THE 28TH ASEAN REGIONAL FORUM HEADS OF DEFENCE UNIVERSITIES, COLLEGES AND INSTITUTIONS MEETING (ARF HDUCIM)

NAVIGATING THE TECHNOLOGICAL HORIZON: BALANCING INNOVATION, RISK, AND LEADERSHIP IN PAN-DOMAIN OPERATIONS BY LT GEN DATUK WIRA ARMAN RUMAIZI BIN HJ AHMAD, VICE CHANCELLOR, NATIONAL DEFENCE UNIVERSITY OF MALAYSIA (NDUM)

Executive Summary

The rapid evolution of emerging technologies, such as Artificial Intelligence (AI), the Internet of Things (IoT), robotics, big data analytics, and quantum capabilities, is fundamentally transforming modern warfare and security dynamics. As armed forces transition toward Pan-Domain Operations (PDO) and Multi-Domain Operations (MDO), integrating capabilities seamlessly across land, sea, air, cyber, space, and information environments, Professional Military Education (PME) institutions must evolve. This paper presents the perspective of the National Defence University of Malaysia (NDUM) on evaluating the opportunities and systemic risks of frontier technologies, defining essential leadership competencies for future commanders, and detailing how PME frameworks must adapt to ensure strategic agility and ethical oversight.

1: Introduction

The contemporary global security environment is undergoing a fundamental transformation driven by the rapid convergence of disruptive technologies, shifting geopolitical dynamics, and the multi-dimensional nature of modern conflict. As armed forces across the globe pivot toward Pan-Domain Operations (PDO) and Multi-Domain Operations (MDO), the seamless integration of capabilities across traditional operational spheres - land, sea, and air- with non-traditional domains (cyber, space, and the information environment) has become a prerequisite for strategic decision advantage. At the core of this transition lies the proliferation of emerging technologies, including artificial intelligence (AI), autonomous robotic systems, the Internet of Things (IoT), big data analytics, and quantum capabilities.

While technological innovation is not inherently novel to military affairs, the current velocity, scope, and complexity of technological change present unprecedented challenges to command structures, institutional adaptability, and strategic governance. The primary mandate of modern defence establishments is no longer limited to acquiring advanced physical platforms; rather, it centres on how military personnel think, decide, collaborate, and innovate under conditions of high uncertainty and rapid data expansion. In this context, Professional Military Education (PME) institutions bear a vital responsibility in shaping officers who are not only technically proficient but also strategically agile and morally grounded. From the perspective of the National Defence University of Malaysia (NDUM) and the broader framework of Association of Southeast Asian Nations (ASEAN) security cooperation, this paper examines the dual-edged nature of emerging

technologies, defines the critical leadership competencies required for pan-domain environments, outlines NDUM's educational approaches, and emphasises the necessity of regional confidence-building to preserve stability across the Indo-Pacific.

2: Opportunities and Risks of Emerging Technologies in Defence

2.1 Operational Opportunities for Decision Advantage and Domain Integration

Emerging technologies offer transformative capabilities that can significantly enhance military operational effectiveness and strategic deterrence. Chief among these advantages is the dramatic acceleration of command decision-making cycles through AI-assisted decision-support tools and big data analytics. By synthesising massive, disparate streams of real-time intelligence from satellite networks, uncrewed sensors, radar systems, and open-source data, AI algorithms enable commanders to achieve comprehensive Domain Awareness and make rapid, evidence-informed decisions under conditions of friction.

Furthermore, the deployment of Internet of Things (IoT) architectures and autonomous robotic systems enhances joint force integration and risk mitigation. Uncrewed aerial, surface, and sub-surface platforms can conduct high-risk surveillance, mine countermeasures, and reconnaissance missions in contested maritime and land environments without putting human lives directly in harm's way. In complex operational contexts, such as safeguarding vast maritime zones and critical sea lines of communication, these networked, autonomous systems provide continuous monitoring and scalable response capabilities, reinforcing national defence postures while maintaining operational efficiency.

2.2 Systemic Vulnerabilities and Ethical Risks

Concurrently, the integration of frontier technologies introduces significant vulnerabilities and ethical dilemmas that demand rigorous evaluation. A primary risk involves the potential erosion of human oversight in automated decision-making processes. The absence of meaningful human judgment in target identification or automated kinetic responses introduces severe ethical risks, including the potential violation of International Humanitarian Law (IHL), unintended collateral damage, and rapid, uncontrolled escalation during crises.

In addition, algorithmic systems remain susceptible to machine learning biases, data poisoning, and false correlations, which can lead commanders to misinterpret strategic indicators. Hyper-connected pan-domain architectures also dramatically expand the offensive attack surface. Adversaries exploiting hybrid, grey-zone, and coercive tactics can launch cyber intrusions, electronic spoofing, and manipulation of the information environment to disrupt automated command networks. Over-reliance on brittle technological systems without resilient manual back-ups creates systemic single-point vulnerabilities that can be paralysed in contested environments.

