially electronics. These systems can be particularly effective against optical or radar components, which are sensitive to physical phenomena.

Tactical and Strategic Implications of Directed Energy Weapons

As critical sectors increasingly depend on advanced technologies, disabling the electronic systems that support these technologies can, in some cases, be more effective than targeting structural components. This rationale underpins the strategic deployment of DEWs.

High-power microwave systems, for example, can degrade or damage electronic systems and are particularly effective against uncrewed aerial systems (UAS), such as drones. These systems are often difficult to intercept through conventional means, whereas the use of microwave energy can disable their electronics without physical destruction.

Particle beams represent another category of DEWs. These systems deliver streams of accelerated particles to a target. Although not yet widely deployed, experimental uses and advanced research programs are underway in select states.

Another category, metal waves, functions primarily as anti-personnel and area denial weapons. These waves can produce a burning sensation on the skin. Their use is difficult to detect and verify, as the effects are both immediate and fleeting—disappearing almost instantly after activation. Tracing the origin of the power source presents an additional challenge. While fixed or ground-based systems may be

easier to identify, mobile systems, whether handheld, sea-based, or airborne—are considerably more difficult to detect, thereby enhancing their strategic utility.

In response to these developments, the United Nations has continued its efforts to monitor and assess the implications of emerging technologies. In July 2024, the UN Secretary-General released a report on developments in science and technology and their potential impact on international security and disarmament. Paragraph 63 of this report specifically identified directed energy weapons as disruptive systems with significant strategic implications.

DEW targets are broadly categorized into two environments: air-based and space-based. Air-based targeting is easier to demonstrate. There exists visual and video documentation of experiments conducted by military and defense institutions. Common targets include vehicles, rockets, missiles, and incoming munitions. In the nuclear context, disabling or damaging an incoming missile could neutralize an adversary's offensive capabilities and shift the strategic balance.

Such capabilities carry the potential both to destabilize deterrence and to reinforce it. On one hand, they may trigger arms races or incentivize preemptive behavior due to perceived vulnerabilities. On the other hand, they may strengthen deterrence by improving defense systems and diminishing the perceived utility of a first strike. States are currently navigating this duality – developing and testing DEWs while signaling to adversaries that offensive actions could be effectively countered.

The central strategic question remains: Can the defensive strength of these technologies deter aggression, particularly from missiles or UAS? This remains an open debate and a subject of ongoing diplomatic discussions. Key concerns include the risks of miscalculation, miscommunication, or misperception, and whether such technologies might genuinely reinforce security or inadvertently escalate tensions.

With regard to space-based targets, significantly more energy and precision are required to effectively deliver a directed energy beam. Effective targeting must also account for atmospheric interference and other physical obstacles. A number of conditions must be met for these systems to operate efficiently, and there remains considerable uncertainty as to whether they can be reliably used for counter-space capabilities.

Risks, Legal Ambiguities, and Verification Challenges of Directed Energy Weapons

If operationalized, DEWs would pose significant risks to satellites, which rely on sensitive electronics, optical sensors, radar systems, and other high-precision components. While ongoing research and development is evident, there is no confirmed or publicly available proof of their operational deployment. Nevertheless, if these systems do become operational, they could exacerbate the risks of misperception and elevate tensions in space-related activities.

The inclusion of this issue in the United Nations Secretary-General's reports on science, technology, and international security signals its growing importance to diplomats, the international community, and disarmament-focused organizations. The presence of DEWs in such reports elevates the urgency of addressing them at multilateral forums.

One reason this is critical is the variable nature of DEW effects. Some effects are temporary and reversible, while others are permanent and disruptive. For instance, low-power lasers – part of the broader DEW category – an cause temporary dazzle or disrupt systems without causing lasting damage. Once the system is powered down, these disruptions typically vanish. This introduces challenges for verification and attribution: if the effects are no longer visible once the system is off, how can their use be proven? How does one attribute the disruption to a particular source? These remain unresolved and pressing questions in international security and legal discourse.

Conversely, high-power microwaves, lasers, and particle beams can induce irreversible damage. These can disable or destroy critical components beyond repair, resulting in physical effects akin to conventional kinetic attacks. Once permanent damage has occurred, the incident effectively constitutes an act of force—raising serious questions regarding thresholds for the use of weapons and the implications under international law. Such scenarios raise concerns about escalation, strategic signaling, and rules of engagement.

These dynamics merit sustained discussion both at multilateral platforms and within national policy frameworks. Critical questions arise: Should certain DEW uses be prohibited or restricted? What threshold of damage or intent constitutes aggression? Is the objective to degrade, deter, or permanently disable an adversary's capability? The legal ramifications of these questions are especially relevant for scholars and practitioners of international humanitarian and space law.

It is also important to note that DEWs have operational limitations. These are physical systems that require specific environmental and technical conditions to function optimally. Line-of-sight access is typically necessary, and their performance can be degraded by atmospheric interference, target material resistance, and platform stability.

In parallel, discussions are also emerging around co-orbital DEW capabilities, which refer to weapons deployed from satellites or space-based platforms. Though not yet operational, such systems are of increasing interest. For a detailed analysis of these capabilities, the '*Global Counterspace Capabilities Report*' published by the Secure World Foundation offers a comprehensive review of state-led R&D activities and doctrinal developments.

In conclusion, while directed energy weapons present novel tactical and strategic opportunities, they also pose serious risks related to escalation, attribution, and arms control. The dual-use nature of many of these technologies further complicates international governance,

making it imperative to build legal, technical, and normative frameworks that can manage their use in both terrestrial and space domains.

LAWS: Escalation Dynamics and Global Security

Dr. Riwana Abbasi
Non-Resident Fellow, CISS, Islamabad

Lethal Autonomous Weapons Systems (LAWS) are not confined to a specific category of weaponry. Rather, they broadly encompass any machine capable of performing military tasks independently—without human supervision or intervention. In this context, autonomy refers to a system's ability to execute operational functions without real-time human control.

These systems rely on algorithm-driven capabilities and are being developed to operate across all military domains: land, air, sea, underwater, and outer space. Militaries worldwide are actively pursuing the integration of advanced AI into weapons platforms, alongside doctrinal innovations that reflect the realities of algorithmic warfare.

Evidence from recent and ongoing conflicts in Ukraine, Palestine, and Libya suggests that autonomous functions are already being deployed in real-world combat scenarios. AI-enabled armed drones, in particular, have emerged as transformative tools, reshaping how surveillance, targeting, and strike missions are conducted.

Globally, countries such as China, Israel, Russia, South Korea, Turkey, the United Kingdom, the United States, and increasingly, India, are investing in a diverse array of autonomous weapons technologies. These include swarm drones, unmanned ground vehicles, lethal robotic systems, space-based platforms, satellite-enabled targeting systems, and hypersonic missile delivery mechanisms.

Many of these systems are being engineered for greater speed, agility, and maneuverability. The goal is to deploy lighter, more expendable robotic platforms capable of extended endurance, complex maneuvering, and even suicidal missions in high-risk environments.

Autonomous land and maritime vehicles are also progressing rapidly toward field deployment.

Operationally, LAWS are typically used for missions involving surveillance, reconnaissance, intelligence gathering, and increasingly, direct engagement. These systems follow a dual-task operational framework, transitioning from an "inside-out" to an "outside-in" orientation.

In the inside-out phase, sensors collect real-time environmental data, which is processed through advanced algorithmic fusion. This allows the system to map terrain, classify objects, recognize targets, and interpret battlefield conditions. The AI then uses this input to assess the situation, evaluate potential courses of action, and autonomously select an appropriate response—often, to engage a target.

Although fully autonomous LAWS have not yet been widely fielded, existing systems are trending toward increasing independence. Human oversight remains present for now, often through a human-in-the-loop or human-on-the-loop model. However, these systems are adaptive by design, learning from operational experience and refining their performance autonomously over time.

LAWS are anticipated to outperform human-piloted systems in speed, accuracy, and survivability. Swarming capabilities – where large numbers of small, networked autonomous units operate in coordination—are a key area of development. These systems can communicate, make joint decisions, and execute synchronized offensive and defensive actions.

By operating inside an adversary's OODA loop (Observe, Orient, Decide, Act), LAWS can preempt human decision-making cycles and outpace opponents in combat. Their capacity for high-speed response, precise target discrimination, and sustained engagement gives them a potential advantage in various mission profiles, including air-to-air combat and missile defense.

In addition to tactical benefits, the cost-efficiency of LAWS is seen as a strategic advantage. Resources saved on personnel-intensive operations can be reallocated to logistics, medical support, cybersecurity, and simulation-based training.

However, the increasing deployment of LAWS also presents significant risks. Their speed and autonomy may outpace human judgment, expanding the scope for miscalculation, accidental escalation, and strategic instability. AI systems, while powerful, remain brittle—prone to error under uncertain conditions. Any malfunction or unintended engagement involving a LAWS platform could compromise strategic deterrence, especially in scenarios involving nuclear or high-stakes conventional weapons.

The integration of AI into command-and-control systems further complicates crisis stability. As these technologies continue to evolve, the margin for human oversight may diminish, increasing the potential for inadvertent conflict initiation. The changing incentives for preemption and retaliation under autonomous warfare conditions could undermine long-standing norms governing the use of force.

A state confronting an adversary equipped with autonomous weapons capable of operating at machine speed is likely to fear a surprise attack. This fear compresses the available window for strategic decision-making. The deployment of such systems during a crisis may generate anxiety over the possibility of a swift and decisive first strike, increasing pressure to act preemptively rather than risk being outpaced or disabled by a delayed response.

In active conflict scenarios, the fear of "losing at machine speed" could escalate tensions dramatically, including to the nuclear threshold. The speed advantage offered by LAWS may undermine first-strike stability, as states recognize that strategic outcomes could be determined faster than ever before. An aggressor leveraging LAWS could, for instance, target and dismantle an adversary's command and control infrastructure, effectively neutralizing retaliatory capability.

This dynamic could incentivize destabilizing postures, such as keeping strategic forces on high alert or considering pre-delegation of launch authority. States uncertain of their capacity to respond in time may adopt risk-prone policies to preserve credible deterrence.

Autonomous weapons may also erode escalation control mechanisms. A significant gap could emerge between the rapid operational demands of military systems and the slower, deliberative pace of political leadership. This disjunction risks sidelining opportunities for diplomacy, signaling, and de-escalation at critical moments.

Although LAWS may reduce battlefield casualties for the initiating actor due to their precision, they simultaneously increase the temptation to use force. As a result, the threshold for kinetic engagement may decline, raising the probability of both symmetrical and asymmetrical responses. Once escalation begins, its trajectory becomes increasingly unpredictable – particularly if the targeted party lacks equivalent precision or response capabilities.

Unintended consequences may include civilian harm and infrastructure damage. In such circumstances, retaliatory actions could magnify collateral effects. LAWS also rely on complex software and networked systems, making them vulnerable to cyberattacks. Adversaries or malicious actors could hijack or disable these systems, creating operational uncertainty. Manipulated or corrupted code poses further risks, potentially degrading system reliability or rendering capabilities inoperable at critical moments.

