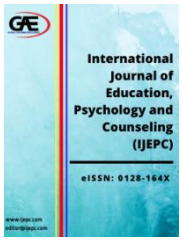
International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049



INTERNATIONAL JOURNAL OF EDUCATION, PSYCHOLOGY AND COUNSELLING (IJEPC)
www.ijepc.com

DEFENDING ON ALL FRONTS: INTEGRATING THE THREAT RESPONSE MODEL INTO MULTI DOMAIN OPERATIONS

Hasmady Alim[1]

[1] Faculty of Defences Studies and Management, National Defence University of Malaysia
Email: hasmadyalim@gmail.com

Article Info:

Article history:
Received date: 14.04.2025
Revised date: 27.04.2025
Accepted date: 24.08.2025
Published date: 17.09.2025

To cite this document:

Hasmady, A. (2025). Defending On All Fronts: Integrating the Threat Response Model into Multi Domain Operations. *International Journal of Education, Psychology and Counseling, 10* (59), 675-682.

DOI: 10.35631/IJEPC.1059049

Abstract:

The complexity of modern military operations necessitates innovative approaches to threat response models, particularly for nations like Malaysia facing diverse and evolving challenges. This article highlighted the integration of the Threat Response Model into Multi-Domain Operations (MDO) to enhance readiness, adaptability, and effectiveness. By aligning detection, assessment, and response capabilities across land, air, maritime, cyber, space, and information environments, the Malaysia Armed Forces (MAF) and other joint forces can achieve strategic and operational superiority in an increasingly complex battlespace. By addressing the unique requirements of the MAF, this model provides a foundation for future research and practical implementation. The article concludes, by adopting a threat response modal in multi-domain approach, aiming to support the modernization and adaptability of the MAF in response to contemporary modern warfare.

Keywords:

Military Operations, Multi-Domain Concept, Malaysian Armed Forces, Forces Response Model

Introduction

The evolving landscape of military operations demands a concept for future operations environments becoming modernizations strategy for addressing complex and multi-faceted threats. Traditional single-domain approaches often fall short in the face of modern security challenges, which are increasingly interconnected and multi-dimensional (Joyce et al., 2024; Morgan-Owen et al., 2024; Schüler & Matuszczyk, 2019: Grossman et al., 2007). For nations like Malaysia, the need for a comprehensive and integrated threat response model is paramount, given its unique geopolitical landscape and security priorities. Malaysia's strategic position in Southeast Asia exposes it to a range of challenges from border security issues and maritime

International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049

disputes to cyber threats and hybrid warfare necessitating a comprehensive approach to safeguarding its concentric defence areas: Core, Extended, and Forward (Ministry of Defence, 2020).

Figure 1 illustrates Malaysia's concentric defence layers: the Core Area comprises the nation's land masses, territorial waters, and the airspace above them; the Extended Area includes the Malaysian Maritime Zone (MMZ), strategic waterways, airspace, and critical lines of communication. The Forward Area extends beyond these zones to locations where Malaysia's national interests may be affected. The Malaysian Armed Forces (MAF) must address emerging threats within this layered framework, recognising the interconnected nature of these defence domains.

