Sorotan DARAT

Volume 1, Number 82, June 2023

THE JOURNAL OF MALAYSIAN ARMY

MULTI-DOMAIN OPERATING ENVIRONMENT

Land Domain Readiness and Challenges

&

CYBER WARFARE

Challenges and Force Readiness

SOROTAN DARAT
JURNAL TENTERA DARAT MALAYSIA
THE JOURNAL OF MALAYSIAN ARMY

DITERBITKAN OLEH
JAWATANKUASA DOKTRIN TENTERA DARAT

SIDANG REDAKSI

PANGLIMA TENTERA DARAT
Jen Dato' Muhammad Hafizuddeain bin Jantan

PENGERUSI JAWATANKUASA DOKTRIN TENTERA DARAT
Lt Jen Dato' Tengku Muhammad Fauzi bin Tengku Ibrahim

NAIB PENGERUSI JAWATANKUASA DOKTRIN TENTERA DARAT
Mej Jen Datuk Marzuki bin Hj Mokhtar

KETUA EDITOR
Kol Norulhisyam bin Md Shuib

EDITOR
Lt Kol Mohammed Amin bin Dollah@Abdullah
Mej Mohd Hairil bin Jaafar

GRAFIK MUKA HADAPAN
Lt M Nur Hanan Syahirah binti Muhamad Rafiai

PENGEDARAN
Bahagian Pembangunan Doktrin, Markas Pemerintahan Latihan dan Doktrin Tentera Darat

KETERANGAN

Sorotan Darat ialah Jurnal Tentera Darat (TD) yang diterbitkan sejak 1 Mac 1983 bagi mempertingkatkan budaya ilmu di kalangan warga TD. Jangka masa pengeluaran ialah setiap 6 bulan iaitu pada bulan Jun dan Disember. Segala isi kandungannya termasuk sebarang ilustrasi, gambar, jadual dan rajah tidak dibenarkan dicetak semula dalam apa corak sekalipun tanpa mendapat kebenaran Kementerian Pertahanan melalui MK PLDTD terlebih dahulu.

Selaku sebuah Jurnal TD, Sorotan Darat adalah bertujuan mewujudkan satu forum bagi perbincangan perkara yang boleh menimbulkan minat profesional terhadap seorang perajurit. Artikel meliputi pelbagai isu dan tema adalah dipelawa dari segenap peringkat dan sesiapa sahaja yang mempunyai pengetahuan khas atau minat terhadap hal ehwal ketenteraan. Isu-isu kontroversi biasanya menjadi nadi penggerak sesebuah jurnal profesional yang mana ia dapat menimbulkan pemikiran dan perbincangan yang sihat. Artikel-artikel seperti ini akan diberi keutamaan, manakala artikel-artikel mengenai operasi-operasi, idea-idea latihan atau kegunaan peralatan adalah antara topik-topik yang sangat dialu-alukan.

Semua pertanyaan mengenai Sorotan Darat hendaklah dikemukakan kepada Ketua Editor iaitu Kol Doktrin, MK PLDTD.

Semua idea yang dikemukakan oleh penulis melalui artikelnya dalam jurnal ini, sama ada sebahagian atau seluruhnya adalah pendapatnya sendiri. Ianya bukanlah pendapat oleh Kementerian Pertahanan Malaysia atau pihak-pihak lain yang berkaitan.

© Kementerian Pertahanan Malaysia 1983

TABLE OF CONTENT

FOREWORD

السلام عليكم ورحمة الله وبركاته

In the name of Allah, the Most Gracious and the Most Merciful. Praise to Allah SWT, because of His guidance and blessing, we are able to continue publishing *SOROTAN DARAT*, the Journal of the Malaysian Army. It has been the Higher Commanders' intent that this journal is able to contribute to the dissemination of military knowledge while enhancing the professionalism of the Army Officers.

Personally, and on behalf of the Editorial Board, I would like to convey my upmost gratitude to all for making the publication of this edition possible. We look forward to your continued interest in writing articles for this journal. I also would like to thank the Editorial Board for maintaining an effort to publish this Army Journal. As an exclusive Army Journal, *SOROTAN DARAT* aims to create a forum for discussion of matters that may arouse professional interest in any military issues. The featured articles covered a wide range of issues, in line with the theme sets for each series of publications.

This 82nd edition is featuring articles related to **Multi-Domain Operating Environment (MDOE) – Land Domain Readiness and Challenges**, and also **Cyber Warfare – Challenges and Force Readiness**. Both issues are very crucial in nowadays security environment whereby a thorough discussion and analysis on these two aspects will cultivate knowledge and perspectives of Army Officers on the matters. May the ideas and key information by writers could enhance ideas and knowledge presented to the readers, as well as supporting the objective to develop Malaysian Army as a knowledge-based organization.

Last but not least, let us pray to Allah Subhanahu Wataa'la for all Army personnel to continue to be given the guidance and strength to bring this organization excel in both locally and abroad. Thank you.

"*Latihan Teras Keyakinan*"

MEJ JEN DATUK MARZUKI BIN HJ MOKHTAR
GOC TRADOC

FROM CHIEF EDITOR'S DESK

السلام عليكم ورحمة الله وبركاته

In the name of Allah, the Most Gracious and the Most Merciful. Praise to Allah SWT, as the first journal of the year 2023, Edition 82 is successfully published to acknowledge the writers' effort in enhancing the readers' mind with informative, useful and meaningful articles. The Editorial Council would like to express our appreciation to all writers who have contributed to the publication of this journal. The commitments and enthusiasm by the thriving writers are certainly a precious aptitude in producing a well-published journal. The golden wisdom in thinking and actions come in many forms as they can be extracted from various sources. Therefore, *SOROTAN DARAT* provides such a platform for the readers to extract the ideas shared by the writers in enhancing their professional knowledge and situational awareness.

This edition of *SOROTAN DARAT* is a bit different from previous publications since it encompasses two different themes which is the **Multi-Domain Operating Environment (MDOE) – Land Domain Readiness and Challenges**, which looks into the concept of MDOE and its impact on the existing defence strategic policies (DWP, SKN 2.0, and 4D MAF) as well as the adaptive measures that each service branch needs to implement in applying the MDOE concept in the organisation and also the theme on the **Cyber Warfare – Challenges and Force Readiness**, which discusses the challenges and roles of the Army as part of a combined team to combat the cyber threats in the Multi-Domain Operating Environment's context.

The Editorial Council welcomes and encourages more new aspiring writers to contribute articles for future publications. Constructive opinions, dynamics comments and potential ideas as well as feedbacks from the readers are highly encouraged to improve the quality of the journal published in the future. Thank you.

"Knowledge is the Core of Confidence"

KOL NORULHISYAM BIN MD SHUIB
Chief Editor

ARTICLE CONTRIBUTORS

Lt Kol Mohd Zuhaimi bin Ismail was commissioned into the General Service Corps (Education) in 1999. He holds a Master in Education (Curriculum and Instruction) from Northern University of Malaysia (2011). He has written an article on “Multi-Domain Operational Environment”. He is currently attached to Malaysian Armed Forces Joint Warfare Centre as the Head of Research and Development.

Lt Kol Dr Abdul Rahim bin Hj Abdul Rahman was born in Melaka on 6th January 1972. Upon completing his degree in Bachelor of Human Sciences in Psychology (Hons) (IIUM) (1996), he entered the military and was commissioned into the General Service Corps (Education). He is currently the Assistant Director of Comparative Technology at Malaysia Institute of Defence and Security (MiDAS). He has a Diploma in TESL (UITM) (2008), a Master Degree in TESL (UITM) (2013) and a PhD in Management (UM) (2021) specialised in digital library system and its operation management.

Lt Kol Kogilabalan Nair a/l Gunasekaran was commissioned into Royal Service Corps on 28th December 2005. Throughout his service, he held notable appointments such as 2IC of 73rd Battalion RSC, Officer Commanding of 932nd Transport Company RSC and Company Commander at PUSASDA. He had also attended Combined Logistics Officer Advance Course (CLOAC) Class 26-15 at CSS School, Philippines. He is currently the SO 1 Service Corps at Headquarters of 1st Infantry Division.

Lt Kol Suzie @ Suzianna binti Yusof was born on 4th January 1981 in Temerloh, Pahang. Her military career started in 2004, when she was commissioned as a Graduate Officer and assigned to the Royal Intelligence Corps. She holds a Bachelor’s Degree in Computer Science from University of Technology Malaysia (UTM). In her military career, she has served in various positions and units. She is currently the SO 1 Training at the Training Directorate, Malaysian Defence Intelligence Organisation (MDIO).

ARTICLE CONTRIBUTORS

Lt Kol Ir Haji Faizal bin Mohamed Yusoff was commissioned to Royal Engineer Corps in 2003 and currently serves as Detachment Commander of 921st Detachment – 92 UPKAT. He obtained a Diploma in Engineering from Coventry Technical College, United Kingdom (1994) and a Degree in Mechanical Engineering from the University of Manchester Institute of Science and Technology, United Kingdom (1998). He holds a Master's Degree in Assets and Facilities Management from Universiti Teknologi Malaysia (1998). He is a professional mechanical engineer registered with the Board of Engineers and The Institution of Engineers Malaysia, as well as a professional technologist registered with Malaysia Board of Technologist.

Lt Kol Ts. Zulkhairi bin Omran joined the service in 2004 and was commissioned into the Royal Electrical and Mechanical Engineer Corps. He has held a numerous of staff and command appointments, the most notable being the Senior Instructor of Engineering and Military Management Branch of Army Institut of Engineering (IJED). He served as the Officer Commanding at 41st Wksp Arty from 2015 until 2017. He pursued his Malaysian Command and Staff Course in 2017 and he holds a Master of Business Administration (Supply Chain and Logistics) from Universiti Pertahanan Nasional Malaysia. Currently, he is the Chief of Electrical and Mechanical Engineer of the First Infantry Division.

Lt Kol Mohamad Faizal bin Abdullah was commissioned into the Royal Signal Regiment on 9th September 2006. He has served in various important appointments within the regiment, namely as troop leader, squadron leader and second in command. He has obtained Degree in Computer Engineering from ATMA-UTM and Post Graduate Diploma in Defence and Strategic studies from UPNM. Currently, he serves as SO1 System and Communication in Markas Pemerintahan Medan Timur Tentera Darat (PMTTD).

ARTICLE CONTRIBUTORS

Lt Kol Denis anak Inggang was commissioned into Royal Artillery Regiment on 7 September 1996 after undergoing cadet training at the Royal Military College, PULADA Camp Ulu Tiram Johor for one year. He had served at 2nd Royal Artillery Regiment, 41st Battery Royal Artillery Regiment and 21st Royal Artillery Regiment throughout his service. He also had the experience serving with MALBATT 850-3 in Lebanon. He is currently serving at ULS Sampadi as a Range Liaison Officer.

Mej Mohd Qazeem bin Ibrahim was commissioned on 21st May 2005 into Royal Malay Regiment Corps through Officer Cadet scheme. He holds a Degree in Management (2016). He has served in various units and positions in the Army including Operation Officer at 17th Royal Malay Regiment (Para). He is currently continuing his studies at PUSPAHANAS, Putrajaya in the field of Strategic and Defence Studies.

Mej Abdul Kadir bin Usamah was commissioned on 15th of January 2009 into Armed Forces Religious Corps through Graduate Officer scheme. He holds the Degree of Islamic Studies – Bachelor of Shariah from Mu'tah University, Jordan (2008). He has served in various units and positions in Armed Forces including at 10th Briged (Para) as Staff Officer 2 Religious. He is currently studying at Malaysia Armed Forces Staff College in Post Graduate Diploma of Strategic and Defence Studies.

MULTI-DOMAIN OPERATIONAL ENVIRONMENT

By LT KOL MOHD ZUHAIMI BIN ISMAIL
GENERAL SERVICE CORPS (EDUCATION)

INTRODUCTION

Multi-Domain Operational Environment (MDOE) is a military strategic concept that encompasses understanding and implementation of integrated military operations by various domains including land, sea, air, space, cyber and information. MDOE basically means in a military armed conflict or campaign or operation, the conduct of battle does not only engage one domain, it however jointly involves a few other domains. Thus, strategy and tactics should be employed in multi-domains perspectives to optimize capability, efforts and resources from every domain involved that will definitely maximize the campaign outcome holistically.

For instance, MDOE application is when an armed force employs air capability to interdict and engage enemy position on land, at the same course, it conducts electronic counter measure to the enemy's communication and cyber bandwidth to reduce his defence capability. This shows how understanding and implementation of MDOE are very important to achieve success in the modern military operations.

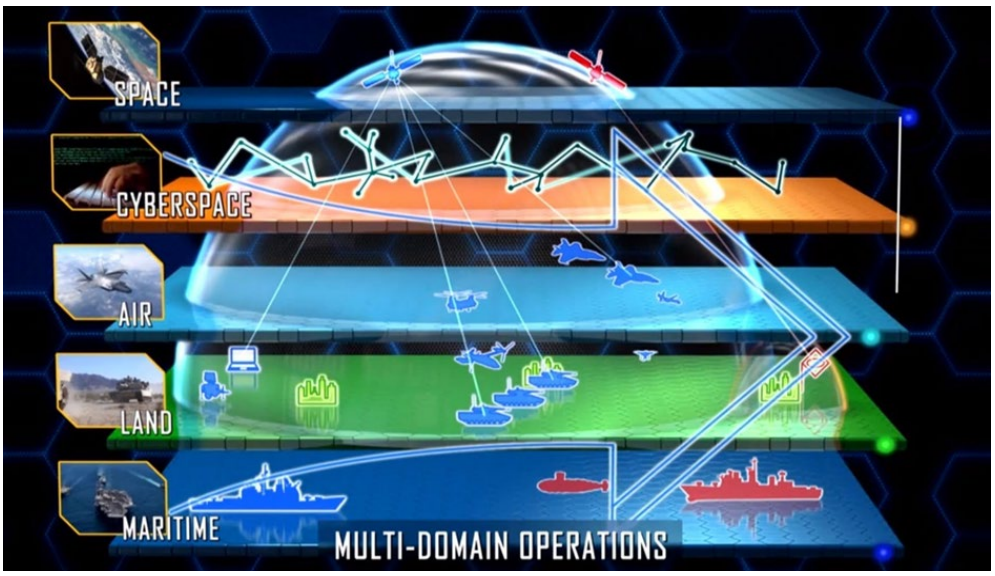

Figure 1: Diagram of Multi Domains Operation

CAPABILITY AND READINESS OF THE ARMY OPERATING IN MULTI DOMAINS

The readiness of the Malaysian Army to operate in multi-domain is important due to the presence of more complex multi-domain threats faced by the nation. Thus, the Army needs to have readiness, capability and competency in strategy, technology, human resource and other contributing elements to enable the force operating effectively and successfully in multi domains environment.

It emphasizes that the Army should have capability and strength in order to be operating in urban, jungle and offshore areas. Nevertheless, the biggest challenge faced by the Army is to be deployed in multi-domain operation where its cyber potency and capability are concerned. Cyber threat may threaten the capability of the Army to conduct their operations. Therefore, the Army needs to enhance and upgrade their defence assets to protect and prevent them from enemy's cyber-attacks besides creating and developing strategy to counter the threat.

Furthermore, the Army also needs to face challenges in terms of technological advancements. Technological developments in various domains, including robotics, remote control, and new weapon technologies, are advancing rapidly. Therefore, the Army needs to ensure that they constantly possess sufficient technological capabilities to address these new threats.

The ability and readiness of the Army to operate in various domains are crucial to ensuring national security and enabling them to effectively carry out their duties under emerging threats from different domains.

MDOE AND ITS CHALLENGES TO THE ARMY

The challenges faced by the Army in the context of MDOE are increasingly complex and require more integrated and holistic capabilities. Some of the challenges faced by the Army in the context of MDOE are as follows:

- **Cross-Domain Operational Capability**. The main challenge faced by the Army in the context of MDOE is the need to manage cross-domain operations involving land, sea, air, cyber, and space forces. This requires more integrated and holistic capabilities in planning and executing operations.

❖ **Complexity of Threats**. Another challenge faced by the Army in the context of MDOE is the increasing complexity of threats, including threats from unknown actors such as terrorist groups and evolving cyber threats.

❖ **Technology and Capability**. Another challenge is the need to upgrade and enhance technology and operational capabilities to meet the current requirements of Army operations. This includes the adoption of the latest technologies in weapons, cyber software, remote surveillance systems, and other related equipment.

❖ **Army Readiness**. Army readiness is a major challenge in the context of MDOE. This requires continuous training and development to enhance the readiness and skills of Army personnel in facing the increasingly complex challenges of MDOE.

❖ **Command and Control**. Effective command and control mechanisms are vital for coordinating operations across multiple domains. The Army must establish clear command structures, communication channels, and decision-making processes to ensure seamless integration and synchronization of actions across land, air, sea, cyberspace, and space.

❖ **Logistics and sustainment**. Supporting multi-domain operations requires efficient logistics and sustainment capabilities. The Army must ensure the timely and effective deployment of resources, including supplies, fuel, maintenance support, and medical services, to sustain operations across different domains.

❖ **Need for International Cooperation**. In the context of MDOE, international cooperation is crucial to ensure a more integrated and holistic Army capability. This includes cooperation with allied forces and international collaboration in various operational domains.

THE ARMY COUNTER THE CHALLENGES

MDOE presents increasingly complex challenges for the Army. Therefore, the Army needs to have more integrated and holistic capabilities in planning and executing operations, upgrading and enhancing technology and operational capabilities, improving Army readiness, and enhancing international cooperation across various

operational domains. To enhance Army readiness in facing MDOE challenges, several steps that need to be taken are as follows:

- **Provide Effective Training**. Effective training is a crucial factor in enhancing Army readiness to face MDOE challenges. Training should be conducted regularly and involve all levels, including land, sea, and air forces, as well as cyber forces.

- **Enhance Cross-Domain Operational Capability**. Army readiness needs to have the capability to manage cross-domain operations and communicate with other forces across various operational domains. This includes developing capabilities in cross-domain technology and operations, including remote surveillance systems, satellite communications, and cyber sensors.