These developments are also beginning to erode the normative authority of international legal frameworks. The effectiveness of existing arms control regimes has diminished in the face of accelerating LAWS development. Many states are pursuing autonomous systems to gain strategic advantage, especially under resource constraints— undermining commitments to the rules-based global order.

International discussions on the regulation of LAWS are underway, primarily under the framework of the United Nations and in partnership with civil society and advocacy organizations. The Convention on Certain Conventional Weapons (CCW) remains the principal platform for deliberations. Since 2016, CCW has convened meetings aimed at examining the ethical, legal, and strategic implications of LAWS, with a focus on potential prohibitions or regulations.

Since 2018, the United Nations Secretary-General has called for a ban on LAWS, describing them as morally repugnant and potentially incompatible with international humanitarian law. A proposed new protocol, targeted for adoption by 2026, seeks to prohibit the possession and use of such systems.

It was emphasized that while the CCW has appropriately focused on the humanitarian dimensions of LAWS, equal attention must be paid to their strategic and doctrinal consequences. The risks of miscalculation, strategic instability, and inadvertent escalation require urgent and sustained analysis. Global regulatory efforts must therefore incorporate military-security perspectives to develop comprehensive and enforceable norms.

Beyond multilateral diplomacy, regional discussions and frameworks must also address these challenges. Transparency and restraint are essential, particularly among nuclear-armed states. These states should publicly reaffirm their commitment to maintaining meaningful human control over lethal force—especially in the context of command, control, and communications (C3) systems – and provide credible reassurances to the international community.

To build trust and reduce uncertainty, the implementation of confidence-building measures (CBMs) is essential. These could include transparency arrangements, technical dialogues, and structured information-sharing among states developing LAWS, contributing to overall global stability.

In this context, the proposal introduced by Pakistan at the CCW forum for an international legal protocol on LAWS has been recognized as significant. It outlines a pragmatic, holistic approach to regulation and restriction, emphasizing the need to maximize human control and minimize automation in the use of force. This proposal merits further international engagement and review.

Academic and research institutions must continue to play an active role in this domain. Scholars, technical experts, and policy analysts have a shared responsibility to highlight the strategic, legal, and ethical risks posed by LAWS. Building momentum for global dialogue, institutional reform, and the establishment of enforceable norms is vital to preserving peace, security, and human dignity in an age of algorithmic warfare.

Question Answer Session

Q: The concept of arms racing and its historical context is well established. Intelligence is never perfect, but how should arms racing be conceptualized in the non-physical world? How should it be understood?

A: Arms racing in the digital realm differs significantly from traditional models. Unlike the physical domain where states often engage in visible displays of military power to deter adversaries, the digital world is marked by deniability and concealment. Capabilities related to AI, quantum computing, or cyber tools are ambiguous and often hidden. This opacity increases the risk of overestimating adversary capabilities and drives states to accelerate their own development efforts, making the arms race more acute and harder to manage. Enhanced transparency could help develop a shared understanding to rein in these dynamics. Perfect security is a myth. From physical walls to missile defense, the quest for invulnerability has always existed, but complete safety remains unattainable. Accepting this vulnerability may help build cooperative security frameworks. Although some discussions are ongoing, substantive progress remains limited due to uncertainty about state intentions and capabilities.

Q: Will LAWS make traditional soldiers obsolete, or will their role remain relevant alongside technological developments?

A: The role of traditional soldiers is not immediately obsolete. While battlefields are evolving and becoming smarter, human presence remains significant. In recent conflicts like Ukraine, both military personnel and civilian actors—including commercial entities and cyber volunteers—played active roles. Soldiers must adapt to technological changes, equipping themselves with the knowledge and tools necessary to function in modern warfare. LAWS may reduce collateral damage and offer smarter tactical solutions, but human and civilian roles continue to be vital. States are investing more in AI-driven military capabilities, which create ripple effects globally and influences

others to follow suit. Militaries must innovate and reduce reliance on costly large-scale technologies, opting instead for smart technologies while preparing civilian populations to absorb shocks and contribute effectively in conflict scenarios.

Q: Given the vulnerabilities exposed by cyberattacks, is the world regressing to a pre-civil state of nature as theorized by Hobbes? Does this vulnerability offer a window for global cooperation, and is there any meaningful progress toward that?

A: The myth of invulnerability must be dispelled. Historical patterns reveal constant efforts to overcome vulnerability – from city quarantines to missile defense – but complete safety is elusive. Accepting this can promote cooperative and stable global security efforts. While discussions exist, progress is hampered by uncertainty surrounding state capabilities and intentions.

Q: In the future of autonomous warfare, will militaries be more detached from guilt over collateral damage? Are autonomous weapons used to deflect human responsibility in combat scenarios?

A1: LAWS and AI-driven systems may reduce collateral damage, but ethical concerns remain. The notion of deterrence originally aimed to avoid war and render victory obsolete, yet warfare persists under nuclear umbrellas. The concept of victory has evolved, necessitating smarter, more adaptive military strategies. Militaries must equip personnel for emerging battlefield realities, while civilians should be trained to respond and contribute. Despite technological progress, human accountability and responsibility remain essential.

A2: Digital arms races still rely on physical infrastructure—data access, computational power, and human expertise. Developing AI and quantum capabilities depends on funding, data collection, talent, and advanced hardware. This competition extends to institutional capabilities and private sector engagement. The private sector's growing role in defense represents a departure from traditional

nuclear-era arms racing models, requiring new regulatory approaches and norms.

Q: The role of non-state actors in conflict remains underexplored. The example of Elon Musk's Starlink in the Ukraine crisis highlights the potential involvement of private entities in satellite networks. There is growing concern about the development and outsourcing of technologies such as drones or cyber capabilities to conflict zones by private actors. How real is the fear of the commercialization of warfare, where private companies produce and supply conflict technologies to various regions?

A: The growing involvement of non-state actors represents an intensification of a long-standing trend. Commercial sector capabilities have long been used in warfare, but what is changing is the deeper integration of commercial and military actors and systems. This creates greater ambiguity and uncertainty about capabilities and intent, particularly when actors straddle both commercial and military spheres. This complexity complicates attribution and regulation. Work by scholars like Almudena – featured in an upcoming panel – provides deeper insights into these dynamics.

Q: Quantum technologies are rapidly integrating into the cyber domain. In the 20th century, nuclear weapons created deterrence; in the 21st century, can quantum technologies and cyber capabilities serve a similar deterrent function? Given their potential for data encryption, can these tools uphold deterrence in cyberspace?

A: Quantum technologies offer benefits such as secure communications through quantum encryption. However, they may also contribute to destabilization due to disparities in access. Some actors are already stockpiling encrypted information with the expectation that quantum decryption will soon make it accessible. This uneven technological access may heighten insecurity. Positive applications do exist – such as using AI to improve space governance and verify compliance with norms. Physical protection also remains crucial. Systems are constantly

being patched and upgraded, even as adversaries seek to undermine them. This forms an ongoing cycle of adaptation.

Q: Advanced technologies like AI, blockchain, and quantum computing are often taught for their peaceful applications. Given the discussions of their destructive potential, how can these emerging technologies be leveraged to combat proliferation, support disarmament, and control dual-use technologies? What mechanisms can ensure oversight of global supply chains?

A: Some states publicly display systems such as directed energy weapons to project power, while others engage in transparency and confidence-building measures. Think tanks and NGOs also play a crucial role by collecting and analyzing open-source data to expose patterns and inform the public. Technological applications for peace depend on whether deterrence is achieved by making attacks too costly or through diplomatic engagement. Strengthening diplomacy, transparency, and communication – especially through digital platforms – is essential. Collective efforts are required to harness technology for global good.

Q: As emerging technologies increase the temptation for first strikes and create new vulnerabilities, what defensive options remain for states seeking deterrence? Can such technologies be integrated into traditional survivability methods like concealment, hardening, and mobility? Can they enhance deterrence by punishment or denial?

A: Many strategic risks stem from imbalances and lack of transparency. Integrating emerging technologies transparently—alongside confidence-building measures and governance frameworks—can enhance stability. Quantum and AI technologies hold promise for nonproliferation efforts, including nuclear material detection and early-warning capabilities. Quantum sensing, for example, could be used by the International Atomic Energy Agency (IAEA) to monitor isotopes or detect preparatory nuclear activities. Emerging technologies can also aid disarmament verification without

compromising sensitive design information. Combining AI and quantum tools presents a viable pathway to strengthen global arms control and deterrence frameworks.

Session V

Weaponization of Space and Advancements in Missile Technologies – Challenges to Global Security

Moderator: Dr Adil Sultan

Dean Faculty of Aerospace and Strategic Studies, Air University

Space as the New Battlefield, Challenges to International Security and Stability

Ms. Almudena Azcárate Ortega
Researcher Space Security and WMDs, UNIDIR

The presentation was structured around three primary objectives. The first was to define key concepts and outline the architecture of space systems alongside their associated threat vectors. The second aimed to examine the principal threats to space security and their implications for international stability. The third objective sought to summarize the ongoing international efforts, particularly those led by the United Nations, to address these growing challenges.

The critical role of space in modern daily life was emphasized, particularly through systems such as Global Navigation Satellite Systems (GNSS), Earth observation satellites, and communication satellites. These systems provide essential services, including navigation, internet connectivity, financial transactions, and the functioning of critical infrastructure such as electricity grids and water supply networks. Any disruption to this space-based infrastructure could result in severe impacts on daily societal functions. Furthermore, such systems also underpin military and defense operations, especially in the areas of positioning, navigation, and timing (PNT), which are fundamental for accurate targeting and coordination across various operational domains.

It was noted that concerns over space security are not new. Since the launch of Sputnik in 1957, discussions on space-related issues have been held under the auspices of the United Nations. However, the strategic and economic relevance of space has increased dramatically, particularly since the early 2000s. This shift has been driven by the rise of commercial entities, which now constitute approximately 80% of the space economy. Additionally, an increasing number of states have emerged as active operators and stakeholders. Space is now recognized as being more congested, especially in low Earth orbit, and more

contested, as it has become a domain of strategic and military competition among nations.

A distinction was drawn between the concepts of militarization and weaponization. The militarization of space has existed since the beginning of human activity beyond Earth's atmosphere, with military uses such as reconnaissance and intelligence gathering generally regarded as consistent with peaceful purposes. In contrast, weaponization refers to the development and deployment of counterspace capabilities. It was further highlighted that the dual-nature of many space systems, where commercial capabilities support military objectives, contributes to further militarization and complicates efforts to regulate space activities.

Space systems were described as comprising three fundamental components: the space segment (e.g., satellites), the ground segment (e.g., ground stations, receivers, and modems), and the data links (i.e., uplinks and downlinks) connecting these segments. Threats to these components can originate from either terrestrial or orbital sources and fall into four broad vectors.