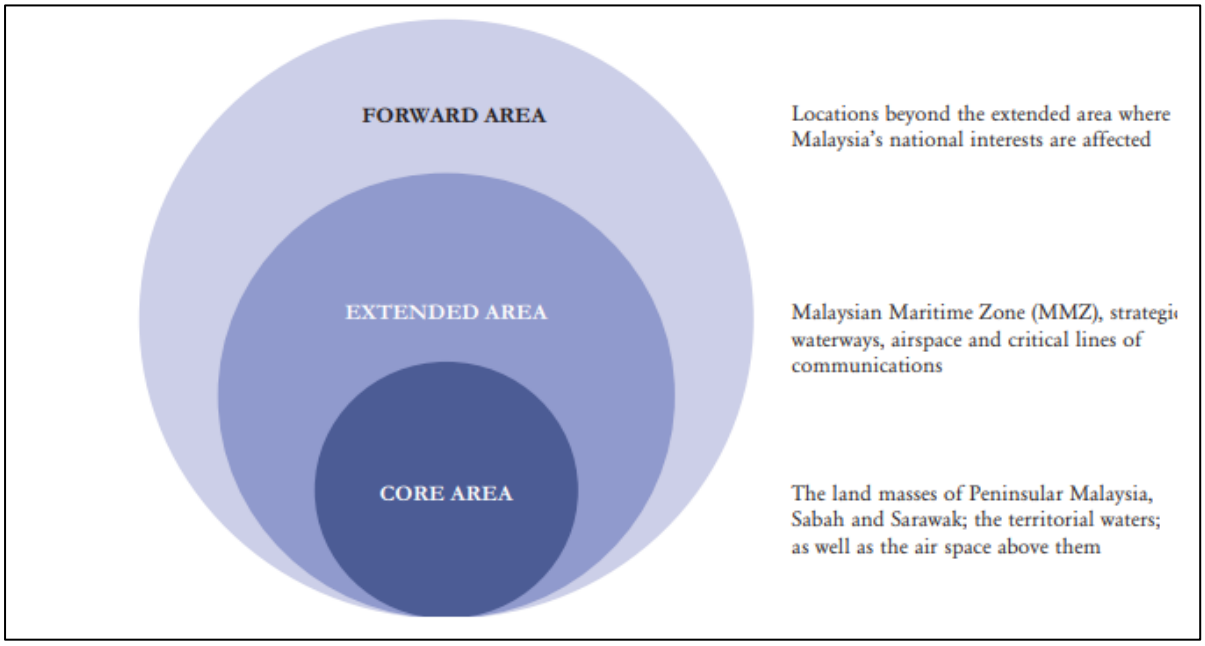


Figure 1: Malaysia Concentric Areas (Ministry of Defence, 2020).

This calls for an innovative approach that transcends the limitations of single-domain strategies and embraces a Multi-Domain Operations (MDO) concept. This article explains the concept of the Threat Response Model tailored to the Malaysian Armed Forces (MAF), emphasizing its relevance in supporting Multi-Domain Operations (MDO) by enhancing coordinated responses across land, air, maritime, cyber, and space domains. By integrating operations across land, air, sea, cyber, and space domains, this approach aims to enhance the MAF's ability to address both conventional and non-conventional threats. The Threat Response Model offers a strategic roadmap for the MAF to enhance resilience and adaptability in addressing evolving military threats, aligning with strategic needs and practical operational demands.

Strategic Need For Forces Response In the Malaysian Armed Forces

Malaysia's unique geopolitical position and security landscape necessitate a shift towards multi-domain threat response strategies (Ministry of Defence, 2020). The country faces a variety of challenges, including border security concerns, maritime disputes, cyber vulnerabilities, and hybrid warfare. These challenges are often interconnected, requiring a comprehensive and synchronized approach to address them effectively. Malaysia's extensive land and maritime borders make it vulnerable to threats such as illegal crossings, smuggling,

International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049

and infiltration by hostile elements. Traditional land or maritime strategies cannot often fully address these issues. A multi-domain approach integrates ground forces, naval patrols, and aerial surveillance to create a cohesive border security system. Cyber capabilities can also play a role in monitoring communications and detecting patterns of illegal activities.

The South China Sea remains a significant area of strategic interest for Malaysia, with overlapping territorial claims and increasing naval activity. Protecting maritime sovereignty requires the MAF to leverage a combination of naval strength, air reconnaissance, and satellite surveillance. Multi-domain operations can enhance situational awareness and enable a coordinated response to potential incursions or disputes.

As Malaysia continues to modernize, its reliance on digital infrastructure increases, making it a target for cyberattacks on critical systems. A multi-domain approach integrates cyber defense with traditional military strategies, ensuring that digital vulnerabilities are addressed alongside physical threats. Proactive measures, such as real-time threat detection and offensive cyber capabilities, can mitigate potential risks.

Non-conventional threats, including terrorism, insurgency, and information warfare, present significant challenges to national security. These threats often blur the lines between military and civilian targets, requiring a flexible and adaptive response. Multi-domain operations enable the MAF to address hybrid warfare by coordinating efforts across all domains, leveraging intelligence networks, and deploying rapid-response teams where needed. By addressing these strategic needs, the MAF can strengthen its operational readiness and resilience, ensuring that it remains prepared to counter a wide range of threats. The next section details the proposed multi-domain threat response concept and its practical application.