- **Upgrade Equipment and Technology**. Existing equipment and technology need to be upgraded and strengthened to meet current operational requirements, including smart weapons, sensor and remote-control systems, and remote surveillance systems. This includes upgrading and strengthening technological capabilities and equipment to meet current operational needs.

- **Enhance Expertise in Cyber and Information Security**. The Army service needs to develop expertise in cyber and information security to ensure the protection of strategic and critical information for the nation's interests.

- **Improve Leadership and Risk Management Skills**. Leadership and risk management skills within the Army organization need to be enhanced to enable the organization to face increasingly complex MDOE challenges.

- **Command and Control**. Multi-domain operations require effective command and control mechanisms. The Army needs to establish clear command structures, communication networks, and decision-making processes that facilitate coordination, synchronization, and rapid response across all domains.

- **Logistics and Sustainment**. Adequate logistics and sustainment capabilities are crucial for supporting multi-domain

operations. The Army must ensure the timely and efficient deployment of resources, including supplies, fuel, maintenance support, and medical services, across various domains to sustain operations.

❖ **Enhance Cooperation with Allied Forces and International Cooperation**. Cooperation with allied forces and international collaboration is essential to strengthen the capabilities of the Army in facing increasingly complex MDOE challenges.

Army readiness in facing MDOE challenges requires steps such as providing effective training, enhancing cross-domain operational capabilities, upgrading equipment and technology, improving expertise in cyber and information security, enhancing leadership and risk management skills, and increasing cooperation with international allied forces.

IMPACTS OF MDOE ON THE DEFENCE STRATEGIC POLICY

MDOE has become increasingly important in understanding how to address complex and rapidly evolving security threats in the present time. In the context of Malaysia, the impact of MDOE on existing strategic defence policies can be observed in the following aspects:

❖ **Inter-Service Integration**. The growing need for integration among the Army, Navy, and Air Force in addressing security threats in the MDOE. This means that Malaysia's strategic defence policy needs to be significantly strengthened to ensure that the Malaysian Armed Forces can effectively function in such operational environments.

❖ **Task Scope Expansion**. The need to expand the scope of tasks for the Malaysian Armed Forces to address threats in the cyber and space domains, where security challenges related to the nation are increasing. Therefore, Malaysia's strategic defence policy should enhance the capabilities of the Malaysian Armed Forces in safeguarding the nation's cyber space and undertaking preventive measures in the space domain.

❖ **Technological Capability**. The requirement for improved technological capabilities and expertise in handling smart weapon systems and complex cyber-attacks in the

MDOE should be given attention and necessitate further action. Therefore, Malaysia's strategic defence policy needs to emphasize defence technology development and provide supportive training to strengthen the necessary skills in handling smart weapons to prevent cyber-attacks.

- **International Cooperation**. The need to foster cooperation with other countries and relevant agencies to address threats in the MDOE. Malaysia's strategic defence policy needs to enhance diplomatic relations with other countries and defence agencies to improve trust and the dissemination of information related to security threats.

MDOE has transformed the nature of security threats, necessitating changes in Malaysia's strategic defence policy. This highlights the need for improvements and enhancements in the capabilities of the Malaysian Armed Forces to ensure that the country can effectively address security threats in an increasingly complex and rapidly changing operational environment.

IMPACTS OF MDOE ON THE NATIONAL DEFENCE WHITE PAPER

MDOE has a significant impact on the National Defence White Paper. As a document outlining the country's defence policy, the National Defence White Paper discusses Malaysia's defence strategy and policies, including the threats and challenges faced by the nation.

With the presence of MDOE, national security threats become increasingly complex and rapidly changing in an integrated and expansive operational environment. Therefore, the National Defence White Paper needs to take into account the threats posed by MDOE and strengthen the country's defence strategy to address these threats. Some impacts of MDOE on the National Defence White Paper are as follows:

- **Inter-Agency Cooperation**. The need to enhance cooperation among agencies and the armed forces in addressing threats in MDOE. The National Defence White Paper needs to consider this factor and focus on closer cooperation between defence agencies and the armed forces to strengthen the Malaysian Armed Forces' (MAF) capabilities in facing threats in MDOE.

- **Expansion of MAF's Task Scope**. The need to expand MAF's task scope in addressing threats in the cyber and space domains. The National Defence White Paper needs to consider the threats related to these domains and enhance MAF's capabilities in monitoring and addressing cyber and space threats.

- **Development of Defence Technology and Training**. The emphasis on the development of defence technology and training to address smart weapons and complex cyber-attacks in MDOE. The National Defence White Paper needs to focus on technology development and training to enhance skills and expertise in handling smart weapons and defending the country's cyber systems.

- **Requirement for International Cooperation**. The need for international cooperation to address threats in MDOE. The National Defence White Paper needs to take into account international perspectives on threats and strengthen diplomatic relations with other countries and defence agencies to improve relationships and address security threats.

MDOE has a significant impact on the National Defence White Paper and requires updates in the country's defence strategy to address increasingly complex threats in an integrated and expansive operational environment.

IMPACTS OF MDOE ON THE NATIONAL DEFENCE STRATEGY 2.0

The National Defence Strategy 2.0 (NDS 2.0) is a strategic policy document that outlines Malaysia's national defence strategy in facing current security threats. MDOE has a significant impact on NDS 2.0 because it has transformed the military operational landscape and introduced greater challenges to national security. Some impacts of MDOE on NDS 2.0 are as follows:

- **Increased Need to Strengthen Military Capabilities in Conducting Operations across all Domains**. NDS 2.0 needs to consider threats in MDOE and enhance the MAF capabilities to conduct operations in all domains, including the cyber and space domains.

- **The need to Expand Cooperation among Agencies and the Armed Forces in Addressing Threats in MDOE**. NDS 2.0 needs to focus on closer cooperation between defence agencies and the armed forces to strengthen MAF's capabilities in facing threats in MDOE.

- **The Need to Enhance Training and Development of Military Technology to Address Smart Weapons and Complex Cyber-Attacks in MDOE**. NDS 2.0 needs to emphasize technology development and training to improve skills and expertise in handling smart weapons and defending the country's cyber systems.

- **The Importance of Emphasizing International Cooperation in Addressing Threats in MDOE**. NDS 2.0 needs to take into account international perspectives on threats and strengthen diplomatic relations with other countries and defence agencies to improve relationships and address security threats.

MDOE has a significant impact on NDS 2.0 and requires updates in the country's military strategy to address increasingly complex threats in an integrated and expansive operational environment. NDS 2.0 needs to strengthen military capabilities, enhance training and development of military technology, and improve cooperation among agencies and the armed forces in facing threats in MDOE.

IMPACTS OF MDOE ON THE MALAYSIAN ARMED FORCES FOURTH DIMENSION

The Fourth Dimension in the MAF refers to the use of information and communication technology (ICT) in military operations. MDOE has a significant impact on the Fourth Dimension in MAF because it has transformed the military operational landscape and introduced greater challenges to the use of technology in military operations. Some impacts of MDOE on the Fourth Dimension in MAF are as follows:

- **Expanded Use of ICT in Military Operations across all Domains**. MDOE has placed greater emphasis on the use of technology in military operations, including the use of advanced systems such as the latest software and remote surveillance technology. This has led to a wider use of ICT in

military operations across all domains, including land, sea, air, and cyberspace.

- **Increased Need for the Development of Advanced Technology and Expertise in Its Use**. MDOE has introduced smart weapons, remote sensing and control systems, and remote surveillance systems, which require the development of advanced technology and increased expertise in their use. The Fourth Dimension in MAF needs to strengthen technology development and expertise in the use of technology to meet current operational requirements.

- **Greater Emphasis on Cybersecurity**. MDOE has introduced greater cyber threats to military operations, making cybersecurity a major issue in the Fourth Dimension in MAF. There is a need to further strengthen capabilities in cybersecurity protection and raise awareness about cyber threats among MAF personnel.

- **Increased Need for Training and Skills Development in the Use of Technology**. MDOE requires more frequent training and skills development in the use of technology, including the use of smart weapons, remote sensing and control systems, and remote surveillance systems. The Fourth Dimension in MAF needs to enhance training and skills development in the use of technology to enhance MAF's capabilities in military operations.

MDOE has a significant impact on the Fourth Dimension in MAF and requires updates in technology development, increased expertise in the use of technology, and greater emphasis on cybersecurity. There is a need to strengthen training and skills development in the use of technology to enhance MAF's capabilities in military operations.

THE IMPACT OF MDOE ON THE ARMY FOR THE NEXT GENERATION

The Army for the Next Generation (Army 4nextG) is a transformation program launched by the Malaysian Army in 2018 to renew and strengthen the capabilities of the Army in facing future military challenges. MDOE has had a significant impact on Army 4nextG as it has transformed the landscape of military operations and introduced greater challenges to the Army's capabilities. Some of the impacts of MDOE on Army 4nextG are as follows:

- **Increased Need for Advanced Technology and Smart Weapons**. MDOE has introduced the use of more advanced technology in military operations, including smart weapons, sensor and remote-control systems, and long-range surveillance systems. Therefore, the Army needs to update the requirements for advanced technology and smart weapons in Army 4nextG to meet current operational needs.

- **Increased Need for Expertise in Technology Utilization**. MDOE requires greater expertise in the use of technology in military operations. Therefore, the Army needs to enhance technology development and expertise in technology utilization to meet current operational needs.

- **Greater Emphasis on Mobility and Efficiency**. MDOE has transformed the landscape of military operations with a greater emphasis on mobility and efficiency in military operations. Therefore, the Army needs to update Army 4nextG with a greater focus on mobility capabilities and efficiency to meet current operational needs.

- **Increased Need for Training and Skill Development in Technology Utilization**. MDOE requires more frequent training and skill development in the use of technology, including the use of smart weapons, sensor and remote-control systems, and long-range surveillance systems. Therefore, the Army needs to strengthen training and skill development in technology utilization to enhance the Army's capabilities in military operations.

MDOE has a significant impact on Army 4nextG and requires updates in technology development, increased expertise in technology utilization, greater emphasis on mobility and efficiency, and increased training and skill development in technology utilization. The Army needs to update Army 4nextG to meet current operational needs and enhance the Army's capabilities in military operations.

PROPOSAL FOR IMPLEMENTING THE MDOE CONCEPT IN THE MALAYSIAN ARMY

To implement the MDOE concept within the organization of the Malaysian Army, several steps need to be taken by each Army service, which include the following:

❖ **Reassessing the Existing Military Strategy and Doctrine**. Reassessing the existing military strategy and doctrine to ensure its relevance in the MDOE operational environment. This includes considering the need to update doctrine in the use of technology and cross-domain operations.

❖ **Developing Tactical and Technical Capabilities**. Developing tactical and technical capabilities suitable for the MDOE operational environment. This includes developing the ability to manage cross-domain operations and the ability to communicate with other forces in various operational domains.

❖ **Strengthening Capabilities in Cyberspace and Information Security**. The Army services need to develop expertise in cyberspace and information security to ensure the protection of strategic and critical information for national interests.

❖ **Updating Existing Equipment and Technology**. The Army services need to upgrade and enhance technological capabilities and equipment to meet current operational needs, including smart weapons, sensor and remote-control systems, and long-range surveillance systems.

❖ **Enhancing Training and Skill Development**. Enhancing training and skill development in the use of technology and cross-domain operations. Training and skill development in the use of technology and cross-domain operations are crucial to strengthen the capabilities of the Army forces in current operations.

❖ **Strengthening Leadership and Management within the Organization of the Army**. This includes developing a culture and values that support the implementation of the MDOE concept and enhancing risk management skills and strategic planning in the MDOE environment.

❖ **Enhancing Cooperation with Allied Forces and International Collaboration**. Cooperation with allied forces and international collaboration is essential to strengthen the capabilities of the Army forces in facing the increasingly complex challenges of MDOE.

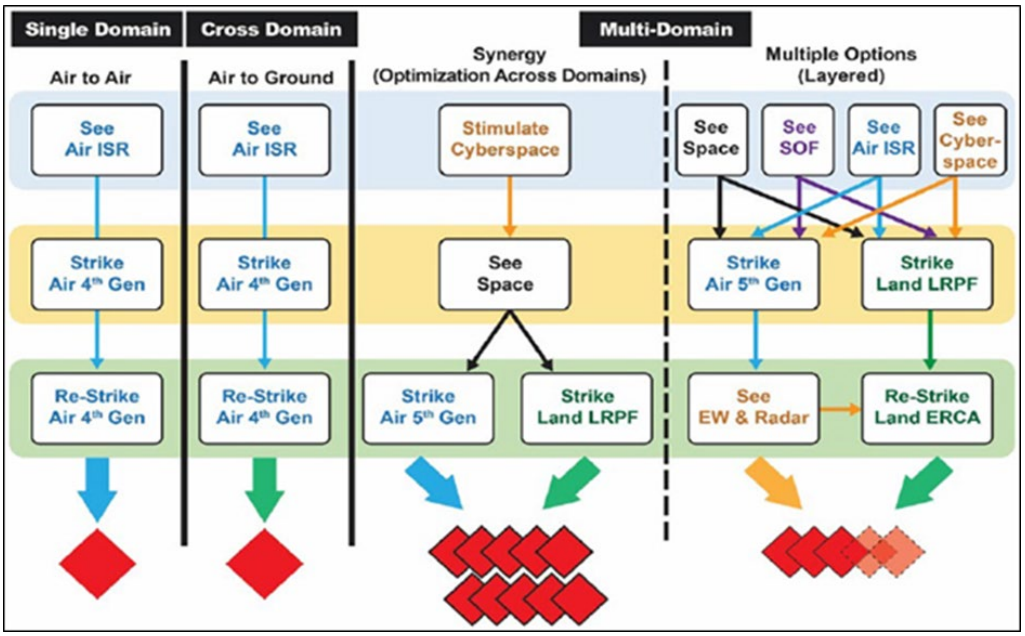

Figure 2: Description of Multi-Domain

CONCLUSION

In conclusion, the steps that need to be taken by each Army service to implement the MDOE concept within the organization include reassessing military strategy and doctrine, shaping tactical and technical capabilities, strengthening capabilities in cyberspace and information security, updating equipment and technology, enhancing training and skill development, strengthening leadership and management within the organization, and increasing cooperation with allied forces and international collaboration.

REFERENCES

Army for Next Generation 2021 - 2025.

Dasar Pertahanan Negara, 2010, Ministry of Defence.

Defence White Paper, 2020, Ministry of Defence.

Dimensi Keempat Angkatan Tentera Malaysia (4DMAF).

Multi-Domain Battle: Driving Change to Win in the Future. Military Review, D. G. Perkins (2017).

Multi-Domain Operations. Journal of Electronic Defense, J. Knowles (2016).

Multi-Domain Ops. Journal of Electromagnetic Dominance, M. Watters (2020).

Pelan Strategik MINDEF 2021 – 2025.

Security and Future, Vol 5 (2021), issue 3.

Strategi Ketenteraan Negara 2.0.

REALIZING THE POTENTIALS OF MALAYSIAN ARMY READINESS AND CAPABILITY IN THE MULTI-DOMAIN OPERATING ENVIRONMENT THROUGH KNOWLEDGE MANAGEMENT SPECTRUM

By LT KOL DR ABDUL RAHIM BIN HJ ABDUL RAHMAN
GENERAL SERVICE CORPS (EDUCATION)

INTRODUCTION

Looking at the future Multi-Domain Operating Environment landscape, the Malaysian Army is mapping out the future development of its force through various strategic direction documents such as the Army 4nextG, 4D MAF, Defence White Paper (2021-2030) and Strategi Ketenteraan Negara 2.0 (SKN 2.0). Prior to that, previous Army Chiefs since the inception of the Malaysian Army in 1933 until now, have set a solid foundation on the force development of the soldiers and the Army as the force of choice of the nation. Hence, without ignoring the contributions made by previous top Army leaderships, there are three major concerns in realising the full potential operating in a multi domain environment, that is, the rectification on the Army capability on security environment (focuses on new generations threats/adversaries), maneuver (how to fight the war) and sustainability (how to sustain the operation). In sorting such noble cause, the Army capability and readiness depends on its viability on rapid development of its training and education that later made the Army as the knowledge force as opposed to hollow force, which are vitals in the new horizon, especially, when facing new generations of warfare, with certain limitations and acceptable gaps. On that account, there are two important considerations for the Army to zoom in, which are, the capacity of each individual soldiers and the dynamic capability of the Army as a force operating in a multi-domain operating environment from the perspective of knowledge management process spectrum.

Keep in mind, in various other industries and disciplines other than the defence and military, such disruption also affects the way ‘people do things’, and it is considered normal and normal to see such transformational and change effort especially in new horizons and outlooks of the current 4.0 Industry Revolution era. Military is no exception. Any disruption as such would lead to instability of any nations globally. Moreover, with diverse geopolitical and geostrategic environment globally, Malaysia is collocated in the most dynamic environment which are the South China Sea, where superpower of the world put the heavily their interest. This very much affected the defence

landscape of which Malaysia is in. To the United States and its allies, the theatre the Malaysia is in is called the Indo-Pacific theatre and the United States has its Force Command located in Hawaii which consist of its Navy, Army, Air Force and Marine Force. Apart from that, other superpower such as China and Russia have also put their interest on the South China Sea region. China as the nearest superpower to Malaysia is aggressive to claim that South China sea is their region. The China military has put its force in a man-made military island in the proximity of 200 nautical miles to Sarawak, one of the states in the Eastern Malaysia. These superpower military are geared with state-of-the-art technology. Malaysia on the other hand is a small nation, with considerable limited defence capability. The Malaysian Army, as the largest force as compared from its sister services, is deemed to operate in multi-domain environment with a limited yet dynamic force.