- **Earth-to-space** threats include kinetic attacks, such as direct-ascent anti-satellite (ASAT) weapons, as well as non-kinetic attacks using directed energy weapons.
- **Space-to-space** threats involve co-orbital ASATs and systems capable of conducting rendezvous and proximity operations (RPO), which possess both benign and potentially hostile applications. The ambiguity introduced by their dual-use nature poses significant verification challenges.
- **Space-to-Earth** threats encompass capabilities designed to support terrestrial military operations through space-based intelligence or strike facilitation, even when such services are provided by commercial or civilian entities.
- **Earth-to-Earth** threats, though less frequently addressed, include cyber and other non-kinetic forms of attack. The cyberattack on

Viasat during the Ukraine conflict was cited as a prominent example of the vulnerabilities faced by ground infrastructure.

Attention was then turned to space security challenges currently under deliberation at the United Nations. A significant obstacle remains the subjectivity of threat perception. Due to divergent national interests and strategic cultures, states often maintain differing interpretations of what constitutes a threat. Moreover, the consequences of threats originating in space frequently extend beyond the space domain, with the potential to cascade across terrestrial systems and borders.

A primary concern is the continued development and potential deployment of counterspace capabilities, both kinetic and non-kinetic. Even precision-targeted systems carry the risk of generating orbital debris, which poses indiscriminate dangers to all space actors. Additionally, the renewed interest in space-based missile interceptors, while not explicitly intended to destroy satellites, may still influence strategic stability and exacerbate existing tensions in space security.

Concerns have also been raised regarding dual-use space objects that serve both military and civilian functions. In times of conflict, any effort to disable or damage such systems, whether reversibly or irreversibly, could yield profound consequences for military operations and civilian life alike, with potential impacts extending across multiple states. These factors must be considered within discussions surrounding the law of armed conflict and the law of neutrality.

Terminology continues to play a pivotal role in shaping space security debates. Terms such as weapon, use of force, and peaceful purposes are subject to differing interpretations based on political, legal, and linguistic contexts. Such divergences may impede mutual understanding, complicate negotiations, and delay agreement within this technically complex and geopolitically sensitive domain.

While national space policies and doctrines may enhance transparency, they can also raise concerns if the language employed suggests a posture of aggression. Phrases such as warfighting or characterizations of space as an operational domain can contribute to heightened

tensions. Accordingly, careful and considered framing of policy language is essential to minimize misunderstandings.

Multilateral initiatives to address space security threats remain ongoing, though substantial progress has yet to be achieved. The Proposed Prevention of the Placement of Weapons in Outer Space Treaty (PPWT), introduced by Russia and China, reflects an interest in establishing a legally binding agreement. Additional measures, such as the 2022 United States pledge not to conduct direct-ascent ASAT tests, represent voluntary efforts to reduce risks and build confidence among spacefaring nations.

Despite these initiatives, considerable challenges persist. Key debates continue over whether it is more effective to prohibit specific capabilities or to regulate behavior. Moreover, divergent interpretations of core principles remain a significant barrier to consensus. In essence, the tensions witnessed in outer space mirror broader geopolitical dynamics on Earth. Thus, it has been argued that greater geopolitical stability on Earth would likely contribute to enhanced stability in space.

Echoing a remark previously made by Jessica West, it was concluded that space security must ultimately be viewed as a human endeavor. These are not merely technical or legal challenges, but issues that require inclusive, multilateral dialogue and cooperative engagement among a diverse range of stakeholders.

Impact of Space-Based Weapon Systems on Global Security

Ms Anna Belolipetskaia
Research Associate, Center for Energy and Security Studies CENESS

Space has already been militarized, a reality that cannot be avoided. This process began with the launch of the first satellite, Sputnik, in 1957. What is witnessed now, however, is an unprecedented level of militarization, with space assets becoming integral to modern warfare and military operations. The strategic value of these assets continues to grow, making it logical for states to seek counterspace capabilities to address vulnerabilities stemming from increasing dependence on space systems.

Counterspace technologies serve various purposes, including disabling or destroying enemy satellites, intercepting missiles, and conducting electronic warfare. These systems can be classified into several categories, kinetic physical, non-kinetic physical, cyber, and electronic.

Among these, weapons based on physical interference are the most disruptive and dangerous. However, such weapons have not been used by states against each other, and there is no confirmed evidence of their deployment. Like many EDTs, space-based systems are characterized by ambiguity. Active defense systems often resemble offensive weapons or can easily be converted into them. This blurring of lines creates an extensive gray zone, complicating efforts to distinguish between acts of aggression and legitimate deterrence.

The potential deployment of space strike systems could trigger a dangerous action-reaction cycle, risking an arms race in outer space and significantly increasing the chances of open conflict or miscalculation. Although the mass deployment of space-based strike systems has not yet occurred, even their limited introduction would represent a decisive shift. Should one state take this step, others are likely to follow. At that point, the discussion would move from

militarization to full-scale weaponization, a race for military supremacy in space rather than a mere technological competition.

Such a trajectory is profoundly destabilizing. The so-called ladder of escalation in outer space is not infinite, and each rung climbed brings the world closer to a tipping point. The next logical step after widespread weaponization would be a military conflict in space. While fictionalized in popular culture, such scenarios are not desirable in reality.

In terms of impact, the first area of concern is deterrence and strategic stability. Traditional deterrence strategies rely on mutually assured destruction. The advent of space-based strike systems introduces new concerns. These assets are technologically difficult to monitor independently, and their capabilities are often classified. This opacity fuels uncertainty, particularly given the dual-use nature of many space systems.

A certain level of transparency and predictability is essential for maintaining strategic stability. However, current levels of predictability are diminishing. Research institutions and commercial entities, such as the Secure World Foundation with its annual reports on counterspace capabilities, contribute significantly by providing transparency. Commercial actors are also increasingly active in offering space situational awareness services. Yet, due to the nature of space operations, the opacity gap cannot be entirely closed.

Second, space-based weapon systems offer rapid response capabilities due to their technical characteristics and broad coverage. These systems could potentially intercept missiles during the early boost phase of launch. While this may seem like a defensive advantage, it raises serious concerns by potentially undermining second-strike capability. Even without the deployment of space-based interceptors, space is already deeply integrated into strategic systems. Missile defense and space-based infrastructure form the backbone of early warning systems. The introduction of actual space-based interceptors would escalate an already militarized environment.

Third, space-based weapon systems are themselves highly vulnerable. Their orbits are predictable, their locations known, and they lack natural defenses, making them easy targets despite their strategic value. This vulnerability creates incentives for preemptive strikes during crises. Upgrades to existing systems or modifications such as further miniaturization or material hardening may be misinterpreted, especially under tense conditions, and fuel further ambiguity and suspicion.

The fear of losing critical capabilities and strategic advantage drives states toward destabilizing actions, including early strikes and conflict escalation. This is particularly important in relation to nuclear command, control, and communications (NC3) assets. Even minor disruptions or misinterpreted maneuvers of dual-use systems could bear serious consequences. Space-based weapons therefore lower the threshold for conflict, including nuclear escalation.

The second area of impact concerns existing legal frameworks. Currently, no legally binding norms directly prohibit space weaponization apart from the ban on placing weapons of mass destruction in outer space. Article I of the Outer Space Treaty mandates that outer space shall be used for peaceful purposes. However, the interpretation of "peaceful purposes" varies. Some interpret it as non-military, which is no longer feasible. Others interpret it as non-aggressive, but the deployment of space-based strike systems would violate both interpretations. This would transform outer space into an arena for military conflict, undermining its designation as a domain for the benefit of all humankind.

Such developments expose the gaps in existing international space law and underscore the urgent need for legal and diplomatic efforts to address the risks posed by space-based weapon systems.

Another concern is the general disarmament efforts. The deployment of space-based strike systems introduces the issue of irreversibility. Much like nuclear arms, reversing their deployment would be exceedingly difficult, if not impossible. Post-facto regulatory

agreements aimed at addressing such threats appear highly impractical once deployment occurs.

Technological asymmetry would also create new divisions. Not all countries would gain access to space-based capabilities, raising concerns over unequal strategic advantages. This disparity may eventually mirror the divide seen in the nuclear context, between nuclear-armed and non-nuclear states, creating a parallel of "haves" and "have-nots" in the realm of space-based strike systems.

The general atmosphere in international relations and trust between states would likely deteriorate. Deployment of such systems would be perceived as hostile and escalate tensions. This escalation would, in turn, exacerbate the security dilemma, accelerate arms racing, and further erode trust. As a weaponized domain, outer space would elevate the stakes of any terrestrial conflict. In the event of a major geopolitical crisis, tensions on Earth could easily spill over into space, intensifying escalation and expanding conflict beyond national borders into the global commons.

Another frequently raised concern in the broader context of international security is not only the use but also the testing of space weapons. Testing significantly increases the risk of generating excessive debris in orbit. These tests may involve intentional collisions or explosions, producing thousands of fragments, many of which are not traceable. Even absent military conflict, vast amounts of debris already exist in space due to ongoing civilian and military activity. This raises the real risk of triggering Kessler Syndrome, a scenario where the density of space debris becomes so high that it initiates a self-perpetuating cascade of collisions.

To illustrate, one can imagine a snow globe, where snowflakes inside represent fragments of debris. When shaken, the snowflakes multiply and obscure the interior. In a similar fashion, increasing debris could make outer space barely usable for future activities.

The way forward requires serious consideration. As with other emerging disruptive technologies, outer space remains a relatively new and unique domain. Although the idea of a legally binding instrument is seen as positive, challenges persist, particularly in establishing clear definitions and verification mechanisms. Draft treaties like the Proposed Prevention of the Placement of Weapons in Outer Space Treaty (PPWT) often face criticism. However, dismissing them as fundamentally flawed without thorough engagement is not a reasonable approach. If there is political will, viable solutions can be developed.

Another point that must be mentioned relates to general disarmament efforts. If space-based strike systems are deployed, irreversibility becomes a central concern, just as with nuclear arms, turning back time would be exceedingly difficult, if not impossible. The prospect of a post-factum regulatory agreement to address the threat after deployment appears highly impractical.

Technological asymmetry would also create new divisions. Not all countries would have access to space-based weaponry, raising concerns that others are gaining strategic advantage. Over time, this situation could mirror the nuclear context, creating a divide between states with and without space-based strike systems.

The deployment of such systems would likely be viewed as a hostile act, escalating aggression between states and exacerbating the security dilemma. This would accelerate arms racing and further erode trust. As a potential weaponized domain, outer space also raises the stakes for any future conflict on Earth. In the event of a major geopolitical crisis, tensions on the ground could easily spill over into outer space, intensifying escalation and expanding the scope of conflict beyond national borders into the global commons.

Another important point concerns the testing of space-based weapons. This significantly increases the risk of generating excessive orbital debris. Tests involving intentional collisions or explosions can produce thousands of fragments, many of which are untraceable. Even without

military conflict, current levels of debris from peaceful and military activities already pose a serious concern. In the long term, there is a real risk of triggering the Kessler Syndrome, a scenario in which the density of debris becomes so high that it leads to a self-perpetuating cascade of collisions.

To visualize this, imagine a snow globe. The decorative snowflakes inside represent space debris. Once shaken, the flakes multiply, obstructing the view of the interior. Similarly, in space, mounting debris could obscure and obstruct orbital paths, making normal operations nearly impossible.