3: Required Leadership Competencies for Pan-Domain Operations

3.1 Technological Literacy and Data Fluency

Operating effectively within a pan-domain battlespace requires a fundamental redefinition of military leadership competencies. Future commanders do not need to be computer programmers, but they must possess robust technological literacy and data fluency. Leaders must understand the underlying logic, operational boundaries, processing limits, and security vulnerabilities of AI models, autonomous systems, and sensor networks. This technical awareness enables leaders to interrogate algorithmic recommendations critically rather than accepting machine outputs with blind confidence.

3.2 Cognitive Agility, Moral Resilience, and Ethical Judgment

Equally essential is the cultivation of cognitive agility and moral resilience. In pan-domain environments, decision-makers are subjected to unprecedented cognitive loads, receiving overwhelming volumes of simultaneous inputs across physical and non-physical domains. Leaders must cultivate the intellectual flexibility to filter noise, extract signal, and evaluate non-military variables, such as diplomatic, economic, legal, and public perception factors, while under severe time pressure. Crucially, commanders must retain moral responsibility, exercising ethical judgment where automated systems lack contextual nuances, human empathy, and strategic intuition.

4: Modernising Professional Military Education: The NDUM Framework

4.1 Fusing Science, Strategy, and Moral Leadership

To cultivate these multi-dimensional leadership competencies, PME institutions must evolve beyond legacy instructional methodologies. As Malaysia's premier defence university, NDUM integrates rigorous academic education with professional military training from the Military Training Academy of the Malaysian Armed Forces. NDUM's educational philosophy rests on combining technical disciplines, such as computer engineering, cybersecurity, defence technology, and maritime systems, with strategic studies, international law, and defence management.

Through this interdisciplinary model, student officers examine emerging technologies not in isolation, but within their broader geopolitical, legal, and operational contexts. Engineering and technology courses emphasise ethical system design and cyber resilience, while command and strategy programs incorporate modules on algorithmic warfare and ethics in autonomous systems. This dual focus ensures that technological innovation remains anchored in moral clarity, national responsibility, and institutional integrity.

4.2 Advanced Synthetic Environments, Wargaming, and Simulation

NDUM places high strategic priority on modernising instructional delivery through advanced synthetic learning and wargaming environments. Traditional classroom instruction is augmented

by multi-domain simulation laboratories where student officers encounter complex, simulated pan-domain scenarios.

These exercises are designed to intentionally expose officers to technological failures, including cyber blackouts, GPS spoofing, and degraded communications. By forcing future leaders to command under conditions of severe electronic disruption and algorithmic uncertainty, NDUM fosters cognitive resilience, problem-solving agility, and the ability to revert seamlessly to tactical initiative when technology fails. Furthermore, NDUM bridges academia, government, and the defence industrial sector in the Triple-Helix Model outlined in our National Defence Industry Policy (DIPN), fostering a whole-of-society approach to national resilience and technological innovation.

5: Promoting Regional Stability and Trust: The ASEAN Imperative

5.1 ASEAN Centrality and the ASEAN Outlook on the Indo-Pacific

In addressing the strategic impacts of emerging technologies, technological adoption must be aligned with the core principles of the ASEAN Regional Forum (ARF) and the ASEAN Outlook on the Indo-Pacific (AOIP). ASEAN's strength lies in its commitment to ASEAN Centrality, non-alignment, dialogue, mutual trust, and the peaceful settlement of disputes. As major powers compete for technological dominance, Southeast Asian nations must ensure that emerging technologies are harnessed to promote regional stability rather than provoke regional arms races or heighten strategic friction.

Defence diplomacy plays a central role in mitigating technological risks. Participating in multilateral forums such as the ARF HDUCIM, the ASEAN Defence Ministers' Meeting (ADMM), and ADMM-Plus allows member states to engage in open dialogue, enhance transparency, and prevent misunderstandings regarding military technology deployments.

5.2 Collaborative Governance, Capacity-Building, and Norm-Setting

Regional defence universities must serve as collaborative engines for confidence-building and policy development. ARF institutions should work together to formulate shared regional frameworks and ethical norms governing the military applications of AI and autonomous platforms. Joint research initiatives, faculty exchanges, and combined wargaming seminars among ARF defence colleges can help establish common terminologies, harmonise risk-assessment protocols, and enhance regional cyber resilience. By promoting shared capacity-building, ASEAN and its dialogue partners can ensure that technological modernisation serves as a force multiplier for collective security, humanitarian assistance, and regional peace.

6: Conclusion

The emergence of frontier technologies in defence presents both transformative opportunities and complex operational risks. As militaries transition toward Pan-Domain Operations, achieving enduring security requires more than sophisticated software and hardware; it demands educated,

adaptive, and ethically grounded military leaders. The National Defence University of Malaysia remains committed to advancing Professional Military Education that fuses technical competence with strategic wisdom and moral responsibility. By fostering regional dialogue, establishing shared ethical norms, and strengthening cooperative frameworks through the ASEAN Regional Forum, we can collectively navigate the technological horizon to safeguard regional peace, stability, and prosperity across the Indo-Pacific.