Malaysia's comprehensive approach to national defence is reflected in the strategic alignment of its vision, interests, and objectives (Ministry of Defence, 2020). As illustrated in Figure 3.1, the National Defence Vision, Interests, and Objectives emphasize the country's unwavering commitment to safeguarding security, sovereignty, and prosperity. The framework outlines key priorities, including the development of multi-domain capabilities, the enhancement of internal resilience, the advancement of the defence industry, and the promotion of good governance. By focusing on these pillars, Malaysia demonstrates a coherent and proactive strategy to strengthen its defence posture and uphold national interests through transparency, accountability, and innovation.

International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049

Figure 2: The Malayia Defence Vision, Interests, and Objectives (Ministry of Defence, 2020).

Multi-Domain Operations Concept

Wesley & Bates, (2020) proposed a framework for overcoming the challenges of future operational environment by suggested that a military concept need to be identify to respond multiple threats. This process involves developing a clear concept of how the Army must operate to counter these threats, analyzing and assessing capability requirements, and formulating a strategy to modernize the Army. Multi-domain operations (MDO) concept represents a paradigm shift in military strategy, emphasizing the integration of capabilities across multiple operational domains to achieve strategic objectives (Takabatake, 2024, Schauer et al., 2023; Walsh et al., 2023; Lindsay & Gartzke, 2022; Gans & Rogers, 2021). This concept acknowledges that modern warfare is no longer confined to individual domains but instead requires a comprehensive approach to counter increasingly interconnected and dynamic threats. MDO is deeply rooted in systems theory, which emphasizes understanding how different components interact within a complex system. In a military context, each domain is viewed as part of an interconnected system where actions in one area can have cascading effects on others.

The concept of Multi-Domain Operations (MDO) is built upon several key principles. Clas (2018) introduces the concept by emphasizing that comprehensive integration enables seamless coordination across the land, air, maritime, cyber, and space domains. Zhu et al. (2022) further underscore that situational awareness enhanced through advanced technologies such as artificial intelligence and satellite systems facilitates real-time threat detection and analysis. Borne (2019) highlights interoperability as a critical enabler, promoting seamless collaboration across units and operational domains. Together, these principles enhance operational efficiency and mission effectiveness, ensuring a unified and adaptive response to complex and evolving threats.

International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049

As illustrated in figure 3, the concept of MDO aligns with contemporary modernizations strategy propose by Wesley & Bates (2020). By applying this concept, the MAF can position itself as a forward-thinking and future-ready force, capable of addressing the complex challenges of modern warfare. The specific strategic imperatives that justify the adoption of the MDO with threat response model within the MAF emphasise the need for integrated capabilities to address evolving and complex security challenges.