It is important to consider paths forward. Outer space remains a relatively new and distinct domain. While a legally binding instrument is a commendable idea, challenges such as defining terms and verifying compliance remain unresolved. Draft treaties like the Treaty on the Prevention of the Placement of Weapons in Outer Space (PPWT) are often criticized for these reasons. However, dismissing such initiatives without genuine effort is not constructive. With political will, workable solutions can be achieved.

Scientific innovation offers a useful parallel. Had the belief prevailed that human flight was impossible, aviation and space exploration might never have occurred. A significant milestone was reached in 2024 when a UN Group of Governmental Experts achieved consensus on substantial elements of a legally binding instrument for the prevention of an arms race in outer space. Although challenges persist and consensus remains elusive in some areas, maintaining momentum remains crucial.

Parallel to this, Transparency and Confidence-Building Measures (TCBMs) are essential for fostering trust. One such initiative is the "no first placement of weapons in space" proposal by Russia. It is especially meaningful that this discussion takes place in Pakistan, a state that supports the initiative. In 2019, Russia and Pakistan jointly signed onto this political commitment.

Such declarations reflect a desire to refrain from deploying space-based weapons, representing a step toward reducing tensions and clarifying mutual expectations. Addressing threats and perceptions at their roots is vital. Transparency in doctrines and strategic plans is necessary, but transparency alone does not resolve concerns. Declaring intentions to construct space-based interceptor systems, for example, can worsen the security situation even if such declarations are made openly.

Statements that define space as a "warfighting domain" are deeply concerning. Rather than adding new sources of instability, the priority must be to eliminate existing ones. Mutual understanding and dialogue are essential, not only for managing emerging technologies in space, but for broader international security.

To conclude, when it is darkest, humanity looks to the stars. The original meaning of this phrase is one of resilience and hope, facing adversity with determination to build a better future. But it can also serve as a literal hope: that the stars remain visible as beacons of peace, not obscured by the fire and fallout of space-based warfare.

Impact of Advancements in Missile Technologies on Nuclear Deterrence

Dr. Christine M. Leah
Fellow, The National Institute for Deterrence Studies

Technological advancements have not yet posed a fundamental challenge to the foundational principles of nuclear deterrence. Although innovations in AI, hypersonic weapons, and decision-making tools may influence certain aspects of strategic stability management, they have not emerged as significant threats to the primacy of nuclear deterrence itself. A historical perspective, particularly regarding the evolution of missile defense, provides valuable insight into the current strategic context. A new era has begun in how missile defense is conceptualized, with several critical elements now evident. These include the increasing precision of technology, the shifting role of missile defense within deterrence frameworks, and a distinct geographic context, especially within the Asia-Pacific region.

Missile defense dynamics in the Asia-Pacific differ markedly from those observed in the European or NATO context. As a predominantly maritime region, the Asia-Pacific has only recently begun to integrate missile defense into its strategic calculations. This shift has been driven largely by evolving geopolitical dynamics. Unlike Europe, no multilateral security structure comparable to NATO exists in Asia, resulting in a unique and fragmented strategic environment. The notion of a "missile age" has been aptly applied to this era, drawing on the work of Professor Paul Bracken. Bracken categorized different nuclear periods according to a range of variables: the number and nature of nuclear-armed states (e.g., superpowers versus smaller states such as Pakistan or France), the structure of the international system (bipolar versus multipolar), levels of economic power, technological advancement, and divergent worldviews and strategic challenges. These variables help explain distinct patterns of state behavior and international interaction.

While recent technological developments may appear novel, they are not without precedent. During the early Cold War, technologies such as jet aircraft, ballistic missiles, nuclear submarines, radar, and satellites were introduced in ways that were initially poorly understood. Strategic actors often possessed clarity regarding adversarial identities, but not necessarily how these actors would exploit new technologies. Each new wave of innovation prompted renewed strategic learning, particularly within nuclear dyads such as India and Pakistan.

Learning behaviors and signaling mechanisms between states remain central to maintaining strategic stability. Questions continue to be raised about the meaning behind specific military actions, such as missile tests, bomber deployments near adversarial territories, or the scrambling of fighter squadrons. These operational movements are routinely interpreted in real time by policymakers and military planners, often based on experience gained in governmental and defense roles.

Historical scholarship offers useful context. For example, a late 1970s publication by the Brookings Institution includes a chapter by Ron Huisken, which addressed the then-nascent debate over cruise missiles. These weapons raised uncertainty regarding their classification as tactical or strategic assets, given their flight paths and limited traceability. This historical debate serves as a cautionary reminder to approach contemporary technologies, such as hypersonic weapons, with a critical yet measured lens, avoiding overstatement of their potential to destabilize deterrence.

The central challenge posed by emerging technologies lies not in the technologies themselves, but in the evolving conceptual and operational frameworks required to manage them. Advances in nuclear delivery systems, decision-making tools, and information processing, especially with the integration of AI, underscore the growing complexity of real-time intelligence operations. Data streams from drones, automatic license plate readers, satellite imagery, and

intercepted communications may now converge around a single decision point. The critical question is whether AI systems can effectively distill this data into coherent and actionable insight.

Nonetheless, no current technological development has fundamentally altered the core principles underlying missile defense or nuclear deterrence. Rather than a reinvention of deterrence, what appears necessary is a more sophisticated management of established principles, including second-strike capability, damage limitation, and strategic signaling. Several noteworthy dynamics are converging in the present environment. First, the profile of states investing in missile defense, especially within the Asia-Pacific region, such as Japan and Australia, which have historically placed limited emphasis on missile defense, are now significantly expanding their capabilities. Traditionally, such systems, particularly advanced platforms like the SM-3 and SM-6, have been associated with nuclear-armed states.

Second, emerging technologies are reshaping both operational capabilities and decision-making structures. These changes are especially pronounced in domains such as targeting, command and control (C2), access, basing, and overflight rights. Greater integration is observed across platforms and among countries that are not formally allied. Instead, these actors operate within a "hub-and-spoke" model centered on the United States, either through Washington or the U.S. Indo-Pacific Command (INDOPACOM). In this strategic environment, most coordination ultimately traces back to U.S. combatant commands.

Third, these developments intersect with the concept of nuclear deterrence, particularly in the context of extended deterrence in the Asia-Pacific. Although the strategic rise of China has long been recognized among analysts, it is only recently that regional governments have begun to publicly frame China as a threat to regional stability. Historically, missile defense has been conceptualized almost exclusively within the framework of nuclear deterrence. A persistent tendency has been observed to conflate nuclear warheads with their

delivery systems, even though these are separate technologies developed independently but concurrently.

This conceptual conflation raises strategic questions of significance. For example, how might the elimination of nuclear warheads, but not the missiles themselves, affect the integrity of deterrence architectures? Missiles compress time and space in military conflict. While bombers significantly reduced the time required to project nuclear force, missiles accelerated this process even further, making the prospect of nuclear devastation a matter of minutes. This compression of time and space must be considered when analyzing the evolving nature of missile defense and deterrence.

It has been suggested that modern deterrence may inherently be missile-based nuclear deterrence, wherein the combination of delivery system and warhead forms the foundation of a credible threat. This raises further questions about the viability of post-nuclear deterrence frameworks. Can conventional hypersonic missiles, absent nuclear payloads, serve as credible deterrents? In certain contexts, this may be plausible; in others, it may prove insufficient. Historically, missile defense debates have focused primarily on the European and NATO contexts. However, a conceptual shift toward the Asia-Pacific is now essential. Key questions include how deterrence and missile defense should be structured within a hub-and-spoke alliance system, where regional partners are connected to the United States but not necessarily to one another.

This scenario introduces several complex operational considerations: How should collective deterrence be organized? What are the implications for command and control, escalation thresholds, and basing arrangements? Can forces from Australia be forward-deployed in Japan, and vice versa? Who retains operational authority, the deploying state or the host nation?

In addition to strategic concerns, logistical factors also demand attention. These include fuel supply, maintenance, resupply, and the overall sustainment of forward-deployed forces. Though often

overlooked, these considerations are essential to the construction of a credible and integrated regional deterrence posture. Bringing these elements together represents a formidable challenge. Policy complexities, ranging from alliance coordination to technological integration, require adaptive and well-structured responses. A crucial issue involves the intentions of major powers, as well as the degree of strategic agency available to allied and partner states.

An often neglected but relevant concept is Technology Readiness Levels (TRLs), a methodology used to track and assess the maturity of technological developments across other nations. Updating national policies in alignment with real-time awareness of TRLs constitutes a necessary, though ambitious, undertaking. This issue connects directly to the broader concept of warning time.

Australia's defense planning previously incorporated a "10-year strategic warning time" as a guiding principle. However, this notion was removed in the latest National Defense Strategy, with no formal replacement announced. The absence of a clearly articulated metric for strategic warning represents a significant gap, particularly in light of today's rapidly shifting threat environment. In conclusion, while new technologies may not yet have fundamentally altered the relationship between missile defense and nuclear deterrence, they are transforming the broader strategic context within which these issues are debated. The current era is defined by a complex interplay between historical frameworks and emerging challenges, encompassing deterrence, missile technology (both nuclear and non-nuclear), geographic realities, political alliances, military logistics, and institutional processes.

The Asia-Pacific region appears increasingly poised for strategic and technological turbulence. Effective preparation for this uncertainty will require adaptable institutions, credible deterrence frameworks, and, above all, strategic clarity.

Implications of India's March Towards Space Weaponization

Dr Zafar Nawaz Jaspal
Dean, Faculty of Social Sciences, QAU, Islamabad

It is pertinent to analyze the pace of India's space weaponization and its implications for both regional and global strategic stability. Building on the earlier overview of space defense systems provided by Christine, it focuses on two central questions:

1. What is the trajectory of India's progression toward space weaponization?
2. How might this development affect the strategic environment in South Asia and beyond?

The Technological Trajectory

The evolution of technology has consistently reshaped warfare. Historically, new technologies have enhanced offensive capabilities and rendered existing defensive systems inadequate, creating imbalances that often precipitate conflict. This pattern continues in the current era of space militarization.

The shift from peaceful uses of space to militarization, and increasingly toward weaponization, is evident. As great power rivalries extend into outer space, the risks of a cascading arms race grow significantly. Space weaponization introduces a dangerous dynamic, prompting other nations to pursue similar capabilities without fully evaluating the long-term consequences.

While over 80 countries are active in space, only a few possess advanced counter-space systems. Notable examples include: United States: X-37B spaceplane; Russia: Nudol anti-satellite missile system; and China: Shijian-17 co-orbital satellite

These developments reflect a growing emphasis on space dominance and the denial of adversarial military advantages derived from space-based assets.

India's Strategic Shift Toward Aerospace Power

India is actively pursuing the transformation of its military into an aerospace power. Its Joint Doctrine classifies space as a vital domain alongside land, sea, air, and cyber, indicating the recognition of space as a future arena of strategic competition.