Before reaching 2050 and becomes matured force, the Army needs to successfully ensure in achieving its milestones as planned, the tomorrow's Army outlook should be a more familiar sight. By doing so, the Army will be able to achieve the targeted strategic direction much earlier. However, there are limitations especially on the cost development. As such, the Army needs to have the fluidity and dynamism to face the hurdles. Although, the Army would have all the resources in the world at its disposal, there is no guarantee that it will succeed in achieving the strategic development milestones. If not careful, the Army would become a hollow organization if there are not any pre-ambled measures taken by the Malaysian Armed Forces (MAF). One of the solutions practiced by the Army elsewhere in the world is the acculturation of Knowledge Management Processes (KMPs) of its military personnel. In the other word, it connotes the importance of knowledge as a catalyst for the future change to the defence outlook. Hence, the nowadays Army put knowledge development as the platform to transform and put the Army as a better organisation in the future. Thus, knowledge development is a must process for the Army to have in overcoming the challenges and hurdles faced, in order for the Army, to become a force of choice in the future. As such, if the effort is move towards filling the knowledge gap of the Army operating in a multi domain environment, the Army has the upper edge to operate in a multiple domain as compared to its sister services.

With the current top MAF leadership, hybrid warfare seems the answer of 'how to fight the war' in current multi-domain environment. As introduced by the incumbent Chief of Defence Force, the application of hybrid warfare can be mould through the Man, Machine, Method and Mates concept which appears in the latest strategic document known as Strategi Ketenteraan Negara 2.0 (SKN 2.0). Hence, in achieving the

objectives set within SKN 2.0, the top Army planner had considered that a sustainable support system for the force development of the MAF through the Man, Machine, Method and Mates (4M) concept for the MAF and its sisters of arm including the Army to operate in a multi domain environment. Yet in reality, for the Malaysian Army to operate in two regions simultaneously in a multi domain environment such as the land, sea, air, cyberspace and other generations warfare, plus with the applications of the strategic documents introduced above are still at the infant stage, the Malaysian Army need to re-emphasize its focuses on the knowledge gap or loopholes exist in order to operate as the force of choice efficiently and effectively in a multi domain environment.

In Army 4nextG outlined plan, it is mentioned that the type of future soldier required to become a knowledge-based Army is the thinking soldier type. In other words, the future outlook of the Army must qualify as a knowledge-based Army. Therefore, roadmap to achieve such status rely on the type training and education possessed. As such, the current training and education is an important element and the latest cutting-edge scientific and technological developments is the vital in future education and training of the Army in achieving the desirable milestone of the Army of having the full spectrum capability operating in multi domain environment. As such KMPs at strategic, operational and tactical level of the Army must be scrutinized. As such KMPs is a must-have organisational tool to have in nowadays military organisation.

As one of the good organisations, to ensure that every strategic plan made is successful, the translation of the Army strategic plans must be translated accurately into workable and measurable action plans at the operational level. Then, it goes down to the lowest level of the organization, the tactical level, where the actions of the action plans are the cascading translation. It would be a headache to the planer at various level just to aligned the plan, action plan and action i.e., if the plan at the strategic level does not translate well at the two levels below in the organization. It would be a mockery to the strategic planning groups for the operational and tactical group to simply copy and paste the exact same plan and wording at the strategic level and without clear direction and purpose, the action plan and actions become exactly the same, indicating a lack of understanding in translating from strategic to operational to tactical level would also lead to lack of composure when drafting the action plan and later promote lack of understanding in the application of the action plan by the military operators at tactical level. If not tackled accordingly, the situation inevitably became uncontrollable and horrendous showing signs of simply parroting, and

that would become the conclusion, if occurred as such. So, to avoid such commotion and problems from occurring, knowledge gaps between the strategic and operational levels, as well as between the operational and tactical levels must be identified.

The Army Learning Centre of the Institute for Army Senior Officer is a good platform to become the centre for the research and development of the identifying the knowledge gap in order for the Army to operate effectively and efficiently in MDOE. The gap of knowledge must be identified at two different levels which are at the individual and organisational level. The knowledge gap at organisational and individual level can be identified through alignment of strategic documents as mentioned above with Army Training and Evaluation Programme (ARTEP), Standard Operating Procedures (PROTAP) and present Army Doctrines and Army Training Management Plan with stakeholders such as the regional command of West and East Command, Training and Doctrine Command, and all Regiment/Corps Subject Matter Experts (SME) at all Directorate of Corps of the Army. The alignments must also include the alignment between the theoretical and practical aspects of the application of the Army able to operate in two theatres simultaneously in multi domain environment. The initial effort towards the Army operating successfully in a multi domain environment must begin with aligning the future and present knowledge of the Army with the practical realm of which Army is facing or expected to face in the future, at least to the maturity period of the Army 4nextG strategic plan in 2055. Hence, in determining the strategic goals to be achieved in accordance with the layout plan, the Army need to prepare its soldiers and organisations to achieve such goals from the perspective of knowledge management spectrum.

At the level of individual cognitive development, a person with such qualities, a thinking soldier, should be equipped with strong basic cognitive developmental abilities. Such cognitive developmental capabilities will illustrate critical thinking ability, problem-solving ability, higher-order thinking ability, and leadership ability. Personnel with such capacities are expected to be able to act according to different situations and different threats and domains. Such future warriors have the ability to see through the fog of war. On a different cognitive spectrum, a thinking soldier is able to evaluate and execute the intent of his immediate commander, from broad to specific course of actions, able to adapt to environmental advancements and technological disruptions and lastly, such a group of soldiers can deduce and arrive at sudden decisions quickly and efficiently. With such individuals, future soldiers who have the advantage of science and technology, this type of soldier is able to propel the Army into a truly knowledge-based

organization thus avoiding in becoming a hollow organization. By having such thinking soldiers in the future, it able to become a full-scale knowledge-based Army. Therefore, it able to strive to share knowledge, analyse data and information and turn it into knowledge that can be adapted in the organisation. It able to strive to manage complex situations quickly and effectively, foster a culture of innovation and organizational learning, cultivate an altruism attitude in future security environment.

Meanwhile, there is normal connotation that the muscles and bones are the only focal points with the Army personnel when it comes to training to equip military personnel for any war and conflict. The cognition and education aspect of training is somewhat not blended well in the learning and teaching system in our current system. This is turn make the intellectual aspect of military training is unattended. For example, one may have the misconception that such as the soldiers from combat, combat support and service support have the same level of competencies. It is in fact that the competencies of each branch can be totally different in phases of war. Hence, with the inability to differentiate the different competencies of the three branches, this would be a total mistake and not rectifying, hence, it would put the Army in a chaotic situation. Hence, it is an undeniable fact that the physicality of a soldier is an important element in soldier development, it is a humbling opinion that in order to surpass future challenges in terms of achieving the strategic goals of the future Army, the cognitive development of the soldiers is very much our major concern.

By overcoming these problems, in the end the Army has soldiers who are able to defend and protect their nation in accordance with the cognitive development contained in the Army strategic planning. In other words, our nation is defended and protected by soldiers who have a strong capacity as thinking soldiers who have strong cognitive and mental readiness. It is expected that in the near future, in order for the Army to guarantee and mould the capacity of its soldiers, the soldiers must have strong individual cognitive readiness, which also has a strong physique, strong muscles, and bones so that they are able to react and face threats from various domains. There should be a clear objective that the knowledge in science and technology of future soldiers is essential. Therefore, knowledge should be a key ingredient in developing thinking soldiers which in turn would ensure that the strategic goals are achieved. In realizing the momentum and full potential, with an eye on developing cognitive readiness, there are several considerations for the planners need to consider and change. In the Army, the top-down initiative is more make-able as compared to bottom-up changes. Hence, it is recommended that for any new

planned review, the starting point is review of the Army doctrine and manual.

Moreover, the Army at the strategic level need to give clear strategic guidance based on the Chief of Army Directive (2023-2026) which is cascading from other strategic documents like Army 4nextG for the stakeholders at the operation level to translate the strategic planning into achievable action plans. The success of the translation into action plans would indicate that the leaderships and its organics at tactical level, is able to develop its own Course of Actions (COAs) as the by-product of the strategic directive (like the Army 4nextG) with clearer sense of directions as one good organisation. By right and then, every member of the Army at all level regardless of ranks must be able to translate any strategic directive from its on platform, or at least, all has the basic understanding and able to act, based on its own role and task, to execute on the matters pertaining to any Army strategic planning such as the execution of the strategic plan of the Army in their day-to-day basis planning. The optimisation of strategic plan can also be maximised with enhancement of knowledge in science and technology for every member of the Army. Hence, the effort to strengthen the knowledge of the organisation can be inculcate through creativity and innovation culture like robotics and analytic s field of which the Army would able to explore and develop as according in its strategic planning. The inclusion of science and technology knowledge development in Army should be read as equally important to the military philosophy as enshrined in current military doctrines and manuals.

Though, it is not yet a common practice to develop a future doctrine in the Army, it is a high time for the Army strategist to initiate such doctrines for the consumption of the Army future generation. This endeavour will in turn influence the future guidance and direction as well as the overall the Malaysian Army Training and Operations philosophy which are affecting the overall operation and training management of the Army in the near future. In sensing such movement, the Army needs to scrutinize by aligning the military knowledge embedded in current doctrines and manuals to match with the Volatile, Uncertainty, Complexity and Ambiguous (VUCA) security environment, as expected and assessed to occur in the near future already occurring in other part of the global, but not possible to occur in our own backyard. Hence, such new and innovative be-like future doctrines and manuals must be developed to meet such threats and challenge. Moreover, such major move and changes must be the guided through directives from the top to bottom manner in order to make such revamps a successful one. In having a clear conscience and a good action plan in its strategic planning in the Army cognitive

development, the Army must have a reliable process in incorporating intellectual values into its training management system.

Moreover, massive effort requires a neat and well-thought-out action plan that can be based on modern military tools such as the KMPs. In the previous era, the soldiers in the Army does not have the privilege to be educated as such in their military service. With the level of military education upgraded throughout their military service such tools are paramount. The tool allows the Army to enhance its teaching, learning, testing and measuring processes in the individual and collective training which in turn will positively impact the Army's overall future operations. The tool also able to alienate inefficiencies in the Army's operational processes. Thus, the tool if leveraged will be vital tool for the Army educators and knowledge managers to effectively support the continuous improvement of the strategic planning of soldier cognitive development and the Army as a knowledge-based organization as stipulated in the strategic planning. In other words, the Army needs to become a successful learning organization before it becomes a successful multi domain operator in any theatres in Malaysia and other place of the world, before the Army, able to can claim itself as one of the good knowledge-based Army that able to operate in multi domain operation environment.

Notably, the KMPs able to ignite the ideal thinking soldiers and should become as a good platform to develop the future Army, and to create a fully knowledge-based Army is the introduction of KMPs into the Army operation and training management The Army has the operational experience since 1933 since its inception. There are hundreds of contacts with the Communist Terrorists (CT) during Emergency 1 and Emergency 2, and the Sulu intruders at Sabah of which many of the new generation of the Army would able to learnt, benefiting with tool such KMPs. Not only that, with KMPs, the Army has the capability to learn and develop the Army operation best practices at all level of strategic, operational and tactical from aspect of G, A and Q matter. With the application of KMPs on any past critical incidents of any conflicts of the world from our Malaysian Army perspective, the later Army generation has the right tool able to learn and continuously improve as well as adapting the best technique, tactical and procedures. Not only that, the application of KMPs would benefit the Army as a whole hence supporting the vision of the Army to become as one good knowledge-based Army that have soldiers that are able to defence its nations based on its development of cognitive and thus have soldiers that are well equipped with modern and state of art apparatus but with the right knowledge and thinking mode that seems

to be as the repertoire of the ideal future Army soldiers in lieu the future outlook of the Army.

The knowledge development to equip the soldiers of the Army to operate in multi-domain environment, in certain degree would also affect the overall process and product of the training and education in the Army. At holistic approach, it surely would affect the overall individual and collective training system which in turn will affect the way the Army train and educate its soldiers. **Table 1** is the glimpse of the Professional Military Education (PME) of an Army Officer of which the highest institution he can pursue his military education is the National Resilience College and the beginning of an Army Officer career begin at the Pre-Commissioning Course or Cadet Course at the Army College. At the operational level, the training cycle of the organics of the two-field command would be transformed. At the moment, predominantly, the training cycle of the division, brigade and battalion level involves mainly on the with land domain. Though, the 21st Special Force Group and the 10th Brigade (Para), able to operate in other domain such as the sea and air, all of the Army organics were not well versed with the cyber domain environment unlike the three Signal Corps regiments under the hierarchy of the Army Headquarters-Signal Corps Directorate (Army HQ-Signal Corps Directorate). As such the gap of knowledge between the professional development of the officer and the gap of knowledge between the best practices of various Command HQ in regard to operate in multi domain environment must be filled with the alignment of the doctrinal and operational documents as the 'Al-Quran and Bible' for various level of command in the Army to operate effectively and efficiently in multi-domain environment.

Name of Courses	Institution	Qualification	Level
National Resilience Course	National Resilience College	Master	Joint
Defence College Course	Armed Forces Defence College	Master	Joint
Staff and Command Course	Armed Forces Staff College	Post Grad Diploma	Joint
Army College	Staff and Tactics Grade 2	Certificate	Army
Army College	Staff and Tactics Grade 3	Certificate	Army
Army Training Centre	Young Officers Tactics	Certificate	Army
Army College	Pre-Commisioning Course	Certificate	Army

Table 1: An Army Officer Professional Military Education

The training and education are also an important element in realizing the potentials of the Malaysian Army readiness and capability in the multi domain operating environment through knowledge management spectrum. The gap of knowledge between pre-service course such as recruit training for young soldier, then career courses, with the rank of Private, Lance Corporal, Corporal, Sergeant, Staff Sergeant, Warrant Officer II and Warrant Officer I. The gap of knowledge between the career course of the soldiers, especially the knowledge attained during those courses with the required knowledge for the actual practices at their respective appointment and units are equally important. Hence, the alignment of knowledge between actual practices and strategic documents with ARTEP, PROTAP and present Army Doctrines and Army Training Management Plan with stakeholders such as the regional command of West and East Command, Training and Doctrine Command, and all Regiment/Corps, SME at all Directorate of Corps of the Army will elevate the potentials of Malaysian Army readiness and capability in the MDOE through knowledge management spectrum.

CONCLUSION

In a nutshell, by recognizing and responding to the need for precise yet futuristic planning, planners at the strategic, operational, and tactical levels in the Army need to flesh out the gaps and types of military knowledge needed in the new horizon, whether they are appropriate to meet the challenges in the future. In addition to that, the Malaysian Army need to decide whether the military knowledge is solely as an art of war or defence science per say or it should be in hybrid form containing of the both two. Moreover, this is vital in the future of the Army, the development of the Army with respect to human, machine, and method development. With Army 4nextG in hand, the Malaysian Army has the comparable advantage when dealing with multi-domain threats and adversaries with strategic tool like KMPs. With such tool, the Army would have the benefit of having a systematic tool in having the lessons learnt capability of its from past critical incident, hence, the tool is an important tool in recognizing the measures and steps taken in realising the goals of the Army strategic planning. So, with a solid foundation and platform, the capacity of future Army warriors and types of organizations is different and have the dynamism to adapt to different security environment and this should be the main concern of the planners of nowadays Malaysian Army. In the end, the information and knowledge gathered for the future endeavours through the well execution of Army 4nextG are the essentials for the Malaysian Army to equip and prepare for the future generation, and then in the long run, hopefully, the development of the Malaysian

Army's future outlook regarding human resource development through education and knowledge management are achievable through the strategic directions for the Malaysian Army force development put in place based on the strategic plan stipulated in the Army 4nextG. So, in long run, by having group of thinking soldiers that are well equipped with knowledge-based Army, the unit of war and the lowest platform of war which is the section commander and its men have also the comparable right capabilities to protect its area of responsibility and the level of readiness at all level able to overcome and adapt to fight the threat and adversaries faced in a multi-domain security environment.

REFERENCES

Ananthan, S., & Inderjit, S. (2014). Capabilities-Based Planning for Force Development: Issues and Challenges for the Malaysian Armed Forces. Zulfaqar Journal of Defence Management, Social Science & Humanities, 1(1).

Ismail, A. S. E. (2019). The Defence White Paper 2019 Offers Chances for Reforming Military and Security Thinking in Malaysia. The Journal of Defence and Security, 11(2), 36-VIII.

Manuri, I., & Yaacob, R. A. (2011). Strategizing knowledge management in the Malaysian armed forces: Towards knowledge-centric organization. Journal of Information and Knowledge Management (JIKM), 1(1), 19-36.

Manuri, I. (2015). Knowledge management strategy in the Malaysian Armed Forces: Towards next-generation knowledge-centric organization. The Journal of Defence and Security, 5(2), 216.

Mat, B., Pero, S., Wahid, R., & Sule, B. (2019). Cybersecurity and digital economy in Malaysia: Trusted law for customer and enterprise protection. International Journal of Innovative Technology and Exploring Engineering, 8(3), 214-220.

Othman, A., & Alshamsi, S. S. (2021). The role of knowledge management in organizational performance: A case study. International Journal of Information Technology and Language Studies, 5(2).

Rahman, A. R. A., Rashid, S. A., & Ab Hamid, N. R. (2018). Agility and digitalization competency in logistics 4.0 in military setting: the challenge, risks and opportunities. Asian Journal of Social Science Research, 1(2).

Rahman, A. R. A., & Hamid, N. R. A. (2019). Achieving logistics performance in military environmental dynamism: The role of organizational capabilities. International Journal of Supply Chain Management, 8(2), 1004-1017.

Rusland, S. L., & Jaafar, N. I. (2020). Investigating knowledge creation processes among the Royal Malaysian Navy (RMN) fleet personnel. International Journal of Business and Management, 4(3), 22-39.

Rusland, S. L., Jaafar, N. I., & Sumintono, B. (2020). Evaluating knowledge creation processes in the Royal Malaysian Navy (RMN) fleet: Personnel conceptualization, participation and differences. Cogent Business & Management, 7(1), 1785106.

Sinaga, O. (2021). Military Skill and Training In Soldier's Bravery. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 1141-1150.