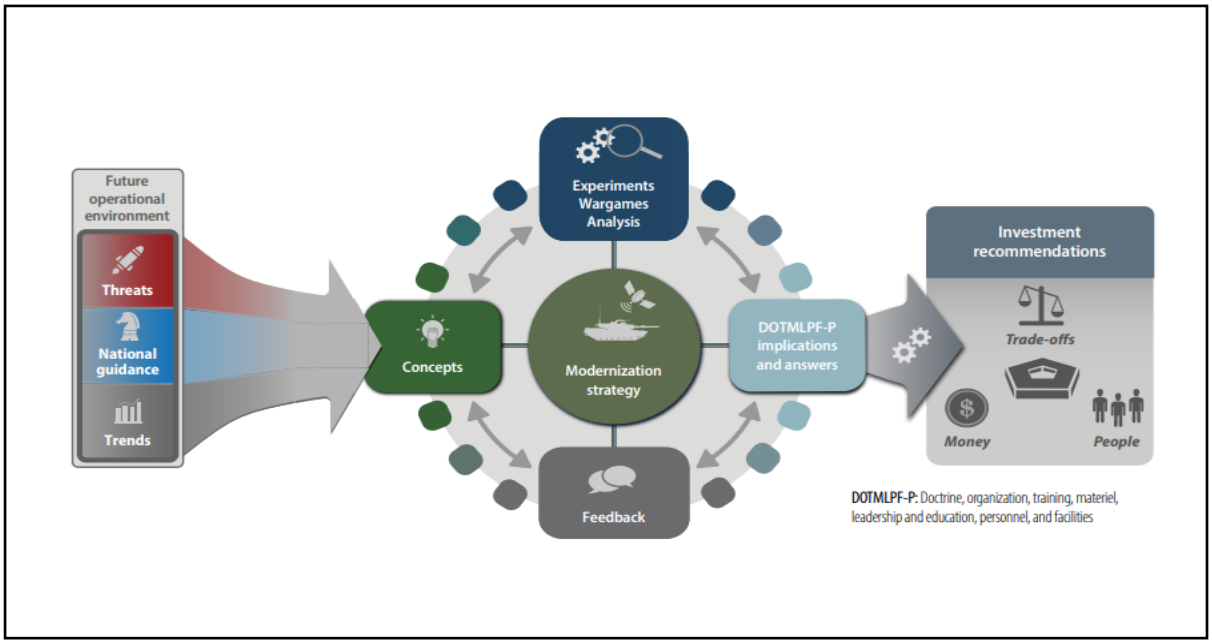


Figure 3: Army Modernization Framework (Wesley & Bates, 2020).

Integrating The *Model Tindak Balas Angkatan* (MTBA) Into Multi Domain Operations

The *Model Tindak Balas Angkatan* (MTBA) or Forces Response Model (FRM) offers a structured and layered approach to addressing security threats that may affect Malaysia's national interests. It aligns closely with the concept of concentric defence areas Core, Extended, and Forward ensuring that responses are tailored to the proximity and intensity of emerging threats. Threat response model for the Malaysian Armed Forces (MAF) emphasizes the seamless integration of capabilities across land, air, sea, cyber, and space domains.

The concept prioritizes the integration of resources and capabilities across all five domains, starting with the land domain, which focuses on strengthening ground operations through advanced mobility systems, real-time intelligence, and modernized infantry equipment. This approach is designed to enhance operational readiness, improve situational awareness, and enable coordinated responses to a wide range of security threats. The air domain leverages superior airpower for reconnaissance, rapid response, and close air support to ground and naval units. For the sea domain, the focus is on enhancing naval capabilities for maritime security and sovereignty, including advanced vessels and unmanned underwater systems. The cyber domain emphasizes establishing robust cyber defense mechanisms and offensive cyber capabilities to protect and exploit digital infrastructure. Finally, the space domain utilizes satellite technology for communication, navigation, and intelligence gathering to support multi-domain operations.

International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049

Key operational components of the concept include detection and awareness, which involve deploying advanced sensors, drones, and intelligence networks to achieve real-time situational awareness and early threat detection (Plevnik & Vuk, 2025). Coordination and command are also critical, with unified command structures ensuring synchronized decision-making and resource allocation across domains. Execution, the final component, focuses on mobilizing multi-domain assets in a coordinated manner to neutralize threats effectively and efficiently. This comprehensive integration and operational focus will enable the MAF to address evolving threats and maintain a strategic advantage in an increasingly complex security environment. Figure 5.0 illustrates the integration of the Threat Response Model into the Multi-Domain Operations (MDO) concept.