Notable milestones include:

- **April 8, 2025**: India launched 52 military satellites dedicated to intelligence, surveillance, and reconnaissance (ISR).
- **Institutional framework**: The creation of the Tri-Service Defense Space Agency (2018) and the Defense Space Research Organization, affirm India's long-term space militarization goals.

India's space program is increasingly dual-use, blending civilian and military applications. Capabilities under development or deployment include:

- Directed energy weapons
- Cyber and electromagnetic pulse (EMP) tools
- Kamikaze micro-satellites and robotic interceptors
- Concepts like missile beds in space

India's satellite fleet, including GSAT-6, GSAT-7, and the RISAT series, supports both tactical and reconnaissance missions.

Anti-Satellite Weapons and Strategic Partnerships

- **Mission Shakti (March 2019)**: India successfully demonstrated a direct-ascent anti-satellite (ASAT) capability using the Prithvi Defense Vehicle Mark-II, validating key missile defense technologies.

- **MIRV developments**: India has tested multiple independently targetable reentry vehicles (MIRVs), most notably with the Agni-V in 2024, bolstering its strategic strike options.

India's partnership with the United States has accelerated its access to dual-use and military-grade space technologies. Key developments include:

- Strategic Trade Authorization-1 (2018)
- Basic Exchange and Cooperation Agreement (BECA)
- Collaboration with Quad members (Japan, Australia) and bilateral space cooperation with France

These developments reflect India's ambition to secure a prominent role in the emerging global space order.

Implications for Pakistan

India's expanding space-based military capabilities pose a direct challenge to Pakistan's full-spectrum deterrence posture. These advances could undermine strategic stability and increase the risk of escalation, whether deliberate or inadvertent.

While Pakistan maintains a policy opposing space weaponization, the evolving security environment may necessitate reassessment. Ensuring credible deterrence could require investments in:

- Space-based surveillance systems
- Defensive counter-space capabilities
- Real-time intelligence, target acquisition, and damage assessment infrastructure

Despite limited resources, Pakistan has a longstanding space program through SUPARCO (Space and Upper Atmosphere Research Commission), supporting remote sensing, communications, and scientific research.

Conclusion

India's advancements in space-based military technology, ranging from ISR and ASAT systems to cyber and EMP tools, enhance its capacity for:

- Preemptive strikes
- Counterforce operations
- Strategic dominance

These developments not only raise the threshold for regional arms racing but also compel Pakistan to re-evaluate its strategic posture.

Whenever technological revolutions occur, they tend to disturb established balances and increase the likelihood of conflict. Therefore, a careful, measured, and forward-looking strategic response is essential to preserve stability in South Asia.

Question Answer Session

Q: To what extent might it be considered that the rise of civilian space tourism missions, such as Blue Origin's recent suborbital flight featuring an all-female crew, has inadvertently diverted global attention from critical issues such as the weaponization of outer space and astropolitics, particularly within the context of ongoing strategic discussions?

A: Civilian space tourism does not necessarily detract from discussions on the weaponization of space. In fact, it may raise broader public awareness about the importance of space security. While concerns exist regarding equity and environmental impacts, the visibility of such missions can highlight the growing strategic and security relevance of outer space, potentially broadening societal engagement in astropolitical debates.

Q: To what extent has the concept of the "responsible use of outer space" been regarded as an alternative to the formal codification of the PPWT? Furthermore, how have calls to ban tests of direct anti-satellite (ASAT) weapons and similar technologies been perceived within the broader context of space security and arms control?

A: Responsible behavior and legally binding agreements are not mutually exclusive. They can and should complement each other. Instruments like the PPWT define and regulate capabilities, while responsible behavior guidelines address how those capabilities are employed. Both are essential in managing dual-use technologies. On banning ASAT tests, support exists in principle due to their potential to create space debris, but concerns remain over selective application and the imbalance between technological "haves" and "have-nots".

Q: What are the potential risks to space-based asymmetric nuclear deterrence and global governance posed by Google's investment in an Indian company manufacturing satellites for the Indian Air Force, particularly in the absence of clear international FDI frameworks for dual-use technologies?

A: The lack of comprehensive international frameworks for foreign direct investment in dual-use space technologies creates vulnerabilities in deterrence stability and global governance. Private sector involvement in defense-related satellite infrastructure introduces ambiguity regarding state accountability and intent. Such investments can inadvertently escalate strategic competition, especially when directed toward ISR capabilities for national militaries. Greater transparency and international regulatory mechanisms are needed to address this emerging risk.

Q: Space debris collection technologies are reportedly being developed but could be repurposed to attack satellites. What are the implications for space security? Second, China tested a Fractional Orbital Bombardment System (FOBS) in 2021. How does this development impact nuclear deterrence between China and the United States?

A: Technologies like Active Debris Removal (ADR) exemplify dual-use dilemmas in space. While developed for peaceful purposes, such systems can be perceived as an offensive tool, particularly if transparency is lacking. This can trigger mistrust and an arms race dynamic. As for FOBS, its potential to bypass traditional missile defense systems presents new challenges for nuclear deterrence and strategic stability, particularly between major powers like China and the United States. Such developments could undermine mutual vulnerability assumptions and complicate crisis management.

Q: How does the growing involvement of private actors like SpaceX impact smaller states such as Pakistan that lack comparable infrastructure and budgets? Could this effect access to space data, reconnaissance capabilities, or raise concerns regarding sovereignty and strategic asymmetry?

A: The growing role of private entities introduces asymmetries that could not be beneficial for smaller states. Commercial actors possess significant funding, infrastructure, and influence, often operating beyond the regulatory reach of less developed space programs. This

concentration of capabilities could limit equitable access to space-based data and services, exacerbate dependence, and complicate issues of sovereignty. Strengthening national regulatory frameworks and encouraging public-private partnerships are essential for balancing this trend.

Q: Considering that 80% of the space economy is dominated by commercial entities, and that current international law requires enforcement through states, is there a need for a more proactive regulatory approach to address the destabilizing potential of private actors in space? Additionally, given the semantic discrepancies across languages in defining terms like "weaponization," are these differences politically driven or genuinely interpretative in nature?

A: Current frameworks, including Article VI of the Outer Space Treaty, already assign responsibility to states for the actions of commercial entities. However, enforcement at the domestic level varies, and gaps persist. The commercial sector's growing role necessitates stronger, more proactive international oversight.

As for terminology, differences are both politically and linguistically driven. Some states intentionally exploit ambiguity, while others struggle with conceptual translation. For example, many languages do not distinguish clearly between "militarization" and "weaponization." Initiatives like the UNIDIR Space Security Lexicon aim to clarify these discrepancies and promote shared understanding.

Q: The Outer Space Treaty is subject to varying interpretations. Given the emergence of parallel norm-building efforts like the Artemis Accords, especially concerning resource extraction and space sovereignty, how do you assess the future of space governance? How should states outside these coalitions, such as Russia and China, engage with this process?

A: Global space governance must be inclusive and multilateral. Treaties like the Outer Space Treaty have near-universal ratification and should be interpreted and evolved collectively, not through

exclusive initiatives. Parallel frameworks such as the Artemis Accords risk creating legal fragmentation and privileging certain actors. States outside such coalitions, including Russia and China, advocate for universal processes through the UN system to ensure equity and prevent hegemonic control over outer space.

Q: How is Indo-U.S. technological and AI cooperation enhancing India's ISR (intelligence, surveillance, reconnaissance) capabilities, and what implications does this have for Pakistan's strategic environment?

A: The Indo-U.S. partnership in critical and emerging technologies, including artificial intelligence and ISR systems, enhances India's capacity for real-time surveillance, target acquisition, and strategic planning. Agreements like BECA and COMCASA have provided India access to geospatial intelligence and satellite-based targeting. This integration reinforces India's military modernization and tilts the regional balance. Pakistan must adapt to this changing landscape by investing in its own capabilities and maintaining strategic stability through credible deterrence.

Session- VI

Emerging Technologies and Arms Controls, Challenges and Opportunities

Moderator

Dr. Asma Shakir Khawaja

Executive Director, CISS AJK

Emerging and Disruptive Technologies: Prospects and Challenges to Arms Control Framework

Prof. Dr. Andrey Pavlov
Head of the Master Program "Strategic and Arms Control Studies" at Saint Petersburg University, Russia

One of the foremost challenges in arms control today lies in the inherent ambiguity and definitional complexity surrounding emerging technologies. A key difficulty is distinguishing between military and non-military applications, as many of these technologies possess dual-use characteristics.

To contextualize this challenge, reference can be made to John Mearsheimer's 1990 article, *"Why We Will Soon Miss the Cold War."* While controversial at the time, the article underscored the strategic predictability and clarity that characterized the Cold War period. By contrast, the current post-Cold War era lacks this clarity. Arms control frameworks developed during that earlier period are proving insufficient in today's more ambiguous and fragmented strategic environment.

During the Cold War and its immediate aftermath, shared definitions, stable political conditions, and mutual recognition of threats enabled the negotiation and implementation of effective arms control agreements. That era is now widely considered a golden age for arms control. The current phase, by contrast, may be viewed as a "dark age," marked by declining momentum, growing mistrust, and inadequate institutional responses to rapidly advancing technologies.

A central problem is the difficulty in identifying which emerging technologies should be subject to arms control regulation. The increasing overlap between civilian and military applications complicates efforts to assess threat levels and strategic implications. This dual-use nature of many technologies introduces profound uncertainty into arms control deliberations.

Moreover, the absence of precise definitions undermines the development of stable and enforceable agreements. Historical experience illustrates this challenge. In the 1980s, for instance, the lack of a clear definition of cruise missiles created enforcement difficulties for the Intermediate-Range Nuclear Forces (INF) Treaty. The emergence of UAVs, which arguably fell under the treaty's scope but were not explicitly included, further highlighted this definitional gap.

A similar issue now arises with hypersonic weapons. When a hypersonic warhead is mounted on a ballistic missile, questions emerge about whether it should still be classified as a ballistic system. This ambiguity complicates the classification and regulation of such technologies under existing treaties or any future instruments.

Beyond the technical and definitional concerns, another significant challenge lies in assessing the real-world impact of these technologies. Traditionally, arms control decision-making has involved weighing the potential military advantage of new technology against its impact on strategic stability. However, when the implications of technology are uncertain or evolving, informed decision-making becomes more difficult.

While emerging technologies clearly offer strategic advantages to those states that adopt and operationalize them, the risks, especially in terms of crisis instability, arms races, and strategic misperception, are less well understood. Experts in strategic studies and arms control may grasp these dangers, but this understanding does not always translate into the thinking or priorities of decision-makers.

This disconnect between technical assessment and political action further impedes progress in arms control. It is not merely a question of political will, but also of conceptual preparedness and institutional adaptability. The field must address not only technological innovation itself, but also the accompanying epistemological and normative gaps in regulation and governance.

A further complication lies in the asymmetry between how the benefits and risks of emerging technologies are perceived and communicated. Technological advantages, particularly in the military domain, are often immediate, visible, and politically attractive. In contrast, the risks are typically long-term, probabilistic, and complex, making them harder to convey and prioritize in policymaking. This imbalance contributes to a lack of political will to impose controls or restrictions on potentially destabilizing technologies.