Venkatachalam, L. C. I. S. (2019). Future Combat Vehicle System (FCVS): The way forward against hybrid threats. The Journal of Defence and Security, 87.

MULTI-DOMAIN OPERATING ENVIRONMENT (MDOE) – LAND DOMAIN SUSTAINMENT READINESS AND CHALLENGES

By LT KOL KOGILABALAN NAIR A/L GUNASEKARAN
ROYAL SERVICE CORPS

INTRODUCTION

The current and future warfare are way different compared to what that were faced by the Malaysian Army during it's formation 90 years ago. Land Warfare Strategy will have to evolve based on the threat that is not traditional. The threat has the dominant capability which includes detection technology, electronic warfare and also cyber which is able to exploit land defence mechanism gaps.

In 2011, General Martin E. Dempsey, then-chairman of the Joint Chiefs of Staff and former chief of the United States Army Training and Doctrine Command (TRADOC) from 2008 to 2011, posed the following query: "What comes after 'joint'? The experiences date back to the early 2000s, when military operations spanned not only land, sea, and airspace but also outer space and the entire electromagnetic spectrum, indicating that a five-dimensional model of warfighting had already been established.

Four interconnected trends are shaping competition and conflict: rivals are vying for dominance in all domains, the electromagnetic spectrum (EMS), and the information environment; smaller armies engage in more deadly and hyperactive combat on larger battlefields; nation-states struggle to impose their will in a world that is politically, culturally, technologically, and strategically complex; and near-peer states are more likely to engage in conflict. The following is how this final point is made and stressed: China and Russia are at odds with one another and fighting.

It was acknowledged that the new strategy must take into account a considerably more complicated environment in 2017, when the concept was known as Multi-Domain Battle: We now have battlefield domain formations thanks to Air Land Battle that can conduct information operations, engage in electromagnetic spectrum (EMS) conflict, and operate across land, sea, air, space, and cyberspace. To capitalise on achievements or defend against potential weaknesses that may arise in other domains, tactical commanders need to understand how their actions affect those domains. This motion over these areas is known as convergence according to MDO. Armed forces

seek to penetrate adversary anti-access and area denial (A2AD) systems, destabilise them, and then exploit the enemy's loss of cohesion to utterly destroy their troops in their advantageous position. The future conflicts that are faced from multi domain operating environment (MDOE) will include physical and non-physical domain. Threat towards the country from multi domain in the future will challenge the Land Warfare Strategy through non-conventional military operation using system and technology intensively. The main aim to be achieved by this threat is to separate integration of Army capability simultaneously to all land domain operation.

Impacts that happened from globalization phenomenon towards security is uncertain, complex and cross boundary. This impact will influence international and regional security development. Non-traditional threat inclusive of environmental, energy, cyber, transnational crime, migration, contagious disease and terrorism becomes the determinant in security aspects. These challenges include the territorial stability of the region and will become more challenging when they involve problems of race, religion, and ideology. Multi Domain Operating Environment will cause the Land Warfare Strategy to go through transformation in terms of doctrine, organization, training, material, leadership, personnel, finance and facilities. Application of Malaysian Army capability to support Land Warfare Strategy must be able to cross Multi Domain Operating Environment and functionality of battle system within the aspects of time and space in order to give acceptable military reaction towards any type of threats.

In the course of analysing Multi-Domain Operating Environment (MDOE) – Land Domain Sustainment Impact and Challenges, this paper will try to unveil the following issues:

- Discuss Multi-Domain Operating Environment – Land Domain Sustainment

- What are the impacts of Multi-Domain Operating Environment Land Domain Sustainment?

- What are the challenges of Multi-Domain Operating Environment Land Domain Sustainment?

- Discuss How to Prepare for Multi-Domain Operating Environment – Land Domain Sustainment

MULTI-DOMAIN OPERATING ENVIRONMENT – LAND DOMAIN SUSTAINMENT

The nation's philosophy, which contains components of territorial integrity, independence, multi-culturalism, and multi-racialism, serves as the foundation for Malaysia's sovereignty. The duty of the Malaysian Army to protect the nation's 328,687 km2 of land territory is to enhance and concentrate on ground defensive mechanisms. The Malaysian Army is also in charge of guarding the country's 2,742-kilometer-long land border. In addition, the Malaysian Army is in charge of providing a secure environment to ensure the safety and wellbeing of Malaysians.

Due to the environment of globalisation, the rapid development of technology, and increasingly complex non-traditional conflict, the concept of combat will substantially change in the future. However, in addition to the currently available kinetic capabilities, future conventional threats will take advantage of quickly developing technology as a crucial capability to harass a nation's defensive system. Threats made against Malaysian Army personnel in the future will have tactical and strategic implications for the traditional capability of the Malaysian Army.

As a result, the operating environment for the Malaysian Army will be increasingly challenging and complex in the future. These traits will reduce the impact of the Malaysian Army's current conventional capability against potential threats. The Objective Force, which provides kinetic reaction capability, will enable this ability to grow and synergize between kinetic and non-kinetic capability. The Malaysian Army will be able to deal with a wide range of challenges from outside its borders thanks to this revolution in capacity.

Future domain activities will involve both physical and intangible entities. Land, Maritime, Air, Aerospace, Cyber, Information, and Human are all included in the notion. The interaction between each domain will transform the traditional operating environment into a multidomain operating environment. The structure of multi-domain battle must permit success in an ever more complicated environment. To combat the breadth and depth of enemy capabilities, multi-domain battle is expanding the battlefield architecture and allowing for seamless transitions between the battlefield and the home station across several domains.

MDOE gets over the five challenges by combining the three principles of convergence, multi-domain formations, and calibrated force posture. Capacity, capability, location, and a calibrated force posture are all factors that affect one's ability to navigate across important distances. When capabilities are properly balanced, the Total Force can provide cohesive, fully capable forward presence troops and expeditionary forces with the ability to deploy within strategically significant timeframes. Army rotational and forward deployed units make up the forces with a forward presence. A key component of the dynamic use of military force is the persistence of advance presence forces, which allows for coordinated strategic manoeuvres with essential combat, sustainment, protection, and mission leadership capabilities.

Multi-domain formations possess the capacity, endurance, and capability necessary to generate the resilience needed to operate across domains. Multi-domain formations are capable of autonomous moves, cross-domain firing, and maximising human potential. Convergence is the quick and continuous integration of capabilities across all domains, the Electro Magnetic Spectrum (EMS), and the information environment that maximises effects to outperform the adversary through synergy between domains and a variety of attack methods, all made possible by mission command and focused initiative.

It's a difficult task to keep the multi-domain battle going. If we clearly comprehend and describe the needs, identify and evaluate the risks, and concentrate our efforts on the outputs and end states, we can respond to the call. More data and information are at our disposal than ever before. We cannot, however, let logistics statuses, figures, and numbers to rule our decision-making. To have a better knowledge of our full range of skills, we must first rely on our leaders' and our professional intuition. This requires that managers and commanders comprehend the leading indications at all levels, foresee needs, and take into account the most pertinent data. Leaders must comprehend how the information we have at hand influences their choices, and they must then carry those decisions out.

Visualising a future battlefield is different. It challenges our preconceived assumptions that the next conflict won't include fleeing to a forward operating post and depending on contractors to maintain our equipment. It is the responsibility of logisticians to conceptually separate the sustainment force from the new battlefield and to assist others in doing the same.

Our future conflict depends on each organization's involvement as sustainers assume their dual roles as innovators and stage-setters. To make sure that our force has what it needs today, is kept in top working condition, and is able to anticipate needs in the future, it is essential to invest in all sustainment initiatives, including transportation solutions, life cycle management, and research and development.

The possibility and vulnerability presented by battles that take place in the air, land, sea, space, and cyberspace are both amazing. As we prepare to support a mobile and expeditionary force, we must assure effective training and the ability to counter and exploit our adversaries. We must question the established quo, hone our skills, and get ready to deliver logistics in a degraded environment.

Our logistics management and delivery systems will be put to the test by the multi-domain battle environment, and our sustainment personnel will be overworked. With that in mind, we can see how each component of our huge material companies has a crucial duty to play as we change logistics processes to prepare for upcoming wars.

IMPACTS OF MULTI-DOMAIN OPERATING ENVIRONMENT – LAND DOMAIN SUSTAINMENT

In Army 4nextG, the multi-domain capability will be improved with a capability made up of components that are balanced, deterrent, mutually supportive, resilient, and sustainable based on the local scenario. To operate as a Battle Group more successfully, the Malaysian Army will be able to combine all combat, combat support, and combat service support units. capability for long-range, high-precision strikes with a concentration on information dominance through control of the information and cyber domain. The incorporation of this capacity would highlight the effects of Malaysian Army responses, which are more reliable, economical, and end up being a deciding factor in Land Warfare Strategy. This therefore, the before mentioned environment will cause non kinetic capability transformation towards Malaysian Army capability as a whole. This capability will be achieved through strengthening infrastructure, asset and software that focusses on dominating cyber and information domain.

Based on the reading, there will be new methods of sustainment as the impact in Multi-Domain Operating Environment. The Innovative Resupply is the first. Forces from the United States and its allies will need to make an effort to minimise its logistical footprint while still making sure that supplies reach the units fighting in the deep battlespace. Future technical advancements will revolutionise the way

that forces are supported in the areas of maintenance, repair, resupply, and healthcare. Examples include 3D printing, the use of alternative energy sources, robotic evacuation systems, and driverless delivery. Utilising new technologies will necessitate the improvement and simplification of logistical support techniques, lowering operational risk and expanding the variety of actions that can be carried out due to the reduction of procedural timeframes. Self-sufficiency will expand as theatres produce consumables and recycle waste energy.

The second technique is called "Theatre Movement and Transport," and it requires that the land component have enough transportation capabilities to support the upkeep, employment, and reassignment of forces in all potential missions across a wide range. The third way is logistics diversification, wherein national and allied forces must establish a network of ally military forces and non-military organisations to support multi-domain operations with scalable logistics in order to maintain acceptable levels of self-sufficiency. Local business providers or outside actors who can give logistical support even in prohibited regions would need to be a member of the logistical networks.

The fourth tactic is to support future forces whose operations will be marked by decentralisation and autonomy, particularly in the field of logistics. Modular, adaptable logistics systems with shared inventories and logistic support techniques will be required in the event of a natural disaster. To conduct sophisticated operations with little logistical assistance, leaders will need to be educated how to exploit the resources already available in the operational region. Military engineering is the final option, but it could cause major A2AD issues for expeditionary operations, especially in metropolitan areas. As a result, there will be a greater demand for mobility and counter mobility, a key component of acquiring and preserving freedom of movement, and unit protection will increase on all levels. Engineer resources must support both military and civilian vital infrastructure in order to maintain a high level of interoperability with non-military components.

The sixth and final option is sustainable medical support, which assumes that catastrophic health crises and pandemics could swiftly overwhelm local health systems, compelling them to turn to the international community for help. Forces will need to be able to quickly deploy medical people and equipment in order to respond to these eventualities, which may occur in severely degraded environments. Future technologies will be able to improve medical care while reducing the logistical burden. Innovative methods will improve robotics, IT

systems, video cameras, and other technologies that enable remote medical operations.

Long-range precision fires, cutting-edge weaponry, and drones are all things that our opponents currently possess or will soon possess. They might be able to access our systems and disrupt our networks, resulting in battlegrounds that are more chaotic and deadly than anything we have yet to witness, including metropolitan areas. The question "what does this mean for logisticians?" may be on your mind. It will be even more important in MDOE to precisely address the needs of the war fighter by providing the necessary materials in the correct quantities at the appropriate times and locations. We can't work with "iron mountains" anymore.

CHALLENGES OF MULTI-DOMAIN OPERATING ENVIRONMENT – LAND DOMAIN SUSTAINMENT

The U.S. Army in Multi-Domain Operations 2028, TRADOC Pamphlet 523-3-1, describes the U.S. preference for future war as seeking to first dissuade adversaries from engaging in future battles against the U.S. and its allies. The reduction of demand by up to 50% is one of the assumptions of MDOE. In other publications, the demand requirements for fuel consumption, water generation, and power consumption were explored. There are new technologies that can reduce needs by using microgrids, hydrogen fuel cells, or auxiliary power units. However, despite early attempts to adopt a hybrid diesel-electric powertrain, even the new tactical vehicle still consumes fossil fuels.

The assumption is that future large-scale combat operations would require greater production to develop and sustain the levels of ammunitions to fight as units desire to fight based on comparisons between the amount of artillery fired during World War II and the rate of spending in present War fighter exercises. Given that modern US Army units rely on complex supply lines and because MDOE calls for autonomous manoeuvres from the strategic support area to the enemy near area, those worries are even more pertinent today. Only an operational pause of up to five months was necessary for the Fifty Army to meet their demands in order to gather sufficient fighting power to resume offensive operations. Even after months of planning, "the conditions favourable to a political outcome" may not be achieved.

Precision logistics management is listed as one of the essential competences in TRADOC Pamphlet 523-3-1. In order to offer the flexible, dependable, and quick-response precision logistics required by MDOE, the military identified holes in the current framework.

Precision logistics is the art of delivering support forward using a combination of sensor-driven predictive analysis, condition-based maintenance at the point of need, and robotic autonomous delivery combined with the advantageous results of demand reduction to enable multi-domain formations to present a credible deterrence during competition, to transition to armed conflict with speed and agility, and to execute Multi-Domain Operations in depth, including resupply of formations conducting independent manoeuvre to extend time and reach of protracted operations.

In order to provide a window of time and a space for manoeuvre to execute offensive operations against the enemy, MDOE relies on the convergence principle while responding to a threat. The concepts of time, space, and capacities are crucial to the convergence principle. In each of these areas, the adversary wants to impose restrictions on the US Army. The enemy's invasion is a fait accompli, thus there is no time to prepare or respond. The area in which US forces can operate is constrained by the enemy's capacity to engage US forces with conventional long-range artillery fire, as well as through cyber, space, or electronic warfare. Due to the limited amount of time and constrained or obstructed physical space, the enemy reduces the United States' capacity to use capabilities like APS. The fait accompli takes advantage of customary US operations to get ready for a major conflict. During World War II, the United States spent years developing the production capacity needed to compete on an equal footing. The luxury of time to plan for movement against the enemy cannot be relied upon for future operations.

US forces employ the temporal principle of duration, frequency, duration, and opportunity in order for convergence to be successful. The political will of the candidates and their supporters may have a significant impact on how long a war lasts. The investment in industrial capacity enables the United States to meet future needs if it anticipates a protracted war. The United States strengthened its capacity for war production because it expected to eventually enter World War II. Today, this would serve as the foundation for the MDO's essential agile, responsive, and dependable precision logistics. The frequency of replenishment is intertwined with the sequence of activities, which includes force preparation, transport, and utilisation.

Logistics Technologies has become the challenges for the Army as the Army is aggressively exploring “leap ahead” technologies that will radically change methods to resupply the forces. To transport supplies to widely separated units, the Malaysian Army must encourage the development of autonomous ground, aviation, and

watercraft capabilities. In the modern day, the Malaysian Army should be able to execute convoys along similar timetables with manned and unmanned teams when weather, geography, and enemy threats pose too many risks, much as the commercial sector can transport goods to consumers' doorsteps with driverless cars and drones.

We are investigating additive manufacturing capabilities for repair parts and tools at forward positions at or close to the point of demand because arriving on a battlefield with the necessary repair components hours after it is needed is not an option. Delivery times, distribution needs, and storage would all be lowered as a result. Soldiers may soon be able to create their own water, burn alternate fuels, and function independently of current power infrastructures.

PREPARATION FOR MULTI-DOMAIN OPERATING ENVIRONMENT – LAND DOMAIN SUSTAINMENT

The Malaysian Army needs to make sure that it is ready for the future battlefield, which might appear sooner than we anticipate. Individual sustainers still have time to get ready for the upcoming challenge.

The first step in preparing is to stay grounded in the fundamentals. While the next war's high-tech wizardry may alter the nature of conflict, it won't matter if we can't get our cars out of the motor pools or our helicopters off the airfields. You might have to carry out tasks the old-fashioned way, such as reading maps, utilising manual war tracking, engaging in more direct communications, and employing analogue technology, when the enemy damages or interferes with our power supply or jams our networks. Using the U.S. Army as an example, operating without power or internet connectivity was one of the main challenges that soldiers encountered in Puerto Rico. Recognise that while you pay attention to the fundamentals, they are also evolving. You'll need some abilities, like a solid grasp of technology.

The second preparation step is to be accurate, timely, and exact; sustainers in the MDOE cannot be slow and bureaucratic. We must move quickly. We need to modernise to be more lethal. We must continue to be a learning and adaptable organisation while providing soldiers with the tools they need to fight and prevail in every discipline.

Understanding how the Army operates is the third prerequisite, and to do this, we must comprehend how present doctrine and policy are both created by and influence force structure. Later on, we'll

discuss how doctrine, force structure, and policy are all connected and support our operational strategy. Knowing our craft is something that needs to be emphasised daily because there have been instances where sustainers had equipment for early-entry forces but it wasn't in the right place, or where they had an abundance of fuel at the port but struggled to get it to the foxhole. We can supply the fight and fulfil needs by cooperating as a disciplined logistics team that has a thorough awareness of the procedure, doctrine, and operational setting.

Our relative military advantages, which have long been our strong points, our ability to outmanoeuvre our adversaries, our development and use of cutting-edge technologies, and our quick adaptation of efficient techniques, tactics, and procedures are all targets of the enemy. The Army has valuable assets that cannot be removed from it, like its culture, leadership, trust, and integrity. However, maintaining it requires a strong dedication, hard work, and sacrifice.

CONCLUSION

As a conclusion, land warfare strategy has changed in response to non-traditional threats, which can exploit land defence mechanisms through the use of detection technologies, electronic warfare, and cyberspace. A novel strategy that addresses a highly complicated environment is called the "Multi-Domain Battle/Operating Environment." This Multi-Domain Operating Environment may conduct information operations, compete the electromagnetic spectrum (EMS), and operate over land, sea, air, space, and cyberspace.