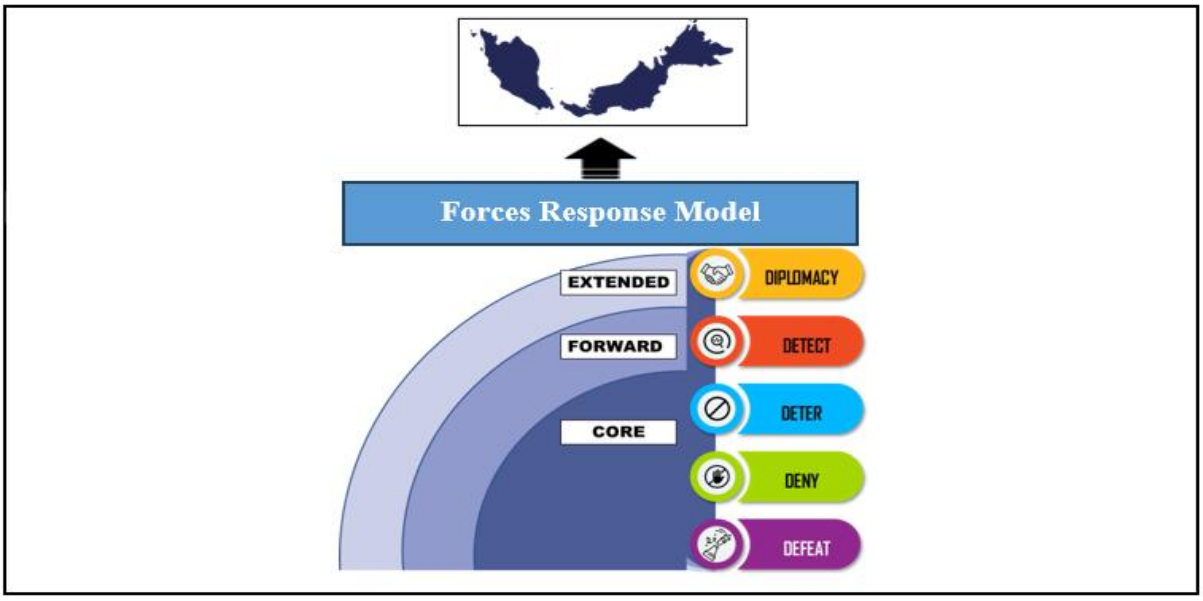


Figure 5.0: Forces Response Model.

The success of the concept relies on several critical enablers (Suleiman & Omojuwa, 2025; Monoranu, 2025; Mader et al., 2024; Pasdar, et al., 2024; Sahu, et al., 2024). Technological advancement is a priority, with investments in cutting-edge technologies such as artificial intelligence, machine learning, and autonomous systems to enhance operational capabilities. Training and development are equally important, with specialized programs designed to equip personnel with the skills required for multi-domain operations. Finally, strong leadership and clear doctrinal guidelines are essential to ensure consistent and effective implementation of the multi-domain strategy.

Conclusion

The integration of the Forces Response Model (FRM) with Multi-Domain Operations provides a critical edge in enhancing modern military readiness. By aligning detection, assessment, and response mechanisms across land, air, maritime, cyber, space, and information domains, armed forces are better positioned to respond to emerging threats with agility, precision, and cohesion. This unified approach ensures that threats are identified early, prioritized accurately, and addressed through synchronized operations, enabling a faster and more effective decision-making process across the chain of command.

International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049

For the Malaysia Armed Forces (MAF), adopting the Forces Response Model for Multi-Domain Operations (FRM-MDO) offers a forward-leaning strategy to confront evolving and hybrid security challenges. This model strengthens situational awareness and supports the development of cognitive readiness among military personnel across services. By leveraging domain convergence, interoperable command structures, and adaptive leadership principles, the MAF can achieve operational dominance and strategic deterrence in complex, ambiguous, and rapidly changing operational environments.

Acknowledgement

The authors would like to express their sincere appreciation to the Malaysian Armed Forces (MAF) for their valuable support and the provision of relevant information that contributed to this work. The views and opinions expressed in this article are solely those of the authors and do not necessarily reflect the official policy or position of the Malaysian Armed Forces (MAF) or the Government of Malaysia.

References

Borch, O. J., & Heier, T. (2024). Toward a hybrid threat response model. *Preparing for Hybrid Threats to Security*, 271.

Borne, M. K. D. (2019). Targeting in multi-domain operations. *Military Review*, *99*(3), 60-67.

Carter, B., & Fay, E. M. (2019). Responding to terror: An empirical analysis of US military activity, public opinion, and transnational terrorism. *Journal of Applied Security Research*, *14*(2), 140-168.

Clas, A. M. (2018). Commanding in multi-domain formations. *Military Review*, *98*(2), 91-99.