This lack of clarity creates confusion not only about which technologies should be regulated, but also how they should be regulated. Arms control agreements vary in nature, from outright bans on certain weapon types to general norms and codes of conduct. This diversity makes it difficult to establish a consistent or predictable regulatory approach across different technological domains.

Additionally, there is significant uncertainty regarding acceptable levels of risk. Arms control decisions must often be made based on projections rather than demonstrated threats, and it remains challenging to determine when a risk is serious enough to warrant formal regulation. As long as this ambiguity persists, effective regulation of emerging technologies will remain elusive.

This brings attention to the notion of preventive arms control. Historically, examples of successful preventive arms control are rare. Most arms control regimes have been reactive, emerging only after the deployment or battlefield use of certain weapons has clearly demonstrated their destabilizing effects. Preventive arms control, while desirable in theory, struggles in practice due to the very lack of clarity it seeks to address.

The second category of challenges concerns the increasingly significant role of private developers and non-state actors in military-relevant technological innovation. Such as the example of complications arising when private companies develop technologies that are later co-opted for military purposes. This is not a theoretical concern; it has already

been encountered in the implementation of the Biological Weapons Convention (BWC).

In the case of the BWC, private laboratories, especially in countries like the United States, operated under government contracts yet remained outside the reach of any binding international verification mechanism. This blurred line between public and private authority made enforcement nearly impossible. Today, similar patterns are emerging with new and emerging technologies that originate in the commercial sector.

There are current conceptual-level discussions within the United States regarding the potential incorporation of private sector components into national ballistic missile defense systems, particularly in launch detection. If implemented, such initiatives could be transformative, but they would also significantly complicate the transparency and accountability expected under international arms control norms.

To some extent, existing regimes have adapted to technological change. Within the Nuclear Non-Proliferation Treaty (NPT) architecture, institutional mechanisms like the Nuclear Suppliers Group (NSG) and the Zangger Committee have conducted technology assessments to update export control lists and regime effectiveness. Similarly, the Organization for the Prohibition of Chemical Weapons (OPCW) maintains a technical secretariat tasked with reviewing scientific and technological developments.

In contrast, the BWC remains structurally disadvantaged in this regard, lacking any formal body or institutional infrastructure to perform science and technology reviews. While the need for such oversight has been acknowledged, progress has been slow and piecemeal. The Missile Technology Control Regime (MTCR) does hold expert meetings to revise control lists, but implementation and enforcement remain dependent on national discretion.

Despite these efforts, the limitations of traditional, state-centric arms control diplomacy are evident. Most arms control frameworks were

designed during a period when current technologies were either non-existent or unanticipated. This has left regimes ill-equipped to address the non-state, transnational, and commercial dimensions of today's technological landscape.

Attempts to incorporate private industry and non-governmental stakeholders into these regimes have been limited and largely unsuccessful. Yet these actors are now among the most important players in the development, deployment, and application of emerging and disruptive technologies.

It is worth noting, however, that not all trends are negative. Emerging technologies may also strengthen arms control regimes by improving verification capabilities. For example, under the New START Treaty, new technologies have helped create a more simplified and cost-effective verification system, without sacrificing credibility or transparency. But realizing these benefits demands long-term institutional commitment, cross-sectoral engagement, and normative innovation. Without such a collective effort, arms control will continue to lag behind the accelerating pace of technological change.

Confidence-Building Measures for Emerging and Disruptive Technologies

Dr HE Miao
Research Fellow, China Arms Control and Disarmament Association (CACDA), China

Confidence-building measures (CBMs) for emerging and disruptive technologies (EDTs) constitute a broad and complex agenda. AI is widely regarded as one of the most disruptive technologies and needs more targeted exploration of challenges and feasible pathways for CBMs.

Primary responsibility for managing and reducing EDT-related risks rests with sovereign states. Disparities in understanding, developmental stages, and governance capacity across countries pose significant hurdles. When building CBMs for EDTs, it is essential to balance the security concerns of all nations; core national-security interests should not be compromised merely to reach consensus, or CBMs risk becoming ineffective and symbolic.

A defining trend in technological advancement is the accelerating pace of development: capabilities move rapidly from laboratories to battlefields, with isolated breakthroughs giving way to systemic integration. In AI, advances in deep learning and autonomous learning models (ALMs) have shortened updating cycles. Automation and autonomy in military systems are advancing quickly. The U.S. military's Joint All-Domain Command and Control (JADC2) concept aims at minute- or even second-level coordination across domains, fundamentally reshaping operational tempo and decision-making structures.

Technology diffusion is increasingly decentralized. Many EDTs exhibit low barriers to access yet high proliferation risks, and the civilian-military boundary is increasingly blurred. Open-source AI models can equip non-state actors with advanced cognitive capabilities, while commercial satellite constellations and remote-sensing data enable

smaller states and private entities to generate strategic-level intelligence. This democratization of technology fosters innovation but also amplifies uncertainty and unpredictability in conflict.

Strategic competition is shifting toward algorithmic dominance. Future stability will depend not only on physical strike capacities but also on information control, decision speed, and situational acuity. EDTs, particularly AI, are becoming arenas for competition in algorithmic superiority, where the ability to deconstruct and reconstruct complex battlefield scenarios through data-driven models can confer decisive advantage.

Security risks are becoming systemic and harder to contain due to tight interdependencies among technologies. AI-enabled unmanned platforms combined with cyber or electronic warfare can enable rapid information masking and destructive strikes, heightening risks of miscalculation and escalation. The integration of quantum communication with AI command systems may introduce opaque, non-explainable "black-box" processes that resist external verification, further eroding the transparency on which CBMs rely.

Traditional arms-control frameworks are increasingly outpaced. Post-Second World War regimes assumed states as sole actors, gradual technological change, and feasible verification. Rapidly evolving, cross-border, and often unverifiable technologies undermine that logic. Key questions follow: how to define responsible use of AI algorithms; what standards should govern such use; how to verify AI assistance in nuclear decision-making given the confidentiality of NC3; and whether globally applicable yet adaptable AI ethics principles are attainable.

The rapid development of EDTs has become a fundamental challenge to global governance and stability. These technologies will shape the trajectory of major-power competition and could tip the balance between peace and conflict, while presenting unprecedented difficulties for the CBMs currently under discussion.

Governance responses are emerging under United Nations frameworks. Mechanisms such as the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) provide platforms for multilateral dialogue in cyber, outer space, and AI. The OEWG has sustained discussions on information security, while the GGE has explored ethical and military dimensions of AI. China has contributed through the Global AI Governance Initiative and the Global Data Security Initiative, advancing a governance philosophy that is people-oriented, secure, controllable, open, and inclusive. In the military domain, a position paper on regulating AI applications calls for stronger oversight and a community with a shared future in AI.

In December 2024, a consensus between Chinese President Xi Jinping and then U.S. President Joe Biden reaffirmed maintaining human control over nuclear weapons, an instructive CBM and a useful reference for broader global agreement.

Significant obstacles persist. First, intensifying geopolitical competition places EDTs at the center of strategic rivalry; some states treat technological superiority as a core imperative and resist transparency or cooperation, weakening foundations for CBMs, for example, by opposing algorithm-sharing or training-transparency mechanisms in AI military applications. Second, innovation outpaces governance: technological progress advances in leaps, while international rule-making evolves over years or decades. Cyber threats such as hacking, ransomware, and AI-generated disinformation proliferate without comprehensive global norms, impeding CBM implementation. Third, confidentiality conflicts with verifiability. Military EDTs depend on sensitive data, algorithms, and operational models whose secrecy requirements clash with transparency demands. Many AI systems function as black boxes; even with algorithmic disclosure, behavior can remain opaque against ethical or regulatory standards, challenging CBM logic.

Practical steps should begin without waiting for perfect consensus, starting with minimal yet meaningful measures to manage risk and build trust:

I. Prioritize soft CBMs. Begin in domains of broader consensus and lower sensitivity. Encourage publication of national technology-policy white papers to articulate governance principles and red lines. Establish bilateral or multilateral expert exchanges for non-binding policy dialogue, fostering shared ethical principles and responsibility mechanisms for AI systems.

II. Draw lessons from traditional regimes. The Chemical Weapons Convention (CWC) and Biological Weapons Convention (BWC) demonstrate incremental institutional design: mechanisms can stand up while negotiations continue, with oversight tailored to local conditions. The CWC's technical secretariat, routine inspections, and state-rights safeguards provide useful references for AI and cyberspace. The P5 nuclear glossary offers a model; a jointly developed glossary for outer space could serve as an effective CBM if truly global and collaborative.

III. Ensure inclusiveness and diversity. Governance should not be dominated by a small circle of major powers. Developing countries have legitimate concerns, AI ethics, data governance, cyber resilience. A fair platform should enable equal participation, shared benefits, and joint responsibility.

IV. Reinforce multilateral platforms. Under UN auspices, multilateral mechanisms should continue to lead in rule-making, capacity-building, and crisis communication and management. Regional organizations, research institutions, and public- and private-sector stakeholders should be engaged to build a collaborative, multi-level governance ecosystem.

Technology is a double-edged sword, but human rationality and cooperation remain the most reliable shields. Even during the tensest periods of the Cold War, the international community established

stabilizing mechanisms, such as the NPT and INF, to curb strategic risks and maintain major-power stability. Today's security environment is more complex and novel; precisely for this reason, forward-looking and constructive approaches, anchored in transparency, trust, and shared resolve, are essential to lay the foundations of a peaceful future.

Evolving International Law on Managing Emerging and Disruptive Technologies

Brig Dr. Zahir Kazmi (R)
Arms Control Advisor – Strategic Plans Division (SPD), Pakistan

The conduct of war is no longer solely about humans and hardware; it is increasingly about code. Unless international law adapts, the next war may be governed not by conscience but by algorithms. The discussion unfolds across five key segments: the shift in the character of warfare; six legal and strategic risks; three normative opportunities; Pakistan's contribution to the discourse; and four practical propositions for governing these technologies.

The term emerging and disruptive technologies (EDTs) encompasses developments such as artificial intelligence (AI), autonomy, quantum computing, synthetic biology, and space systems. However, many of these technologies are no longer merely emerging; several have already entered military use and begun altering operational doctrines. It is therefore more appropriate to refer to them as emerging and disruptive military technologies (EDMTs). These systems are not simply enhancements of existing capabilities but enablers of a new mode of warfare. In many respects, they are already outpacing the legal regimes intended to govern their misuse.

International law, particularly the law of armed conflict or IHL, was constructed around human judgment. It presumes that a soldier can distinguish between combatants and civilians, avoid excessive harm, and take necessary precautions before launching an attack. The question arises: how can an algorithm make moral decisions? Even as certain systems are designed to simulate empathy or interpret emotional cues, such features remain approximations. While potentially useful in civilian contexts, they are inadequate for ethical decision-making in combat scenarios.

This transformation signifies more than a change in tools; it represents a rupture in the legal and moral fabric that governs warfare. Six legal and strategic risks require urgent attention.