Future operating conditions for the Malaysian Army will be increasingly challenging and complex, making the impact of the Malaysian Army's current conventional capability against impending threats less significant. Multi-domain formations have the capacity, capability, and endurance needed to generate the resilience required to work across domains. Multi-domain formations can use cross-domain fires, undertake autonomous manoeuvres, and maximise human potential. Our logistics management and delivery systems will be put to the test in a multi-domain battle scenario, and our sustainment forces will be overextended. With this knowledge, we can restructure our logistic operations to prepare for upcoming battles. Each component of our huge material companies has a crucial role to play.

The multi-domain capabilities in Army 4nextG will be improved with elements that are balanced, deterrent, mutually supportive, resilient, and sustainable based on the Malaysian situation. To operate

as a Battle Group more successfully, the Malaysian Army will be able to combine all combat, combat support, and combat service support units. The integration of capability will highlight how the Malaysian Army's response will affect us, making us more dependable, efficient, and a key component of our land warfare strategy. As a result, the aforementioned environment will lead to a revolution in the non-kinetic capabilities of the Malaysian Army as a whole. This capability will be attained by enhancing the system, set, and software that concentrate on controlling the information and cyberspace.

To transport supplies to widely distributed forces, the Malaysian Army must encourage the development of autonomous ground, aviation, and watercraft capabilities. When weather, topography, and an enemy pose too many hazards, the Malaysian Army should be able to perform convoys along identical timetables with manned and unmanned teams if the commercial sector can do so with autonomous vehicles and drones.

REFERENCES

Army 4NextG - Teras Pembangunan Keupayaan Masa Hadapan (Tahun 2021-2050), Edisi 1.1, Markas Tentera Darat, Wisma Pertahanan.

Bradley Cooper. “Precision Logistics: Sustainment for Multi-Domain Operations,” Institute of Land Warfare, no. 19-4 (2019): 2.

Christian Seabaugh, “Oshkosh JLTV First Drive Review,” Motortrend, last modified 2019, accessed February 26, 2020, https://www.motortrend.com/news/oshkosh-jltv-first-drive/.

D.G. Perkins (2017). Multi-Domain Battle: Driving Change to Win in the Future. Military Review, 97 (4), 6-12.

Gen Gustave Gus Perna, “Sustaining the Force in Multi-Domain Battle”, Army Sustainment, January – February 2018, PB 700-18-01 Headquarters, Department of the Army.

Italian Army Headquarters, General Plans Department, Plans Office: Future Operating Environment post 2035 – Implications for Land Forces (2019)

J. Watling & D. Roper (2019). European Allies in US Multi-Domain Operations. Royal United Services Institutes for Defence and Security Studies, London.

Landis Maddox, “Overcoming Multi-Domain Battle Sustainment Challenges through Demand Reduction Initiatives” (US Army War College, 2018), 1.

Lt Gen Aundre F. Piggee, “Multi-domain Battle: Fundamentals in an Evolutionary Environment”, Army Sustainment, January – February 2018, PB 700-18-01 Headquarters, Department of the Army.

TRADOC Phamplet 525-3-1 (2018): The U.S.Army in Multi-Domain Operations 2028. Department of the Army Headquarters, United States Army Training and Doctrine Command, Fort Eustis.

MULTI-DOMAIN OPERATING ENVIRONMENT – LAND DOMAIN READINESS AND CHALLENGES

By LT KOL SUZIE @ SUZIANNA BINTI YUSOF
ROYAL INTELLIGENCE CORPS

INTRODUCTION

The Malaysia Armed Forces (MAF) began as an experimental Army company in 1933 which, established by the British Army in Malaya. Since then, MAF has evolved from forces focusing on counter-insurgency operations towards forces that can carry out various spectrum operations. The advancement of technology in the borderless communication world is indirectly capable to derives debilitation against national defence and security. An increasingly volatile operation characterised by Multi-Domain Operating Environment (MDOE) demands a MAF to be prepared for the most lethal and challenging threats. Enhancing warfighting function capability entails significant improvement for man, machine and method for all services. Even though Malaysia is not beset by military conflict with other countries, three main security challenge, namely uncertainty big power relation, tough Southeast Asian neighbourhood and non-traditional security threats, has shaped the security environment towards uncertainty and cross border. In addition, the complexity of MDOE causes a severe impact on MAF defence strategy and capability.

This article endeavour to discuss the MDOE, with the aim of highlighting land domain readiness and challenges as well as action taken for each service, particularly the Army, in terms of implementing the concept of MDOE in the organisation.

LAND DOMAIN READINESS

The implication of globalisation and the information revolution also triggers more aggressive threat scenarios across multiple domains. Therefore, future Malaysian Army needs to have the ability to provide kinetic and non-kinetic military responses to overcome the diversity of potential future threats. Conforming with MDOE, the Army has adapted, improved, and continued to advance. Malaysian Army is prepared to continually (and persistently) shape the security environment to our advantage and deter adversary aggression through strength and ability to protect national security, sovereignty and prosperity. Aligns with the strategic goal of operating in two theatres simultaneously, the Army will be developed intensively and balanced

in both regions, focusing on capability goals, namely Detection, Survive and Strike, Sustainment, Protraction and Nation Building. These efforts also include Human Resource Development, Doctrine and Training, which focuses on the cognitive, psychomotor and spiritual elements as a whole. The outlined land warfare strategy will enable the Army to operate efficiently and effectively in MDOE (MKTD, 2018).

Currently, the Army is attempting to develop capability-based and network-enabled forces to address multi-spectral challenges. Military capability can be defined as the capacity to produce a desired outcome. Suitable force structures and readiness generate it and depend on combat formations' capability to synchronise the components of equipment, personnel, services, facilities, organisation, training, doctrine, and readiness. Meanwhile, a capability-based approach geared towards acquiring critical capabilities for the Army rather than acquiring assets focused on the Core Brigade has emerged as the methodology for 21st century defence development. This approach enables the Army to operate effectively, comprising geopolitical atmosphere, threat spectrum, national policies and current fiscal robustness (MKTD, 2018).

MULTI-DOMAIN OPERATING ENVIRONMENT (MDOE) CONCEPT AND IMPACT

The MDOE involves the increasingly interconnected nature of modern warfare. In the MDOE, military operations occur across multiple domains, including land, air, sea, cyber, space, and electromagnetic. This interconnectedness requires a new approach to military operations emphasising joint, multi-domain operations and effective coordination among services. The concept of the MDOE highlighted that current military operations are not limited to a single domain. Instead, military operations are increasingly characterised by integrating different domains to achieve a common objective. For example, a military operation may use ground forces to establish a presence in a specific area, while air and sea assets provide support and protection. At the same time, cyber and space assets may be used to gather intelligence and disrupt enemy operations (Perkins, 2017).

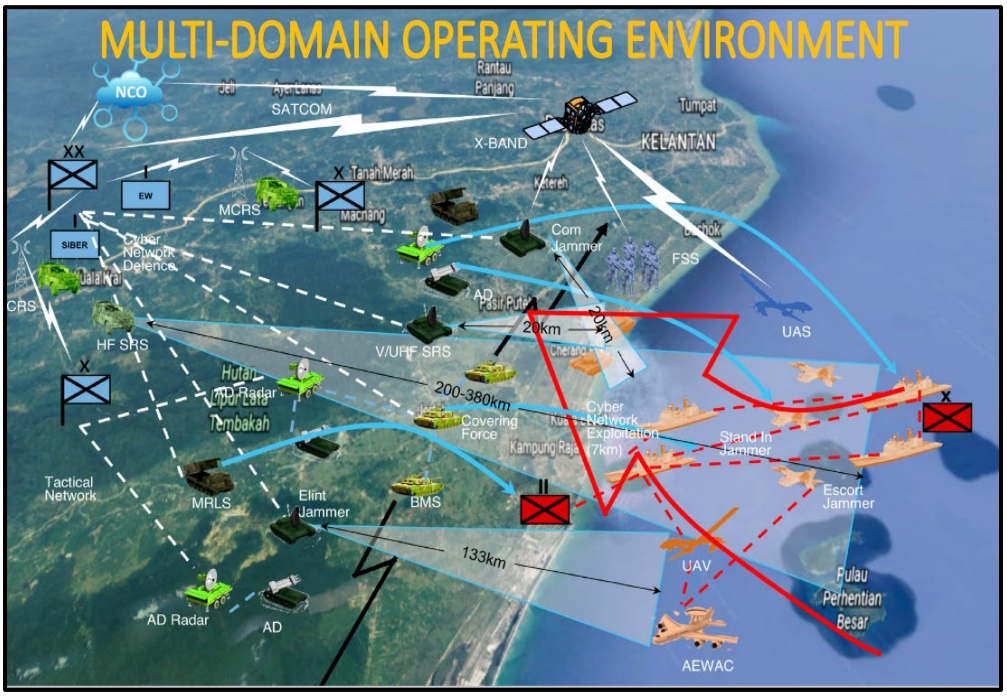

Figure 1: Multi-Domain Operating Environment (MDOE)

MDOE significantly impacts defence strategies as it requires a more integrated and comprehensive approach to military operations. Traditionally, military operations were conducted in separate domains, and each domain was treated as a distinct operational area. However, in the modern battlefield, multiple domains are increasingly necessary to achieve success. As a result, a defence strategy must be designed to integrate operations across multiple domains to achieve a synergistic effect. One of the key challenges of MDOE is the need for interoperability between different services and systems. To effectively operate in this environment, defence strategy must prioritise interoperability, collaboration, and coordination between the services. This requires a greater emphasis on joint training and exercises and improved interoperability between different military services and partners. For example, air, land, and sea forces may need to work together to achieve a common objective, such as neutralising a target or protecting a region (Russell et al., 2019).

Another significant impact of a multi-domain operating environment on defence strategy is the increased importance of information superiority. In this environment, gathering and analysing information from multiple domains is critical to achieving success. Defence strategy must prioritise the development of capabilities to

collect, analyse, and disseminate information across multiple domains. Enhancing situational awareness and intelligence capabilities is paramount to effectively monitoring and responding to threats across multiple domains. Thus it may involve using advanced sensors and analytics tools to gather and analyse data from various sources, including satellite imagery, social media, and cyber networks. MDOE also requires a more dynamic and adaptable approach to defence strategy, as adversaries can rapidly shift their tactics and capabilities across different domains. This requires the ability to quickly adjust plans and respond to emerging threats in real-time and the development of flexible and agile military forces (Perkins, 2017).

LAND DOMAIN CHALLENGES

Malaysia's geography comprises maritime and land borders prompted cross-border crime to become rampant and skyrocketing in recent ages. It is difficult for enforcement organisations, including the Malaysian Army, to man the border since it is so large and porous. Additionally, organised crime groups have used the development of communication technologies in the twenty-first century to broaden their network and carry out international crimes. A non-traditional security concern, cross-border crime is more frequently associated with organised crime groups. The Army has faced the most difficult hurdles due to the problems actively and aggressively occurring in recent years. This challenge requires the Army to enhance its readiness and resilience in combating cross-border crimes (Abu Bakar, 2019). The commencement of the Fourth Revolution Industry and globalisation give organised crime groups the drive to operate globally. On the other hand, corruption among enforcement officials also makes the border more accessible (Othman et al., 2014). Implementing effective enforcement at sea requires the task of increasing patrol in hot spot areas, inspection, asset readiness, radar optimisation, and improving standard operating procedures.

Uncertain big power relations increase economic pressure and security tension among the claimants. These are the most significant bilateral relationships in the contemporary world and Malaysia's most significant external factor. While this competition between great powers and their attempts to increase influence may present opportunities for Malaysia and other regional nations, it may also impede regional cooperation. Meanwhile, China has militarised the features it occupied and deployed its sophisticated warship as an act of provocation and military bullying against small countries. Thus, to ensure the disputed island is not lost to China or other claimants, MAF must equip

themselves with sophisticated warplanes, warships and missiles in the region to counter any untoward incidents (MINDEF, 2020).

While the politics of major powers affect Malaysia due to their power, the Southeast Asian neighbourhood conflict implies Malaysia due to its proximity. Malaysia's national security and interests are impacted by the actions, policies, and spillovers of its immediate neighbours' internal processes and the bilateral relations amongst ASEAN member states due to their geographical proximity. Due to proximity, there is also more regional interdependence. At the regional level, Malaysia's government emphasises shared wealth, shared security, and shared identity. The conflict in Myanmar involving Rohingya, for example, caused a direct impact on Malaysia. Most Rohingya escape from the conflict and prefer Malaysia to be their destination. Internal conflicts in the region are driving the influx of illegal immigrants. This conflict causes thousands of people to escape the genocide to Bangladesh, Malaysia and other places in the area. People try to escape because the government of Myanmar does not give their rights (Putra et al., 2019). On the other hand, from the Krizek catastrophe to the Tak Bai disaster, the southern Thailand community has been afflicted by racial conflict. The violence in southern Thailand remained a source of concern. Thailand views the situation in the south as an entirely domestic issue. Malaysia concerns that the region's instability could spread across its border. The establishment of multiple bilateral projects focusing on the southern region of Thailand and northern Malaysia demonstrates that the situation in southern Thailand is a strategic interest for Malaysia (Zahrul et al., 2017).

In the 21st century, social media has become the most influential media used to spread fake news and slander. The medium was the most influential in shaping the values and culture of society. Media roles are crucial in disseminating information. However, some news will be distorted or misconstrued when it is unverified from the original sources. Nowadays, there is a lot of application provided to us to connect with people around the world. The high demand for online service causes our generation becomes IT Savvy. All parties, including the land domain should consider the threats to peace and security of cyberspace. The threat of social media and the existence of new cyber and electromagnetic elements show that the dimensions of warfare among challenges cause an impact on the land domain.

The COVID-19 pandemic is another challenge for land domain readiness. The Army has been requested to deploy its personnel as the first responder to the affected area. The task may include law enforcement support, restoring essential government services, health

service support and providing emergency relief to affected people's locations. COVID-19 has affected Malaysia directly in the aspect of operation, training, human resources and logistic. This challenge requires MAF to adapt to the new norm and practice self-awareness. An operation such as Op BENTENG is crucial to strengthen Malaysia's border control from the intrusion of illegal immigrants to curb the spreading of COVID-19 (Tharishini, 2020). The control of national borders needs to be strengthened in order to prevent incursion and smuggling. It is necessary to step up efforts to enhance border control and surveillance through coordinated and ongoing measures. Among the actions that must be performed include bolstering inter-agency enforcement in a more coordinated manner, boosting the use of technology, and enhancing infrastructure. The lack of sophisticated assets such as a fast patrolling boat, monitoring combat ship, drones and Unmanned Aerial Vehicles (UAV) to strengthen the national border may reduce the effectiveness of land domain readiness.

Advanced science and technology development, including the capabilities of terrorist networks and extremist movements, accompany the threat of bioterrorism. Bio-terrorism or biological attack is an act of violence that uses chemical and biological agents or micro-organisms such as viruses, bacteria and toxins that react to paralyse and poison and kill humans and other living things. In contrast, biological weapons are categorised as Weapons of Mass Destruction (WMD) consisting of Chemical, Biological, Radiological and Nuclear elements (CBRN). Therefore, it is necessary to enhance the field and general engineering capabilities in both regions by integrating the entire team of engineers by establishing an organic Field Engineer Group under Western and Eastern Command. This group of engineers will have defensive capabilities against nuclear, biological, and chemical threats and tactical bridge systems, field engineering, and general engineering capabilities (MKTD, 2018).

Natural disasters cause major shocks and the biggest challenge for the land domain that requires MAF's involvement, particularly the Army in search and rescue operations. The landslide at the Father's Organic Farm campsite in Batang Kali near here on December 16, 2022 was the second largest incident involving the number of fatalities after the 1992 Highland Towers Condominium collapse that claimed 48 lives. Thus, nation-building capability will be able to contribute to the development of the country. The Army needs to produce a positive image to gain the support of the people and target groups' support. The people's belief that the Army is a pillar of sovereignty and national integrity is core to the existence of the Army to remain relevant. The Army's capabilities in carrying out Military and Civil Cooperation

operations and Humanitarian Relief Operations and Natural Disasters should be enhanced to assist the country in determining the well-being and safety of the people. Disaster events of a complex and large-magnitude that occurs both locally or abroad can affect people's lives and hinder the country's administration (NSC, 2021).

Meanwhile, in a resource-constrained environment, transforming allocated resources into military capabilities according to government policy is another challenge for land domain readiness. Resources comprise the 5Ms or Man, Machine, Method, Material and Money, which are the requirements for the military capability inputs, including Training, Equipment, Personnel, Information, Doctrine, Organisation, Infrastructure and Logistics (TEPIDOIL). Defence organisations, like all other government agencies, are facing constant pressure to "do more with less" due to the limited allocation of resources. Hence, the budget allocation constraint to acquire new assets and the need for national development often quoted the catchphrase "guns or butter". Inadequate financial resources due to economic problems may damper military modernisation aspirations. In addition, capability development plans that are routinely adjusted due to budgetary constraints may not produce a coherent force structure. Defence forces constantly face the dichotomy between force modernisation and force readiness for current and anticipated operations (Ananthan et al., 2020).

MEASURES TO IMPLEMENT MDOE CONCEPT IN THE ORGANISATION

The government shall develop the MAF into an integrated, agile, and focused force capable of responding to traditional and non-traditional threats in times of peace and war, with a high level of operational preparedness despite an unpredictable security environment. The government's long-term commitment to increasing the MAF's preparation with the requisite assets and equipment and a knowledgeable and professional staff geared toward the smart soldier concept and other skills is essential to this force growth. The Future Force is joint, interoperable, technology-based, able to operate simultaneously in two theatres, and mission-focused. These traits will allow the force to be swift, deployable, and multi-role, capable of acting in all four domains (maritime, air, land, and cyber electromagnetic) and engaging different challenges along the concentric zones (MINDEF, 2020).