Gans, N. R., & Rogers, J. G. (2021). Cooperative multirobot systems for military applications. *Current Robotics Reports*, *2*, 105-111.

Grossman, J. B., Woods, D. D., & Patterson, E. S. (2007). Supporting the cognitive work of information analysis and synthesis: A study of the military intelligence domain. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *51*(4), 348-352.

Joyce, R. M., McLauchlin, T., & Seymour, L. (2024). "Train the World": examining the logics of US Foreign Military Training. *International Studies Quarterly*, *68*(2), sqae044.

Lindsay, J. R., & Gartzke, E. (2022). Politics by many other means: The comparative strategic advantages of operational domains. *Journal of Strategic Studies*, *45*(5), 743-776.

Mader, M., Gavras, K., Hofmann, S. C., Reifler, J., Schoen, H., & Thomson, C. (2024). International threats and support for European security and defence integration: Evidence from 25 countries. *European journal of political research*, *63*(2), 433-454.

Mattingsdal, J., Johnsen, B. H., & Espevik, R. (2025). Effect of changing threat conditions on police and military commanders' preferences for urgent and offensive actions: An analysis of decision making at the operational level of war. *Military Psychology*, *37*(1), 33-49.

Ministry of Defence (2020). Malaysian Defence White Paper. ISBN 978-967-16437-6-1.

Monoranu, I. R. (2025). Approaches to the Concept of "Multi-Domain Operations" in the Doctrinal Vision of NATO and its Main Strategic Competitors. *Romanian Military Thinking*, (1), 14-37.

Morgan-Owen, D., Fox, A., & Gould, A. (2024). Sources of military change: Emulation, politics, and concept development in UK defence. *The British Journal of Politics and International Relations*, *26*(3), 864-885.

International Journal of Education, Psychology and Counseling
IJEPC
EISSN : 0128-164X
Volume 10 Issue 59 (September 2025) PP. 675-682
DOI 10.35631/IJEPC.1059049
Pasdar, A., Koroniotis, N., Keshk, M., Moustafa, N., & Tari, Z. (2024). Cybersecurity solutions and techniques for internet of things integration in combat systems. *IEEE Transactions on Sustainable Computing*.

Plevnik, M., & Vuk, P. (2025). Navigating the uncertainty of the modern environment: multi-domain operations for the defence of small states. *European Security*, 1-28.

Sahu, K., Kumar, R., Srivastava, R. K., & Singh, A. K. (2024). Military computing security: Insights and implications. *Journal of The Institution of Engineers (India): Series B*, 1-25.

Suleiman, M. R., & Omojuwa, K. (2025). Strategic intelligence and Nigeria's diplomatic engagements: enhancing national security in an era of transnational threats. *Journal of Policing, Intelligence and Counter Terrorism*, 1-10.

Schauer, S. G., Rizzo, J. A., Walrath, B. D., Baker, J. B., Gillespie, K. R., & April, M. D. (2023). A conceptual framework for non-military investigators to understand the joint roles of medical care in the setting of future large scale combat operations. *Prehospital Emergency Care*, *27*(1), 67-74.

Schüler, M., & Matuszczyk, J. V. (2019). Safety climate in military organizations: A pilot study of an adjusted multi-domain instrument. In *Proceedings of the human factors and ergonomics society annual meeting*, *63*(1), 1373-1377.

Takabatake, F. (2024). Nato's approach to multi-domain operations: From the perspective of the economics of alliances. *Defence and Peace Economics*, *35*(3), 281-294.

Walsh, G., Andersen, N. S., Stoianov, N., & Jänicke, S. (2023). Visualizing Military Operations: Extended Geospatial-Temporal Survey. In *International Joint Conference on Computer Vision, Imaging and Computer Graphics*, (pp. 374-396).

Wesley, E. J., & Bates, J. (2020). To change an Army-winning tomorrow. *Military Review*, *100*(3), 6-17.

Zhu, Y., Sheng, Q., Cao, J., Nan, Q., Shu, K., Wu, M., ... & Zhuang, F. (2022). Memory-guided multi-view multi-domain fake news detection. *IEEE Transactions on Knowledge and Data Engineering*, *35*(7), 7178-7191.