• **Delegation of lethal decision-making:** When autonomous weapons select and engage targets without human oversight, accountability disappears. This is the most fundamental ethical concern.
• **Nuclear-AI convergence:** The fusion of AI with nuclear command and control compresses decision timelines and risks misreading intent, rendering deterrence dangerously brittle.

• **Asymmetric diffusion:** AI-enhanced drones, deepfakes, and cyber weapons, once the preserve of major powers, are now accessible to weaker states and non-state actors, disrupting power balances and creating new threats.

• **Dual-use opacity:** The same technology that powers hospitals or airport security can be weaponized for surveillance or targeting. Facial-recognition systems, for example, can assist both a doctor diagnosing a patient and a military unit selecting a target, identical code, divergent consequences. International law is struggling to keep pace with this dual-use ambiguity.

• **Verification vacuum:** Many of these systems operate as deep-learning "black boxes." Even their designers do not fully understand how or why certain decisions are made.

Under Article 36 of Additional Protocol I to the Geneva Conventions (1977), each new weapon must be reviewed for compliance with IHL. Yet the challenge remains: how can a system be legally reviewed when it is not fully understood? It is akin to approving a weapon without knowing what triggers it or who it might target. This complexity underscores the urgent need for developing countries in the Global South to simultaneously strengthen their technical and legal review capacities.

Another strategic concern is the widening regulatory rift between China and the United States, and even within the Western bloc.

Competing models of regulation are fragmenting not only access to technology but also the rules that govern it. The world is no longer merely racing to regulate; it is racing to remain relevant. Alarmingly, this race is shifting from legal instruments to lines of code. The risk of decoupling is that states become locked into opposing regulatory blocs, where the laws of war may increasingly mirror great-power rivalries rather than a global consensus.

Law must lead, not because it always prevails, but because without it a dangerous void emerges. Within that void lie risk, miscalculation, and impunity. Even imperfect law is preferable to no law at all.

Three principles are essential to guide the governance of emerging and disruptive technologies:

• **Anchoring restraint in law and ethics:** IHL must be reaffirmed, especially the Martens Clause and the concept of meaningful human control. The Martens Clause, first articulated in the 1899 Hague Convention, holds that even in the absence of a specific treaty, the principles of humanity and the dictates of public conscience remain binding. In legal gray zones, humanity must serve as the guiding compass. Humanitarian organizations such as the International Committee of the Red Cross (ICRC) have made clear that delegating lethal decision-making to machines crosses a moral red line. Civil-society initiatives, including the Stop Killer Robots campaign and the United Nations Institute for Disarmament Research (UNIDIR), are actively advocating preventive action before algorithms begin defining the rules of war.

• **Treating precedent as both power and caution:** Historical experience offers lessons. In 1995, the Convention on Certain Conventional Weapons (CCW) adopted a protocol banning blinding laser weapons before their first use in combat, an instance of law anticipating misuse. The Biological Weapons Convention (BWC), although lacking robust verification, has endured for five decades because it codifies an ethical consensus respected by states. These examples illustrate that legal frameworks need not wait for catastrophe; they can be implemented if

there is political will. In a divided world where consensus is elusive, progress must begin where possible. Soft law, transparency frameworks, and regional arrangements provide viable pathways that can mature into binding instruments.

• **Letting soft law pave the way:** Soft-law mechanisms, including declarations, voluntary moratoria, and national review processes, should not be dismissed as weak substitutes. They serve as strategic footholds. In an era when formal treaty-making is stalled, soft law shapes behavior, fosters transparency, builds trust, and clarifies red lines. This is not legal idealism but legal realism. When technological innovation outpaces diplomacy, soft law must form the floor, not the ceiling, of regulation. It provides a starting point for states that possess political will but lack the necessary leverage to forge binding rules.

Pakistan's Contribution to the Global Discourse

Pakistan brings considerable value to the international debate. The country has maintained a principled and strategically grounded position in discussions on emerging military technologies. In multilateral forums, such as the UN First Committee, the CCW, the Disarmament Commission, and the Conference on Disarmament, Pakistan's voice has remained consistent, responsible, and ethically clear.

In its April 2025 submissions to the UN Disarmament Commission and to the UN Secretary-General's report on the military applications of AI, Pakistan reaffirmed its stance. It cautioned against the unchecked expansion of algorithmic capabilities and advocated for a binding international instrument that prohibits fully autonomous weapons systems lacking meaningful human control.

Pakistan's position rests on four consistent principles:

• Opposition to the development and deployment of fully autonomous weapons operating without human oversight.

• Support for legally binding international rules and the progressive codification of humanitarian law.

• Defense of the right to peaceful uses of dual-use technologies.
• Demand for equity and inclusiveness in shaping international norms, not only for Pakistan but for the Global South as a whole.

These positions reflect legal reasoning as well as strategic foresight. The moment has come for Pakistan to move from principled advocacy to proactive leadership, shaping global norms and establishing itself as a constructive, future-oriented actor.

Practical Proposals for Pakistan

Four practical proposals offer realistic starting points for bridging the gap between technological innovation and governance:

• **Model protocol on military AI and lethal autonomous weapons systems:** Pakistan, together with like-minded states, could advance a model protocol with four objectives: prohibit fully autonomous systems that violate IHL; regulate compliant systems under strict spatial and temporal conditions; demonstrate that Pakistan is not opposed to innovation; and reaffirm that legality and human dignity remain non-negotiable.

• **Global legal observatory:** A normative hub, possibly under UN auspices, could monitor developments, track state practice, support capacity-building and national legal reviews, and issue advisory opinions, particularly assisting Global South states in interpreting complex challenges. Functioning as an IAEA or OPCW for emerging military technologies, such an observatory would promote clarity rather than control.

• **Regional restraint mechanisms:** Islamabad could spearhead a South Asian Code of Conduct on military AI to prevent misperception and unintended escalation. This could include commitments to retain human oversight in decision-making, voluntary transparency measures, and an instrument prohibiting deployment of fully

autonomous systems in crisis zones. Regional initiatives would complement, rather than replace, global agreements by grounding them in regional realities.

• **Institutionalizing national capacity:** Credibility abroad begins with capacity at home. Pakistan could institutionalize legal reviews under Article 36 of Additional Protocol I to the Geneva Conventions, establish inter-agency technical-legal teams led by the Ministry of Foreign Affairs, and partner with leading universities and research centers such as the Artificial Intelligence Technology Centre (AI Tech), the National Centre for Physics at Kaiser University, and the PF Centre for AI and Computing.

Towards a Norm-Shaping Role for Pakistan

Taken together, these steps can position Pakistan not merely as a participant but as a norm-shaping power in the governance of future warfare. The central challenge lies in the divergence between lawyers who seek rules, engineers who design code, and AI systems that rely on data.

History demonstrates that international law often follows war. The Non-Proliferation Treaty (NPT) emerged after Hiroshima; the Chemical Weapons Convention (CWC) after the horrors of chemical warfare. This time, the world cannot afford to wait. The imperative is not to ban innovation but to govern it. If future conflicts are governed by algorithms rather than human conscience, the international community risks abandoning one of its essential responsibilities: crafting rules that protect life even in the midst of war.

Pakistan must endeavor to shape that future, not out of fear of technology, but from confidence in the stabilizing power of law. The rules for governing EDMTs must be co-authored, not imposed; they must include the Global South as much as the Global North and involve technologists alongside jurists. This is not the time to ban innovation; it is the time to govern it wisely and collectively.

Emerging Technologies and the Future of Nuclear Arms Control

Dr. Olamide Samuel
Network Specialist – Open Nuclear Network

The nuclear deterrence relationship between India and Pakistan is entering a perilous new stage. Long-standing issues such as territorial disputes, asymmetric warfare, and domestic political pressures continue to strain bilateral relations. Layered with the influx of emerging technologies in both countries' arsenals, the picture becomes even more complex.

Both India and Pakistan are actively developing and acquiring technologies to gain a strategic edge, often using the other's advancements to justify their own. India's test of the Agni-5 ballistic missile and its development of new delivery systems, some potentially with Multiple Independently Targetable Reentry Vehicle (MIRV) capability, have not gone unnoticed in Islamabad. Pakistan, for its part, has pursued the MIRV-capable Ababeel missile and continues to diversify its nuclear deterrent. Both countries are now showing interest in integrating AI into military decision-support systems. Reports suggest India is aiming to use AI for improved targeting, while Pakistan will understandably attempt to keep pace, albeit on a more limited scale. If left unchecked, this escalating action-reaction cycle may evolve into a destabilizing arms competition that could erode the already fragile strategic stability of the region.

Global Implications and Urgency for Risk Reduction

The implications of this rapidly shifting deterrence dynamic extend beyond Pakistan and India alone. Studies into the long-term consequences of nuclear war in South Asia consistently show that a breakdown in deterrence would have catastrophic and potentially existential implications for the entire planet. This concern becomes even more pressing when considering the disruptive influence of emerging technologies on this fragile deterrence balance.

Urgent and practical measures are needed to mitigate the risks of a potential nuclear confrontation. The discussion therefore surveys viable options for nuclear risk reduction, arms control, and multilateral nuclear diplomacy that can help dampen the destabilizing effects of advanced technologies.

Case Study: The 2022 BrahMos Incident

The seriousness of the regional risk was underlined by the accidental Indian missile launch into Pakistan in March 2022. During routine maintenance, a BrahMos cruise missile was inadvertently launched and landed in Pakistani territory. Fortunately, the missile was unarmed and caused no casualties. Pakistan's response was measured and restrained, avoiding rash retaliation despite understandable alarm. The leadership assessed the situation and determined that the event was an accident, responding diplomatically rather than militarily.

The situation could, however, have unfolded very differently had the missile struck a sensitive target or resulted in casualties. Notably, India did not immediately utilize military hotlines to inform Pakistan, creating a dangerous period of ambiguity. The incident stands as a stark warning: technical malfunctions or miscommunications in a nuclear environment can have devastating consequences.

Future incidents could occur in a more complex operational environment where AI-generated intelligence and potential cyber interference further cloud decision-making. In such a scenario, clarity and restraint may be compromised. Key questions, therefore, arise: would decision-makers be able to differentiate between accidents and aggression in time? Could a technical malfunction be mistaken for a preemptive strike? These remain pressing questions for regional security.

Existing Confidence-Building Measures: Progress and Gaps

Risks are exacerbated by the geographical proximity of India and Pakistan and the hair-trigger readiness of their nuclear forces. Missile flight times across the border are only a matter of minutes, leaving little

room for hesitation or error. While there have been efforts to institute CBMs, the record is mixed.

Both nations have agreed to pre-notify each other of ballistic-missile tests, a useful measure. However, this agreement does not extend to cruise-missile or hypersonic-weapon tests, a significant gap, particularly in light of the 2022 incident. Additionally, both sides annually exchange lists of nuclear facilities and commit not to target them, a reassuring gesture, yet many other CBMs have stalled.

India has shown reluctance to engage in sustained dialogue with Pakistan. Meetings of the Joint Committee on Nuclear CBMs, stipulated by prior agreements, have not been consistently held. This situation breeds complacency: each crisis that passes without escalation may create a false sense of confidence. Close calls, from the 1999 Kargil conflict to the 2019 Balakot airstrikes, illustrate how quickly the situation can deteriorate.