In Malaysia Madani's Budget 2023, the Ministry of Defence secured a budget of RM10 million for the procurement of equipment and assets under the Ministry of Defence to deal with disasters. Often assets to deal with catastrophic disasters such as floods can also be used during military operations, e.g. combat boats and engines for combat boats. In order to ensure harmony and unity, the Ministry of Defence secured a budget of RM17.7 billion. From this amount, to increase the level of defence and maritime control of the country, the government agreed to approve the procurement of 3 Littoral Mission Ship (LMS) ships for RM2.4 billion. RM4.1 billion is for the maintenance and purchase of MAF assets and RM1.1 billion for the Sabah, Sarawak & Peninsular Border Control development. In Budget 2023, RM20 million was allocated to empower Local Communities for border control. In drawing up strategic planning and capacity building, the country's economic capability factor is an essential element to consider and also needs to be aligned with the country's defence policy. Consistent government commitments and stable and adequate defence investment are needed to meet the needs of force development in each financial planning (M.Hanif, 2023).

Chief of Air Force, General Dato' Sri Mohd Asghar Khan bin Goriman Khan RMAF emphasised that empowerment on the development of RMAF capabilities continues to be a priority based on defence needs aligned with the current strategic environment and threats. The evolution of the RMAF development is now in line with the concept of inclusive multi-domain operations which is used as a platform for this force to create strategic planning based on the characteristics of the future forces that have been inspired in the National Military Strategy (SKN). Geo-strategic perspectives at the global, regional and domestic levels that are uncertain require the RMAF to review the implementation of air operations in the future in order to remain credible and relevant. The development of air power capabilities is in line with the security and defence needs so that the RMAF is always able to cope with any threat. RMAF capabilities must now be developed based on modern armament applications, the latest combat technologies and tactics (Perajurit, 2022).

Meanwhile, RMN continues prioritising the vigilance of the Fleet, continuing the modified RMN 15-to-5 Transformation Plan, maximising integration and support to the aspect of togetherness as well as intensifying the process of providing human resources. According to the Chief of Navy, Admiral Datuk Abdul Rahman Ayob, the transformation is aimed at equipping the RMN with 55 ships by 2050 to meet the operational needs of the country's navy. In the meantime, RMN will continue its desire to enhance integration and support the

aspect of togetherness. According to him, this aspect is a necessity in all operations involving defence elements. RMN needs to work hand in hand with our brothers from the Army and Air Force services (M.Daim, 2023).

Geo-strategic perspectives at the uncertain global, regional, and domestic levels require the Army to review the implementation of land operations to remain credible and relevant. The development of combat power capabilities aligns with the security and defence needs so that the Army can always cope with any threat. Land domain capabilities must be developed based on modern armament applications, the latest combat technologies and tactics. Thus, future Army development is to consider the concept of multi-domain defense operations to form a national defense future force as inspired in the white defence paper (MINDEF, 2020). Evolving capabilities in the MDOE demand the Army's ability to match the concept to the doctrine, organisation, training, materiel, leadership and education, personnel, facilities and material modernisation requirements. Thus to implement the concept of MDOE in the Army organisation, capabilities that can be considered to develop are long-range precision/cross-domain fires, next-generation combat vehicles, the network, air/missile defence and soldier lethality.

The Army must acquire multifunctional weapons and sensors for long-range precision fire and air-dropped electronic warfare. The objective is to infuse lethal and nonlethal fires from the land domain to all other domains. It is vital to deliver precise fires at extended ranges to limit the hazards connected with semi-independent manoeuvres and provide the conditions required for deep manoeuvres against an integrated fires complex. The next generation of combat vehicles will be outfitted with new, urban-capable, long-range weapons. They will be smaller and optionally manned, enabling greater manoeuvrability in confined spaces. In addition to reduced fuel and ammunition usage, they will have active protection and sophisticated materials. The next generation of combat vehicles will be equipped with cutting-edge technologies such as networked targeting systems, directed energy weapons, semiautonomous wingman teaming, and long-range missiles. These will enable the semi-independent manoeuvring required in a conflict involving multiple domains.

The network will boost the speed and flow of the correct information to the right people, enabling quicker comprehension and action while limiting our adversaries manoeuvrability on the "electronic battlefield." To do this, the MAF must develop a unified end-to-end network framework with superior offensive and defensive cyberspace

capabilities. The network will provide a shared awareness of the operating environment, horizontal and vertical information sharing across all services and partners, and information management from the home station to the tactical edge. Using artificial intelligence, offensive and defensive cyber capabilities safeguard the friendly network and generate windows of opportunity while disrupting and denying the adversary's utilisation of the electromagnetic spectrum. Meanwhile, the operation of a Command and Control Center equipped with an Information Fusion Center (IFC) and supported by Network Centric Operations (NCO) is needed to cope with MDOE. Therefore, the targeting process can be effectively implemented by integrating and synchronising weapon sensor systems or other non-kinetic elements.

The Army must defend key fixed sites and provide effective air and missile defense protection of maneuvering forces by modernising short-range air defense and Terminal High Altitude Area Defense systems and developing onboard aerial and ground vehicle advanced protection systems. Success and distribution of these capabilities will determine the unit's ability to survive. As an enabler, expanding ground-based firepower will provide joint force commanders with greater options while protecting the force from enemy missiles and strikes by manned and unmanned air systems. As a deterrent, locating and displaying these capabilities will thwart opponents' efforts to fragment the unified force.

In the context of soldier lethality, Army troops should be capable of both physical and mental performance. To be effective in high-intensity battles, weapons and equipment must be superior. There must be a balance between fire and manoeuvrability in terms of lethality, with systems that boost the delivery of accurate and lethal rounds while increasing the manoeuvrability of individual soldiers. By implementing new fire control systems, ammunition, and weapon designs, the Army is enhancing the accuracy of its close and long range small weapons. Introducing robots in the form of exoskeleton suits and manned-unmanned teaming will increase small unit range, coverage, and responsiveness while enhancing the soldier's manoeuvrability. The idea of a future complete soldier is about delivering a modern Army that is prepared and fit for the challenges of the future security environment. MDOE requires a soldier to be more lethal, agile, and expeditionary, meeting the characteristics of a military that is able to fight, win battles, and claim victory. Moreover, physical resilience indicates a soldier's strength and agility and the extent to which he or she can be effective on the battlefield. The integration of body and mind is essential for preparing and maintaining warriors, as it defines their combat capabilities whenever required.

The ongoing conflict in Ukraine demonstrates the critical necessity for states to create defence strategies that reflect current and future modes of operation in warfare. This essential document will shape military plans and forces to achieve national objectives. The establishment of the Defence Cyber and Electromagnetic Division (BSEP) in line with the essence of the Chief of Defence Forces and the Defence White Paper (KPP) at the Ministry level as well as the transformation plan of the MAF through the Fourth Dimensions of the Malaysian Armed Forces (4DMAF) which has now been realised and demands that the MAF strengthen cyber and electromagnetic space defences. Nevertheless, a group of knowledgeable and competent Officer's Corps is essential for achieving organisational goals and upholding national objectives. Similarly, organisational silos must be broken to ensure effective inter-agency partnerships and civil-military cooperation. Similarly, military diplomacy must be actively employed to ensure the mass effect of coalition operations if the situation so requires.

In general, all MAF services are dedicated to the convergence of capabilities across the combined force through the integration of numerous domains in a continuous manner, as this cannot be accomplished individually. The military can win battles and campaigns, but only the entire government can win wars. Our interagency allies' familiarity with and understanding of our warfighting concepts and doctrine benefits the overall enterprise. When it comes to warfare, no one is more effective than the military and its allies and partners combined. Recent measures by Russia and China demonstrate that the operational environment is changing and that nation-state-level competition has re-emerged. It is necessary to win the "competition" that precedes and follows a dispute (Csengeri, 2021).

CONCLUSION

In conclusion, the concept of the MDOE recognises the increasingly interconnected nature of modern warfare and the need for a new approach to military operations. The MDOE concept requires joint and effective coordination among different services and commanders to achieve a common objective. MAF must be able to operate seamlessly across multiple domains, using advanced technologies and data analytics to make informed decisions in real-time. The MDOE concept is critical to the success of modern military operations and requires ongoing investment and innovation in training, equipment, personnel, information, doctrine, organisation, infrastructure and logistics (TEPIDOIL). Integrated and comprehensive

approach is indispensable to be emphasised in defence strategy. It requires the integration of different services, the development of interoperable systems, and the prioritisation of information superiority. By adopting a multi-domain defence strategy, MAF can achieve a synergistic effect and success on the modern battlefield.

REFERENCES

Abu Bakar, M. F. (2019). The Role Of Malaysian Army In Controlling Illegal Transborder Activities At The Malaysia-Thailand Land Border. Universiti Kebangsaan Malaysia.

Ananthan, S., Amirudin, S., & Wong Wai Loong. (2020). Defence Spending In An Era Uncertainty and Budgetary Constrains.

Csengeri, J. (2021). Multi-Domain Operations-A New Approach in Warfare?

M.Daim. (2023). Tahun 2023 masa untuk TLDM nilai semula, bermuhasabah untuk maju ke hadapan. Air Times.

M.Hanif. (2023). Meningkatkan Keupayaan Peperangan Asimetrik di Laut China Selatan: Bahagian 1 – Membina Keupayaaan Pasukan Khusus. Perajurit.

MINDEF. (2020). Defence White Paper: A secure, Sovereign and Prosperous Malaysia. Ministry of Defence, Kuala Lumpur. https://www.mod.gov.my/images/mindef/article/kpp/DWP.pdf

MKTD. (2018). Army 4nextG.

NSC. (2021). Dasar Keselamatan Negara 2021-2025. In Prime Minister's Office.

Othman, Z., Shafie, R., & Hamid, F. Z. A. (2014). Corruption – Why do they do it? Procedia - Social and Behavioral Sciences, 164(August),248–257. https://doi.org/10.1016/j.sbspro.2014.11.074

Perajurit. (2022). WAWANCARA BERSAMA PANGLIMA TENTERA UDARA, JENERAL DATO' SRI MOHD ASGHAR KHAN TUDM. Perajurit.

Perkins, D. G. (2017). Multi-Domain Battle: The Advent of the Twenty-First Century War. MILITARY REVIEW, 6.

Putra, B. A., Darwis, & Burhanuddin. (2019). ASEAN political-security community: Challenges of establishing regional security in the southeast Asia. Journal of International Studies, 12(1), 33–49. https://doi.org/10.14254/2071-8330.2019/12-1/2

Russell, S., Abdelzaher, T., & Suri, N. (2019). Multi-Domain Effects and the Internet of Battlefield Things. Proceedings - IEEE Military Communications Conference MILCOM, 2019-November. https://doi.org/10.1109/MILCOM47813.2019.9020925

Tharishini, K. (2020, June 8). COVID-19 Is Reshaping Border Security Enforcement in Malaysia. The Diplomat. https://thediplomat.com/2020/06/covid-19-is-reshaping-border-security-enforcement-in-malaysia/

Zahrul, S., Royal, P., & Navy, M. (2017). Civil Unrest in Southern Thailand: Roles and Challenges of Malaysia.

MULTI-DOMAIN OPERATIONAL ENVIRONMENT (MDOE) – LAND DOMAIN'S READINESS AND CHALLENGES

By LT KOL Ir HAJI FAIZAL BIN MOHAMED YUSOFF
ROYAL ENGINEER REGIMENT

INTRODUCTION

Research into the new operating landscape paints a picture of uncertain standards and enduring chaos in the years to come. The first iteration of the idea of multi domain warfare was simply an Information Age version of the traditional air-and-land conflict. The first white paper on multi domain warfare, which was published by the United States Marine Corps, focused on the development of multi domain operations, which originated from the ideas behind air-and-land battle. The Air-Land Combat concentrated largely on two domains; however, the current operational environment requires new ideas for fighting to occur in a cohesive way across all domains. This dichotomy between the two types of combat is what led to the development of the Air-Land Battle. In the present time, countries all over the world face enemies in the physical realms of air, land, sea, and space, as well as in the abstract domains of cyberspace, the electromagnetic spectrum, the information environment, and the cognitive dimension. As a consequence of this, defence forces need to adapt the manner that they are organised, trained, equipped, and postured in order to discourage prospective enemies and, if necessary, defeat them.

Adversaries may employ economic pressure, misinformation, and the prospect of military action to intimidate neutrals, partners, and allies into helping them to accomplish their goals. These operations either operate below the threshold that triggers a decisive government or military reaction, or they create a fait accompli before the Joint Force can discourage them. Adversaries will utilise economic, political, technical, informational, and military means to exploit cracks in current systems of operation, and they will do so with deceit, surprise, and speed (Easterling, 2016). It's also possible for these foes to manage the risks of escalation by using or threatening to use nuclear weapons and other weapons of mass disruption or devastation.

Aggressive strategies of revisionist nations are made possible by modernised adversarial armies that pose a threat across all domains, including the electromagnetic spectrum (EMS) and the battlefield of human perception. It is expected that the military would face sensor-rich armies of peer states and proxies utilising precision-

guided weapons on extremely deadly battlefields, which may limit Joint Force freedom of movement and operation (Joint Publication 3-01, 2017). Opponents will neutralise supreme strengths like air and sea dominance and impair vital capabilities by restricting access to space, cyberspace, and the Electronic Warfare System (EMS). Opponents will take advantage of what they see as the military's vulnerabilities, such as the length of time it takes to deploy soldiers, the locations of logistical hubs, and the security of command and control systems. Technologically sophisticated foes have researched how the security forces integrate air and naval power with technology surveillance and satellite communications to provide the ground troops more leeway and overmatch. Therefore, the Joint Force can no longer take for granted absolute dominance in any field.

MULTI-DOMAIN OPERATIONAL ENVIRONMENT (MDOE)

After the limitations of the Joint Forces Operational Concept were exploited, the concept of Multi-Domain Operations (MDO) emerged as a response to the changing character of conflict. The innovation dates back to the early 2000s, when military operations expanded beyond the traditional three dimensions of land, sea, and air to include the complete electromagnetic spectrum. The prevailing evolution of contemporary battlespace environment can be witnessed by evaluating the following trends (Csengeri, 2021):

- Exploitation of multiple domains such as the electromagnetic spectrum and information environment by hostile forces.

- The vast (and expanding) mismatch ratio between the battlespace’s physical and virtual dimensions (and lethality) versus size of forces.

- Political, cultural and technological challenges that are faced by nation states in surviving a strategically complex environment.

- Non-lethal (and kinetic) rivalry between neighbouring and regional non-adversaries that are poses greater challenges and near-impossible resolutions.

- Heightened conflict and rivalry among major world superpowers.

One of the primary motivating factors for the growth and development of the multi domain idea was the changing nature of conflict. Warfare in the modern era is evolving in such a way that adversaries intend to achieve their goals by splitting a nation by breaking their bonds with their allies without resorting to war by pushing the political, military, and economic components into a stalemate (T. D. Biddle, 2019). New era warfare is evolving in such a way that adversaries intend to achieve their goals by splitting a nation through breaking their bonds with their allies. Subsequent to that, when armed conflicts break out, adversaries will then extend and spread the stalemate over the whole operating environment, including many domains and subordinate environments. This will happen when there is a standstill. On most occasions, the traditional operational environment is the physical environment, which includes the domains of land, sea, and air as shown in **Figure 1**. However, in multi dimensional settings, the physical operational environment evolves into an informational operational environment, which includes various other aspects that affect multi domain operations in different ways as shown in **Figure 2**.

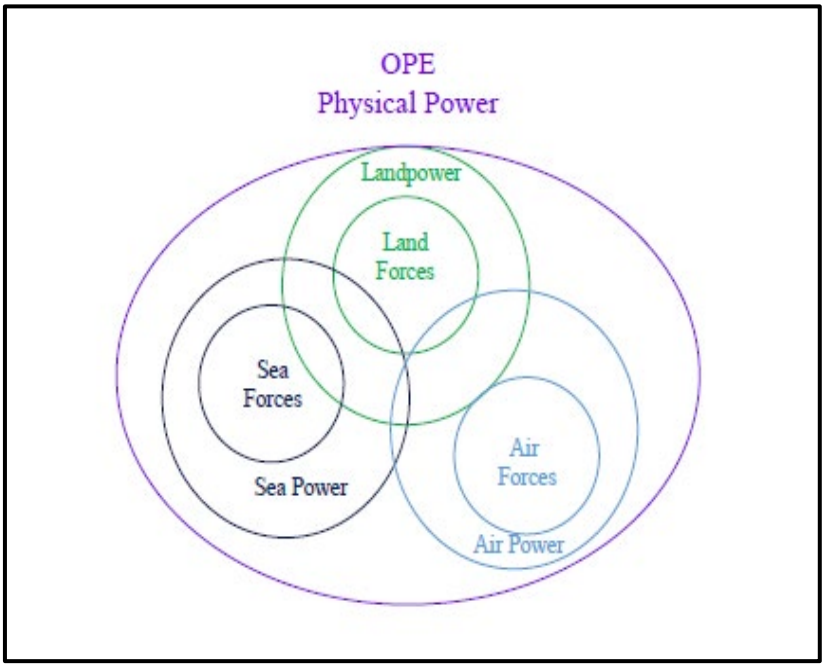

Figure 1: Traditional Operating Environment (Johnsen, 2014)

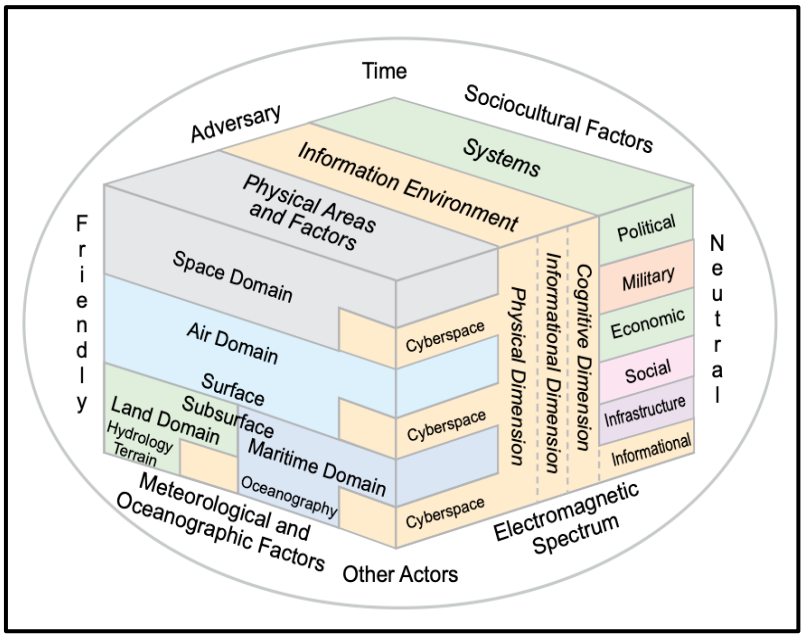

Figure 2: Holistic View of the Operational Environment (Joint Publication 2-01.3, 2014)

As far as multi-domain battle involving the Combined Arms in the 21st century is concerned, it requires ground combat forces to be ever ready to wipe out adversaries physically and cognitively through the extension of combined arms across all domains. At the joint operations level, joint forces are required to be able to form a resilient and functional synergy of capabilities to form windows to facilitate multi dimensional manoeuvre and sustainability across the size, depth and fluidity of the battlefield in order to retain initiative, exploit adversary vulnerabilities and defeat them by inflicting maximum casualty to their manpower and equipment to ultimately fulfil military objectives (Wilde, 2019). It should be carried out in a way that it aligns with subsequent operations to not only gain lasting psychological and physical advantages on adversary but also assert dominance over every aspect and layer of the multi-domain battlespace/environment (Chase, 2020).