Direct communication between the Indian and Pakistani leadership remains minimal. Misperceptions are widespread, and mutual trust is severely lacking. Yet paradoxically, it is precisely when political relations are strained that risk-reduction measures are most crucial in preventing accidents, misunderstandings, or inadvertent escalation.

Recommendations: A Constructive Path Forward

With the above in mind, a set of constructive and diplomatically sensitive recommendations is warranted to support nuclear risk reduction in South Asia.

- **Strengthen and modernize communication channels.** Real-time crisis communication requires active, reliable, and updated mechanisms. In addition to maintaining the Director General of Military Operations (DGMO) hotline, a secure line dedicated to nuclear and high-tech emergencies should be established. In the event of an incident akin to 2022, emergency protocols should mandate immediate notification with maximum available data, trajectory, system type, and

presumed cause to reassure the other side. A direct line between the two national command authorities could be considered, potentially mediated by a neutral party, for use when nuclear risks emerge in a crisis. Communication remains the least costly CBM, demanding political will yet yielding outsized dividends by dispelling confusion and buying time during fast-moving situations.

- **Expand pre-notification agreements to new domains.** The existing ballistic-missile test pre-notification regime should be expanded to include cruise-missile tests, hypersonic glide-vehicle launches, and long-range autonomous or unmanned systems. Inclusion would reduce surprise and signal benign intent.
- **Revive and widen exercise notifications.** Reciprocal notification of major military exercises, especially those involving strategic forces or new-technology demonstrations, should be revitalized under prior CBM frameworks. Such steps would help prevent misreading routine activities as provocations.

Pakistan does not exist in a vacuum; its deterrent relationship has security implications for its neighbors, the sub-region, and the entire planet. In the keynote address, General Sahil Mirza of the Joint Chiefs of Staff Committee (JCSC) affirmed that Pakistan is a responsible nuclear-weapon state, highlighting long-standing support for universal, non-discriminatory conventions on nuclear disarmament and championing a convention on negative security assurances. In recent statements at the Conference on Disarmament (CD), it was underscored that Pakistan's nuclear deterrent is need-driven rather than prestige-driven.

Global Perception, Scientific Knowledge, and Pakistan's Role in Multilateral Nuclear Diplomacy

Despite long-standing aspirations for regional stability, global concern is growing that a failure of deterrence in South Asia could trigger a catastrophic global nuclear winter. Several scientists and disarmament advocates, primarily from Western countries, consistently highlight South Asia as the region most likely to witness nuclear conflict. This perception has generated a significant reputational challenge, with the current deterrence dynamic increasingly viewed as prioritizing the strategic needs of one or two countries over the survival of the broader international community, irrespective of legitimate security concerns detailed in recent dialogues.

Given this context, it is timely for Pakistan to reconsider the prevailing narrative and adopt a more proactive stance in multilateral nuclear diplomatic engagements. The shift should extend beyond traditional forums such as the CD. Pakistan's track record of active participation provides a foundation for expanded engagement.

This broader engagement is necessitated not only by the rapid pace of technological evolution but also by concurrent developments in multilateral legal mechanisms, which are increasingly informed by new scientific knowledge. These mechanisms may significantly influence the future direction of nuclear-deterrence policies and practices.

Scientific understanding of the consequences of nuclear-weapons use is vital for effective arms control. Advances in computing power, climate modeling, and environmental sciences now enable more accurate assessments of the effects of nuclear warfare. The last UN-mandated study on the impacts of nuclear war was conducted in 1988. Since then, higher-resolution models have markedly improved simulations of atmospheric effects, including the spread of soot and dust, and the cascading environmental and humanitarian consequences of nuclear conflict.

Recognizing this gap, the Scientific Advisory Group of the Treaty on the Prohibition of Nuclear Weapons (TPNW) recommended in 2023 that the UN commission a fresh assessment of the global impacts of nuclear war using contemporary scientific tools and methodologies. In November of that year, a resolution was adopted to establish an independent scientific panel tasked with evaluating the effects of nuclear war.

The resolution received overwhelming international support, with 144 countries voting in favor, 30 abstaining, and three opposing. Among the nuclear-armed states, France, the United Kingdom, and Russia voted against; Pakistan and India abstained; China voted in favor. The voting pattern reveals an important insight: scientific data concerning the humanitarian and environmental impacts of nuclear war is increasingly seen as a challenge to the traditional framework of nuclear deterrence. Nevertheless, embracing such data may open a new avenue for strategic restraint and credibility.

Therefore, aligning with evolving scientific discourse, alongside China, could represent a strategic and reputational opportunity for Pakistan as it seeks to further solidify its position as a responsible nuclear-armed state. Engagement with emerging scientific assessments of nuclear war may provide the intellectual and diplomatic foundations for fostering greater restraint and stability in the South Asian sub-region.

Question Answer Session

Q. How can a comprehensive ban on fully autonomous weapon systems be verified when many platforms already carry advanced software, dual-mode (human/auto) capability is proliferating, and autonomous armored deployments have been reported in Ukraine?

A. Verification is not currently feasible because there is no universally accepted definition of "full autonomy." Without agreed, testable criteria (e.g., functional thresholds, control modes, auditing standards), a verification regime cannot be designed or enforced. Historically, major arms-control verification, especially for WMD, has only been negotiated once technologies plateau or achieve stable operational integration, and when states bargain from technological/military strength or at a strategic equilibrium. Neither condition exists today for lethal autonomous weapon systems.

Q. Given that emerging technologies differ fundamentally from past innovations, how can they be effectively governed under international frameworks?

A. Governance should start by identifying the specific functions and lifecycle stages that require oversight, then tailoring instruments to those points. The binding constraint is not technical feasibility but political will: without it, no regime endures. Once political commitment is secured, empowered technical experts can design viable mechanisms, definitions and scope, reporting and transparency rules, auditing and testing protocols, export and use controls, and compliance/enforcement measures. Today's challenges are not unprecedented; in the 1960s, a U.S.-Soviet arms control regime appeared implausible amid profound technical and political barriers, yet determined leadership produced durable agreements. History shows that where political will exists, workable regulatory solutions follow.

Q. How can it be ensured that emerging technologies are not misused to hinder or block the development of certain countries? How can a fair and balanced system be created that includes all states equally?

A. While the notion of a fair and balanced system is widely acknowledged as ideal, the current international environment remains driven by national interests. In such a system, each state tends to act in its own strategic interest. Therefore, it becomes imperative for countries to invest in the independent development of emerging technologies, even if the process is lengthy and resource intensive. Self-reliance in technological innovation offers the most viable safeguard against exclusion or marginalization.

Q. What are China's views on developing its own political declaration on responsible military AI use, especially in the nuclear domain, given its non-signature of the U.S. declaration and the REAIM blueprint, while Pakistan has endorsed a joint statement?

A. China's position is anchored in the principle of "AI for good": AI must serve constructive, peaceful purposes, with strict red lines in sensitive military and nuclear domains. In 2023, China convened an international AI conference in Shanghai, attended by Premier Li Qiang, which released policy documents detailing the ethical and responsible use of AI; these documents are publicly available on the Ministry of Foreign Affairs website. Further multilateral engagement is anticipated, with a follow-up conference tentatively planned for summer 2025 in Shanghai, open to global scholars and experts. China's approach emphasizes dialogue-driven, internationally accessible processes as the avenue to shape future AI governance mechanisms, including restraint and risk-reduction principles relevant to nuclear command-and-control contexts.

Conclusion

Framed by the recognition that nuclear stability is increasingly shaped by developments in artificial intelligence, cyber capabilities, and space systems, the conference offered a timely reflection on the complex challenges and opportunities facing global and regional security today.

The keynote address by General Sahir Shamshad Mirza set the strategic tone of the conference. Describing the international landscape as one of "fluid multipolarity," he observed that emerging regional powers are increasingly asserting themselves, often at the expense of multilateral cooperation and economic interdependence. He warned of the erosion of established security architectures and the reemergence of nuclear modernization, compounded by the integration of AI, autonomous systems, and space capabilities into military doctrines. These developments, he argued, not only complicate crisis stability but also reduce the margin for human judgment in nuclear command and control.

In a special session on the second day, Former Chairman Joint Chiefs of Staff Committee, General Zubair Mehmood Hayat, discussed the emergence of multi-domain deterrence, a concept previously absent from strategic calculations, and how it presents a new and complex challenge to the existing global security architecture. He highlighted an alarming truth that India is the only nuclear-armed state governed by an extremist ideology whose strategic behavior is unfolding across three dimensions – ideological, political and technological. The BJP, the political wing of RSS, promotes forced Hindu nationalism. Yet, the world chooses silence. Why? India is a large country, and the West's focus is fixated on containing China. These are the double standards, and they pose a danger to global peace and stability. He emphasized that India today possesses the fastest-growing nuclear program in the world and has remained the largest arms importer for over a decade. India's missile development program is increasingly signaling its military ambitions. Former CJCSC also stated that "India is no longer 'India,' it is now 'Bharat, ' and this is not just a name change – it is a

signal. When the Indian Prime Minister attends international forums and sits behind a nameplate that reads "Bharat," it reflects a more profound ideological shift from the secular liberal democracy of India to a Hindu Rashtra.

Against this backdrop, the sessions that followed offered a wide-ranging and multidisciplinary engagement with the key questions shaping the future of nuclear deterrence.

The conference demonstrated the role of CISS as an inclusive platform for dialogue on complex security challenges at the intersection of emerging technologies and nuclear deterrence. By convening a diverse set of global voices across disciplines, regions, and policy perspectives, the conference facilitated informed exchanges on the risks, gaps, and opportunities shaping strategic stability in a rapidly evolving environment. The discussions underscored the urgent need for anticipatory governance, ethical responsibility, and multilateral engagement to ensure that technological innovation supports rather than undermines global and regional security.

Photo Gallery


CISS In
CLEAR


CISS
CISS International Conferen
on
NUCLEAR DETERRENCE IN THE A
EMERGING TECHNOLOGIES
22-23 April 2025


NUCLEA
CISS
CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING TECHNOLOGIES


CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING


EMERGING


ALL THE TH
THAT COUL
HAPPEN NE


EM GING





on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING TECHNOLOGIES



ational Conference



EMER


CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING TECHNOLOGIES


CISS International Conference
on
EMERGING TECHNOLOGIES
22-23 April 2025


EAR DETERR
EM GING


CISS International Conferenc
on


CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING TECHNOLOGIES


CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING TECHNOLOGIES


CISS International
on


CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING TECHNOLOGIES


EAR DETE
EM GIN


RENCE IN
TE NO


CISS International Confer
on
UCLEAR DETERRENCE IN
EM NG TECH


rnational Conference
on
THE AGE OF


Nuclear Deterrence, New
Technologies and Great
Power Competition


CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
CISS International Conference
on
NUCLEAR DETERRENCE IN THE AGE OF
EMERGING TECHNOLOGIES