Multi-domain operational idea is an attempt to solve the issue of layered stalemate by the quick and continuous integration of all areas of warfare. This integration is meant to serve as a deterrent and help us triumph in competitions that do not include armed confrontation (Balboni et al., 2020). If deterrence fails, then Army formations, working in concert with other elements of the Joint Force, will attempt to penetrate and disintegrate enemy anti-access and area denial

systems; exploit the resulting freedom of manoeuvre to defeat enemy systems, formations, and objectives; achieve strategic objectives; and consolidate gains in order to force a return to competition on terms that are more favourable to a nation, its allies, and partners (Townsend et al., 2019). It aims to employ this strategy by enabling Land Forces to possess the ability to manoeuvre beyond strategic distances, by enabling multi domain formations to exploit various capabilities across all domains to assert force on adversary till they collapse and finally to achieve the ability to integrate all domains to overpower adversary capacities and capabilities.

Joint Force must apply the proven principles of combined arms manoeuvre and massing of effects at decisive spaces in order to meet the demands of the evolving operational environment as well as the challenges posed by superpowers, particularly in the creation of political and military stalemate (Reilly, 2016). As far as the demands from land components are concerned, they have to be able to integrate joint capabilities in a holistic manner at a higher level and across all levels with speed and agility (Pamphlet 525-3-1, 2018). Yet, the Army must not forget its traditional functions and responsibilities, which include taking control of new territories and grounds, destroying hostile troops, and safeguarding friendly forces as well as civilians. They must constantly have the goal of outperforming their enemies in any manner possible, including in terms of speed, mass, force, and strength. In the end, they have to be capable of maximising the integration and use of every existing domain in order to multiply their production.

LAND DOMAIN'S READINESS

Echeloned units of the Army carry out Multi-Domain Operations, which include intelligence, manoeuvre, and strike operations across the information environment and the electromagnetic spectrum as well as the traditional "five domains" of air, land, sea, and cyberspace (EMS). The Joint Force Commander is given more leeway to complicate the enemy's operations by the Army's echelon's capacity to converge capabilities in a wide variety of ways and in different orders (Pamphlet 525-3-8, 2018). Strategic and operational manoeuvring by forces from outside the range of anti-access and area denial systems is made possible through echeloning of forces, which prevents forward-positioned forces from being isolated within the stand-off range of enemy anti-access and area denial systems at the outset of a conflict. The Army's ability to move at echelon opens up supremacy openings that allow the Joint Force to overwhelm enemy military systems with various problems and massed impacts.

A key criterion of a successful and effective multi domain operation that land components need to grasp is the capability of converging cross-domain capabilities. Convergence of cross domain capabilities enhances the versatility of land domain to be integrated across all domains effectively (Wormuth, 2020). It provides the Joint Force an upper hand in deploying land components all over the theatre to operate under any domains which significantly hampers the operational capabilities of adversary forces and in return, exposes their vulnerability for exploitation. As mentioned earlier, multi domain operations does not require lethal responses at all time as it aims to create a political, economic and military stalemate. Through convergence, adversary's efforts to create stalemate can be neutralized and ultimately paralysed.

Fundamentally in multi domain operations, land forces are required to be able to establish force posture in such a way that they are capable of operating physically and geographically across the theatre to be able to counter all forms of adversary's offensive efforts and operations. It is also important to retain the status quo from escalating into an armed conflict as well as not being pushed into a stalemate (James, 1997). It demands land forces to exhibit such a strong show of forces to navigate being a free-stalemate and non-conflict state. In doing this, it is essential for land components to continuously carry out intelligence preparations across the theatre to facilitate the deployment and employment of troops and equipment as well as supplies for their sustainability. This is of paramount importance to deter adversary information warfare and to stay ahead of them to establish superiority.

A chief feature of multi domain operation is that, as stalemates escalate into armed conflicts, they often take place or conclude in the land domain (urban terrains). Thus, it is important for land components to be able to operate effectively in urban settings to seize all the available strategic opportunities and exploit enemy vulnerabilities to establish superiority. In order to achieve superiority in multi domain operations generally and urban terrains specifically, land components must first be able to develop great understand their own capabilities in urban terrain operations (CJCSI, 2021). Subsequent to that, they must master the terrain supremely to be able to establish sufficient logistic points precisely on all strategic parts of the terrain to ensure sustainability of their operations. Logistics in this sense has to be reliable agile and responsive to cater the needs of not only land domain but also every other domain that are involved.

The ability of land forces to operate effectively in urban terrains is heavily reliant on the doctrines that govern the tactics of such operations. It is of utmost importance that these doctrines are developed accordingly with respect to adversary capabilities, equipment inventory and tactics in order to be precise and accurate in mission planning. Forces must be split into multiple echelons at various levels across the theatre to ensure maximum utilisation of resources accurately with high speed to push adversary to a state of shock and to render him helpless (Hale, 2020). On top of all these, effective practices of command and control is crucial to ensure the deployment and employments of troop efficiently across all domains throughout the theatre to acquire strategic and tactical gains which increase the speed at which troops operate, the accuracy in information acquisition and delivery of lethal and non-lethal effects onto enemy.

A modern military's land force relies significantly on creative, flexible people who can swiftly adjust to new situations. To be effective, ground forces need to attract and retain talented individuals, then shape them into cohesive units via rigorous training. The high morale and esprit de corps fostered by this shared goal makes the group more effective than the sum of its parts. Land force has little chance of winning without this pool of skill. To be sure, land force relies on human interaction and invention more so than the other facets of military power (Lewis et al., 1998). No part of military might can function without competent individuals, that much is certain. Both air and naval forces rely heavily on weapons systems and support platforms that can't function without human operators. In contrast, land troops often enlist members and then provide them with necessary gear.

LAND DOMAIN CHALLENGES

In conducting their multi domain operations. Land domains are mainly served with two fundamental challenges which is time and distance. As mentioned earlier, multi domain operations is not entirely based on armed conflicts. However, armed conflict is the eventual direction that it heads towards after sufficient stalemate is achieved by adversaries to an extent where a nation is held paralysed. When it eventually ends in an armed conflict, land forces have to be ready and prepared to overcome the constraints of time and distance since the multi domain is a high-speed realm where adversaries do not entirely rely on kinetic and lethal means to attack (McConville, 2021). Thus, land components must possess the ability to conduct swift operations to deter, deny, engage and fix these challenges. In addition to that, the land is largest physical domain of operation in which a military force operates. Therefore, it is vital for land components to be able to operate

throughout the theatre to deny enemy to gain advantage within the domain and overpower them to seize every opportunity that arise within the domain.

Joint Forces must be ready and able to converge at range and speed to win the operational battle in forward regions (Pamphlet 525-3-1, 2018). It is no longer practical to confront state actors after having to start from scratch. Before, this would have been accomplished by projecting power from home base. In disputed arenas, nothing can replace the dynamic presence of formations. The Army's troops are well suited to develop such a presence because of its organisational make-up, which includes a wide variety of capabilities that allow for both depth of reach and speed, and which also benefit from substantial land power networks with allied militaries. The Joint Force must have a competitive, Calibrated Force Posture (CFP) in order to enter into a crisis or war. If the force is not prepared for a crisis from the outset, state actors will not give it the time it needs to assemble and deploy military force, severely undermining the capacity of national decision makers to impose their will.

Land force is necessary to strengthen connections with allies and partners in the event that the enemy seeks to outflank the Joint Force in competition. Alliances and partnerships provide every nation a significant edge in competitiveness, but it is by no means certain that this advantage will be maintained in the contemporary struggle for regional and global leadership. Alliances and collaborations that are win-win are, thus, essential. Land components allow the Joint Force to offer quick reaction options in any crisis through cultivating mutually advantageous alliances (David et al., 2017). Adversaries often try to avoid or shorten the length and scope of open confrontation. With this goal in mind and the emergence of capabilities to impede intervention, adversaries will shrewdly position themselves to either achieve their strategic goals without fighting or to seize their objectives quickly as a fait accompli before they reach the point of no return and resort to open hostilities.

Adversaries are constantly on the lookout on the conduct of operations, procurement of equipment, change in doctrines and exercises by homeland forces to tailor made and design their tactics in ways that will overpower and overwhelm that of homeland. This poses a great challenge for land forces in the conduct and practice of their operations as they will need high level of flexibility, versatility and freedom of action in conducting operations in ways that will be out of reach and out of the anticipatory capacities of adversaries (Guha & Galbreath, 2018). It also requires land forces to be able to sustain

longer in the theatres to withstand, overcome and eventually overwhelm adversaries' capacities and capabilities. Due to the advancements in the range, speed, lethality, and accuracy of opponent weapon systems as well as the global presence, basing, and activities of adversaries, the Joint Force should expect to face continual engagement throughout the battlespace. It will be difficult to find permissive locations, and the country will no longer function as a refuge; this will make it more difficult to generate forces and deploy them.

Adversaries will use novel multi domain combinations to disrupt Joint Force links because they are aware of the significance of joint and combined integration to the conduct of war. Attacks on essential military infrastructure, intense multi domain warfare, and unique opponent force designs are the three major methods in which the enemy will try to break apart and dissolve the Joint force. In times of rivalry and war, the electromagnetic spectrum (EMS), space, and cyber domains will continuously disrupt Command and Control (C2) for ground operations as part of joint operations. Isolating dispersed units increases the likelihood of failure during times of crisis and war if adequate joint C2 is lacking (Liy, 2018). Adversaries will develop new capabilities that are equal to or superior than those of the Joint Force. Dual-use, disruptive technologies like artificial intelligence, materials science, and biotechnology will usher in these capabilities as they become more accessible to a wider audience. The Joint Force has to adapt to counter the increasing sophistication of our enemies' military, which is increasingly based on technology developed in the 21st century.

Multi-domain theatres are very volatile and fluid as to pose threat in various direction and forms to an operating force. Although attrition is not main agenda, it demands a high degree of sustainability from troops operating in this realm (S. Biddle, 2010). As mentioned earlier, achieving stalemate is the immediate and initial objectives of adversaries which will require land forces to be resilient to distractions, disruptions and harassment. They must be aware that this is not an immediate but a prolonged process. Although they will physical attrition will not take place (yet), it will erode their readiness and will to fight. Therefore, force projection assessment and planning are necessary. Land forces must develop and establish communication linkages with representatives from every domain to stay in a common grid of battle rhythm with all stakeholders and abreast of adversaries. This is aimed at improving their sustainment and protection. When armed conflict finally initiates, land forces must make use of novel techniques to dynamically position its units, equipment, and troops so that it may

swiftly narrow the distance with our adversaries in the first fight and win right from the start (Black et al., 2022). Both defensive and offensive measures will be able to be sustained, enabled, extended, and expanded in reach throughout all warfighting domains thanks to the capabilities of the Army.

During multi-domain operations, both the adversaries and security forces will aim to expand the battlefield as much as possible as allowed by their technological capabilities. This is mainly to integrate as many subdomains as possible into the theatre to weaken each other. As far as the multi domain is concerned, expansion of the battlefield means employment of more and more ground troops into the theatre to withstand, produce and deliver mass lethal effects onto the adversary (McConville, 2021). The advanced capabilities and capacities of the opponent will need the deployment of vast numbers of covert, deadly "inside troops" that can move quickly, aggregate and disperse themselves according to the situation, and have a low signature. During large-scale combat operations, these low-signature forces will replace static, high-signature operational outposts while constant displacement will be the norm: units will have a tendency to have broad fronts, will rarely have secure flanks, will engage in compartmented battles, and will not have air and naval superiority. Since this would be a non-contiguous battlespace, commanders will need to be able to combine long-range precision shots and produce impacts that span several domains.

Given the interconnected nature of multi domain operations, the Army, which is a component of the land domain, is not restricted to using just forces from the theatre of operations in its fight. They plan to work together to strengthen their ability to threaten an enemy's strategic flank, seize vital global territory, and protect vital lines of communication (Roderick, 2021). It will be essential to combine these forces in order to counter the dangers presented by equal adversaries with global reach and land-based expeditionary capabilities. Future non-linear battlefields have chances for asymmetric methods, which may acquire relative advantage and present the opponent with many operational challenges while simultaneously expanding the battlespace. Forcible entrance, raids, and close battles will be used by the Army to grab and hold critical territory, manage resources, and protect people, particularly in segmented areas. If used effectively, asymmetric techniques may provide the Joint Force the upper hand against a technologically and numerically equal but more numerous oppositions.

Multi-domain operation concerning the land domain does not deviate far from the fundamental philosophy and tactics of ground combats. As such being the case, adversaries will always seek to achieve superiority through the delivery of long-range fire onto security forces, especially to their rear. Deep striking capabilities is a proven measure of key victory. Therefore, land domains must always operate in a way that their theatre is expanded beyond the reach of enemy fires. In line with that, the expansion must also constrict adversary of his freedom of actions and manoeuvring windows to constrict him and engage him to destroy him ultimately. However, a major shortcoming in the natures of multi domain operations is the integration of information and technology realms in the course of operations (Watling & Roper, 2019). As far as log range fires are concerned, adversaries have now developed Inter-Continental Ballistic Missiles (ICBM) with GPS and satellite guidance which has the capabilities of travelling thousands of miles into our territory with substantial accuracy. These weapons aim to neutralise strategic installation and equipment. Therefore, and added responsibility of forces operating in land domain is to deter these capabilities and safe guard critical strategic assets.

Land domain may employ unmanned systems' advantages in deep operations to accomplish surprise, simultaneity, and speed. The flexibility of deep operations should be maximised so that it may hit the greatest operational value targets, such as those who are either able to or are planning offensive actions against our troops. The adaptability and reactivity of deep operations will be enhanced by the development of ISR supported by machine learning. In order to effectively counter the enemy's strategic plan, deep operations are required. In order to provide a more advantageous correlation of forces in the immediate region, tactical actions will limit the combat effectiveness of enemy forces that have not yet come into touch with one another. Interdiction at both an operational and strategic depth will generate wide-ranging impacts on the operational level.

CONCLUSION

Warfighting scenarios that are used to create, assess, and evaluate prospective choices for risk and opportunity need to adapt as the joint operating environment continues to grow across warfighting domains and geographic areas. The temporal horizons of force employment, force development, and force design should be clearly connected wherever possible throughout the scenario design process. Because of this, the invention and testing of really innovative methods of military conflict are made possible. The scope of land domain involvement in multi domain operations will be vast. Challengers on a

global scale are called peer adversaries. They don't stay inside the predetermined jurisdictions of the several Combatant Commands. The scenario also takes into account the fact that various strategies for success may be needed depending on location. Countries who are at war have political systems that allow them to prepare strategically over a period of decades, rather than years. Land forces, if it is to maintain its relevance and effectiveness, must seek a coherent conceptual image from a future perspective and broaden its temporal framework. Strategic settings of rivalry, crisis, and war will all be included in the Global Near-Peer Scenario, with their full ramifications throughout the government taken into account. Several processes work together to shape the modern Army, including the gradual refinement of doctrine and the growth of new ideas.

Following pointers can be taken as a guide in developing a more sustainable land domain in facing multi domain realm in the future:

- Military overmatch at every level is ensured by long-range precision fires that allow multi domain troops to infiltrate and kill adversary strategic installations from which their fundamental capabilities are generated.

- In the future, multi domain operations involving ground troops will place a premium on mobility, but manoeuvrability will be the primary issue. Next-generation combat vehicles provide ground troops an advantage in battle by increasing their firepower, speed, and survivability, and by allowing them to work in tandem with robotic vehicles.

- The land domain forces should take advantage of inter-domain integration. Under these conditions, new vertical lift platforms and technologies will expand the operational reach and efficacy of ground forces against near-peer rivals by enhancing their mobility, endurance, lethality, and survivability. Hence, it is crucial to invest heavily on the land domain's aviation capabilities.

- Protecting the Joint Force, allies, and partners against human and unmanned air and missile threats is the responsibility of air and missile defence capabilities. The greater a land force's ability to defend its airspace, the safer the air domain will be, not only for the use of land forces but for the benefit of all other domains, from which dominance in operations can be established.

REFERENCES

Balboni, M., Bonin, J., Mundell, R., & Orsi, D. (2020). *Mission Command of Multi domain Operations*.

Biddle, S. (2010). *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton University Press. http://hdl.handle.net/10945/38372

Biddle, T. D. (2019). *Air Power and Warfare: A Century of Theory and History*. https://press.armywarcollege.edu/monographs/378

Black, J., Lynch, A., Gustafson, K., Blagden, D., Paille, P., & Quimbre, F. (2022). *Multi domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea*. www.rand.org/about/principles.

Chase, H. W. (2020). The Fantasy of MCDP 1. *Marine Corps Gazette*, 33–37.

CJCSI. (2021). *JOINT STRATEGIC PLANNING SYSTEM*. https://www.jcs.mil/Library/

Csengeri, J. (2021). Multi domain Operations-A New Approach in Warfare? *International Scientific Journal Of Security & Future*, *5*(3), 78–80.

David, G., Perkins, G., & Army, U. S. (2017). Multi domain Battle Driving Change to Win in the Future. *MILITARY REVIEW*, *6*.

Easterling, J. (2016). *Multi domain Battle: Combined Arms for the 21st Century*.

Guha, M., & Galbreath, D. J. (2018). *"The Multi domain Battle Concept: A Preliminary Assessment."* https://www.researchgate.net/publication/334451700

Hale, A. (2020). Countering Threats in The Future Operational Environment. *Military Intelligence Professional Bulletin*, *34*(20), 5–120.

James, T. S. (1997). *Campaign Planning: An Effective Concept For Military Operations Other Than War*.

Johnsen, W. T. (2014). *Re-examining the Roles of Landpower in the 21st Century and Their Implications*. https://press.armywarcollege.edu/monographs/474

Joint Publication 3-01. (2017). *Countering Air and Missile Threats*.

Joint Publication 2-01.3. (2014). *Joint Intelligence in the Operational Environment*

Lewis, Leslie., Schrader, J., Schwabe, W. L., & Brown, R. A. (1998). *Joint warfighting capabilities (JWCA) integration*. Rand.

Liy, J. L. (2018). *Multi domain Battle: A Necessary Adaptation of US Military Doctrine*.

McConville, J. C. (2021). *Army Multi domain Transformation: Ready to Win in Competition and Conflict*.

Pamphlet 525-3-1. (2018). *The US Army in Multi Domain Operations 2028*.

Pamphlet 525-3-8. (2018). *The U.S. Army Concept for Multi domain Combined Arms at Echelons Above Brigade, 2025-2045*.

Reilly, J. M. (2016). Multi domain Operations A Subtle but Significant Transition in Military Thought. *Views*, *Spring*, 61–74.

Roderick, E. E. (2021). *New Weapons, New Options: Electronic Attack in Multi domain Operations*.

Townsend, G. S., Army, U. S., Crissman, M. G. D., & Mccoy, M. K. (2019). Reinvigorating the Army's Approach to Mission Command It's Okay to Run with Scissors (Part 1). In *MILITARY REVIEW ONLINE EXCLUSIVE* (Vol. 4).

Watling, J., & Roper, D. (2019). *European Allies in US Multi domain Operations*. www.rusi.org

Wilde, J. H. (2019). *An Unfavorable Mismatch: The Inherent Conflict Between the Marine Corps' Maneuver Warfare Doctrine and its Manpower Systems.*

Wormuth, C. (2020). *The Role of Allies and Partners in U.S. Military Strategy and Operations*. www.rand.org

CYBER WARFARE – CHALLENGES AND FORCE READINESS

By LT KOL Ts. ZULKHAIRI BIN OMRAN
ROYAL ELECTRICAL AND MECHANICAL ENGINEERS CORPS

INTRODUCTION

"Cyber warfare is as much about psychological strategy as technical prowess." – **James Scott**

Mankind has waged war throughout the start of history, moving from sword battles to unmanned aerial vehicles strikes in this day and age. All of this war is conducted to further national agendas in an ever-changing international game of power. As time passes by, the wage of war has driven the advancement of technology. The development of armoured vehicles, aircraft, ships, artillery and the use of electronics and telecommunications has increased the complexity of warfare and expanded the battle space. The more advanced a country is in terms of its technology, the more advantage it has over its adversary. The emergence of cyber warfare in this 21st century has branched many new strategic possibilities and threats, causing unprecedented actions all around the world.

The 21st century has seen the rise of Internet and it has become a 'must' for society in this day and age to live with. Almost every smartphone user in this world has some sort of social media (Facebook, Instagram, and Twitter) or instant messaging applications such as WhatsApp or Telegram. Any information can be obtained via Google through a quick tap on the phone or even just voicing it out, making information far more accessible than it was in the 20th century. The banking industry has used this to their utmost advantage and all the banks in the world are equipped with internet banking which makes online transactions between countries nor continents without a hassle. However, all of these conveniences are more often than not are target for malicious groups or individuals who aims to use this for their personal agenda, thus the rise of the cyber warfare in this century. Increasing media coverage of cyber warfare (Watts, 2011) has helped raise public awareness that cyberspace is an arena of war. Understanding what constitutes and the terms use in cyber warfare will further increase awareness among the general public.

TERMS USED IN CYBER WARFARE

There is always a constant confusion in the area of cyber warfare as there are no clear terms or agreed definitions worldwide. Defining these terms in the paper will remove the confusion caused and better address the issues at hand. First of all, what constitutes as cyber space?

Kuehl's (Robinson et al., 2014) research has identified four aspects of cyber space that a definition should reflect, encompassing:

- An operational space – People and organisations use cyberspace to act and create effects, either solely in cyberspace or across into other domains.

- A natural domain – Cyberspace is a natural domain, made up of electro-magnetic activity and entered using electronic technology.

- Information based – People enter cyberspace to create, store, modify, ex-change and exploit information.

- Interconnected networks – The existence of connections allowing electro- magnetic activity to carry information.

Thus, the definition of cyberspace offered by Kuehl in his own words are as follows:

"A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies."

Second, the definition of cyber warfare. There have been many different definitions of cyber warfare used in mainstream media and as such, there are no agreeable definition. Jeffrey Carr defines cyber warfare as such:

"Cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood." (Robinson et al., 2014).

This definition is a bit contradicting as a cyber-attack on a critical national infrastructure such as power grid and hospitals may result in the loss of life. Robinson however argues that cyber warfare is defined as the use of cyber-attacks with a warfare-like intent (Robinson et al., 2014). Through his research, he uses the actor and intent definition model as it gives the definition a more comprehensive meaning. He states that this model goes through a methodical process whereby definitions of harmful events in cyber space can be described. The idea behind this model is to break down any hostile cyber situations into two basic concepts which are: an actor launching a cyber-attack, with some kind of harmful intent.

Third, defining information warfare. Information warfare may seem simple to understand, however there is more underlining it. Libicki suggests that the term information warfare needs to be broken down into smaller parts for it to become understandable and meaningful (Robinson et al., 2014). He describes it as follows:

Form	Description
Command-and-control	Attacks on command centres, or commanders themselves to disrupt command effectiveness
Intelligence-based	Increasing your own situational awareness while reducing your opponent's
Electronic	Use of cryptography and degrading the physical basis for transferring information (e.g. radar jamming)
Psychological	Use of information against the human mind. Propaganda to demoralise troops or influence civilian populations
Hacker	Exploitation of viruses, logic bombs and trojan horses to attack computer systems
Economic information	Possessing and being in control of information leads to power
Cyber	Information terrorism, semantic attack, simula-warfare, Gibson-warfare

Table 1: Libicki's Seven Forms of Information Warfare (Robinson et al., 2014)

This clearly shows that the term information warfare used is very broad but goes beyond the cyber space. These three definitions: cyber space, cyber warfare and information warfare are three important terms that needs to be defined clearly in order to have a comprehensive understanding of the concept of the challenges in cyber warfare.

OPERATIONAL BOUNDARIES OF CYBER WARFARE

Cyber warfare has created a new boundary that has never been seen before by mankind compared to the traditional boundaries which are physical. Battlespace as defined by Gazula is to signify a unified military strategy to integrate and combine armed forces for the military theatre of operations, including air, information, land, sea and space to achieve military goals (Gazula, 2017). This also includes the environment, factors and conditions that must be understood to successfully apply combat power, protect the force or complete the mission. Before delving more into the operational boundaries of cyber warfare, the four traditional domains of war fighting landscape needs to be explored first. They are the lands domains, sea domains, air domain and space domain. All these respective domains belong to each service, namely the Army, the Navy and the Air Force (including the space domain). However, the rise of cyber warfare raised a question mark of which service is responsible for the cyber domain? Is it the Army since most computer services or hardware are found on the ground, the Navy since internet cables are mostly passed through underwater or the Air Force since modern internet data are passed using geostationary satellites? As such, it still remains as a question mark and the best way to tackle this is through a coordinated centre to fight cyber warfare. Cyber warfare, which is a man-made and newest domain of warfare, is still significant as other domains. Military plans have not fully adapted yet to this new way of fighting since there is not much military history or experiences to draw upon when developing plans and strategies.

CYBER WARFARE AS A DATA WEAPON

The fast-evolving nature of warfare and the surge of non-traditional threats has changed the playing field. The nature of warfare is always marked by ‘Volatility, Uncertainty, Complexity and Ambiguity (VUCA)’. Non-traditional threats range from terrorism, crime, cyber, environment, disaster and humanitarian crisis. The idea of using logical bombs to attack a cyber-infrastructure is easy to understand, but carrying out these attacks without a strategic purpose is not effective and doesn't distinguish one from other chaotic cyber-partisans. The real advantage of any type of warfare comes from integrating it with other forms. In the kinetic warfare doctrine, troops on the ground moves forward after aerial attacks have severely damaged enemy positions. This is done through various methods of reconnaissance and intelligence-gathering methods. Gazula argues that ‘combined warfare’ comes in to play when the troops on the ground are able to call for close air support, artillery strikes or armour to support their mission, but

what happens when the concept of information – both as a weapon and as an objective to be attacked or captured – comes into play? (Gazula, 2017).

In the realm of information warfare, there are two main objectives that are competing for dominance: controlling information by gaining access or denying access to it, and influencing the information. These objectives may seem vague and unrelated to warfare, but they can have significant tactical implications. For instance, denying access to information could involve using logical attacks to manipulate an air defense system's radar data, which could provide the invader with a tactical advantage by obscuring the scale and composition of the attack and maintaining surprise until the last possible moment. On the other hand, using kinetic warfare to achieve the same effect, such as bombing radar installations, would result in losing the element of surprise and only denying information about the attack's early stages. The influence factor could cause the radar systems to show false positives, making the data unreliable and degrading the quality of decisions based on that data. Attacking a bank or civilian target is not considered more aggressive than restricting the scope of an attack on military targets. This is considered as ‘hard threats’ and it is usually hard to prove without any strong evidence.

Cyber warfare is more generally known to contribute towards ‘soft threats’ such as espionage, propaganda and denial-of-service attack. Edward Snowden, a former computer intelligence consultant from the National Security Agency, dubbed as the biggest whistle blower in the history of the United States, had disclosed thousands of top-secret documents about the United States intelligence agencies’ surveillance towards American citizens (Davies, 2019). This came as a surprise to the citizens as the government that they have faith and put trust in has been spying on them for their own personal agenda instead. The U.S intelligence agencies have been abusing the privacy of its citizens by collecting and intercepting communications from all of its citizens under the pretext that they just might need the information in the future and just to see if there is anything interesting popping up. This clearly shows sabotage (not in the traditional way between two nation states) but shows how far the government is willing to go for information warfare.

The all-time famous case study of Stuxnet, which happened in mid-July 2010, is a clear example of sabotage through cyberwarfare. Stuxnet is a malicious computer worm that was first discovered in 2010 and targets supervisory control and data acquisition (SCADA) systems. This virus was developed by the intelligence agencies of the United

States and Israel with the intention to derail the Iranian program to develop nuclear weapons (Fruhlinger, 2022). Stuxnet was designed in a way to attack all layers of its target infrastructure which are Windows (Windows XP at that time), the Siemens software running on windows that controls the programmable logic controllers (PLCs), and the embedded software on the PLCs themselves. The virus then proceeded to vary the rotation speed of the centrifuges in the Iranian nuclear facility causing more damage than normal wear and tear. This raised alarm initially by the International Atomic Energy Agency (IAEA) but it wasn't until the virus was spread to the general public that it was identified. This was because the virus was designed to be delivered via a removable drive such as USB stick and since the nuclear facility is an air-tight facility, it is still not clear to this day how the virus got out. This shows how cyber warfare has been used to sabotage nation states through sabotaging their critical infrastructure. Although this does not cause any harm to human life, it is still critical to show how cyber weapon is still dangerous when it falls to the wrong hand.

Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack is the most common form of attack in the cyber warfare world. The biggest DDoS attack happened to Estonia in 2007. Estonia, a country which built on having a high-tech government and economy, was crippled down in a day when multiple banking systems and government servers were down, some which lasted for weeks (The Associated Press, 2009). A normal government and bank websites that gets 1,000 visits a day were crashed when the attackers launched 2,000 visits within a second. The attackers used globally dispersed and virtually unattributable botnets of 'zombie' computers which made identifying the attackers extremely difficult and until this day, the main culprits behind this attack are still unknown. Although Estonia claims that Russia was the main culprit behind it due to the Bronze Soldier statue issue, there were no conclusive evidence that points towards Russia. Estonia which is a nation member of North Atlantic Treaty Organization (NATO), raised this issue to NATO and it became increasingly alarming that the attack could have been more devastating if critical infrastructures such as water supply, air traffic controls, power grid or military weapon systems were targeted (Herzog, 2011). This prompted NATO to enhance their cyber defence capabilities and make cyber-attacks a criminal offense. The main threat that lies here is that the national sovereignty of a nation can be easily threatened through the use of Internet by non-state actors and also, state actors.

CYBER WARFARE CHALLENGES IN MALAYSIA

The increasing reliance of digital technology and the growing complexity of cyberspace including the rise of Internet of Things (IoT) and Industrial Revolution 4.0 (IR 4.0), have made it easier for malicious actors to launch cyber-attacks that can disrupt critical infrastructure, steal sensitive data and cause significant economic damage. The Malaysian Armed Forces (MAF) website was hacked back in 2020 and that was the first publicly known incident of cyber-attack towards the MAF (Bernama, 2020). Although the damage was very minimal, this shows that cyber-warfare is a key area that needs to be paid attention by the Ministry of Defence. The challenges faced in Malaysia are as follows:

- **Lack of awareness**. One of the most significant challenges faced in Malaysia in dealing with cyber warfare is the lack of awareness among the general public about cyber threat (Bernama, 2021). Cyber Security Malaysia reported that an average of 31 cases of cyber-crimes were being reported in Malaysia and that amounts to roughly around 900 cases in a month and up to 10,000 cases in a year (Meikeng, 2021). This clearly shows that the general public is still unaware of the importance of cyber security and the need for adequate security monitoring tools. This lack of awareness has made it easier for cyber attackers to exploit vulnerabilities in computer systems and network. In 2021, Cyber999 Help Centre recorded fraud, hacking and dangerous codes as the top three offences reported. The public needs to equip themselves with knowledge on cybersecurity, the latest technology and to always be on alert to the latest form of cyber threats. The Malaysian government has recently launched the #BeCyberSmart campaign to promote cybersecurity best practices through engagements to reach out to citizens (Bernama, 2023). In January 2023, the MAF released a statement regarding a new hacker group, identified as Dark Pink, has been using phishing emails and advanced software to compromise military defences in Malaysia and several other countries. The modus operandi for these hackers is executed through phishing email sent towards official email networks used by several agencies in the Ministry of Defence and the MAF. However, hacker activities were detected early and preventive measures were implemented as soon as possible thus the MAF communication network exposed to internet access is found to remain secure. These hackers are not only a threat to MINDEF and MAF but also a threat to the National Defence Strategic Communication Network.

❖ **Shortage of Skilled Personnel**. Cyber security requires specialized skills and knowledge, and there is currently a shortage of trained cyber security professionals in Malaysia. Fortinet, a global leader in the world of cyber security, reported that this talent shortage has indirectly caused security breaches and subsequently loss of money (Othman, 2022). This skills gap remains a top concern for almost all C-level executives and is becoming a top priority since most business and organisations are more digitalised nowadays. The shortage of skilled personnel could be attributed to the better pay and demand in overseas compared to in country. These attracts more graduates to work in Western countries where the pay and benefits are much better. Local small and medium business enterprises (SMEs) need to offer better attractive salary and benefit package so that local graduates will be attracted to work in country than moving to overseas. Another reason is because of job upskilling. Some companies do not offer job upskilling to its IT workers, hence they tend to find companies that are willing to send them for professional courses that can increase their skills (Othman, 2022). Training and certifications to increase employees' education is crucial because this shows that their cybersecurity knowledge is validated. This is very important in the terms of cyber security as the threat is always ever changing and people working in the cyber security sector needs to constantly be up to date with the current threats, plus learn how to defend or minimize the damage from the threat. Fortinet in its report found that finding and retaining the right people to fill critical security roles ranging from cloud security to security operations center analysts as a main challenge. Almost 60% of organisation leaders in Asia struggle with recruitment and to maintain talent (Othman, 2022).

❖ **Limited Resources**. Although Malaysia has recognised the critical significance of cyber security and cybercrime, the resources allocated for this commitment is still not enough to combat the cybercrime in Malaysia. The rise of Covid-19 saw the value rise in e-commerce, from 8.5% in 2019 to 12% in 2020. This surge has opened doors of opportunity for hackers and fraudsters to exploit the innocent public. Under the 2023 Budget, the government has allocated RM 10 million to the National Scam Response Centre (NSRC) to upgrade its equipment and start a campaign to raise awareness as well as promote the NSRC's 997 hotlines. Cyber-Security Malaysia (CSM) which is under the Ministry of Communications also received an increase in allocation from RM 27 million in 2021 to RM 73 million

(Bernama, 2023). This increase in budget is good but it is still not enough to keep up with the constantly evolving nature of cyber threats. The limited resources have also made it difficult to recruit and retain skilled cybersecurity personnel, which is essential in developing an effective cyber defence strategy.

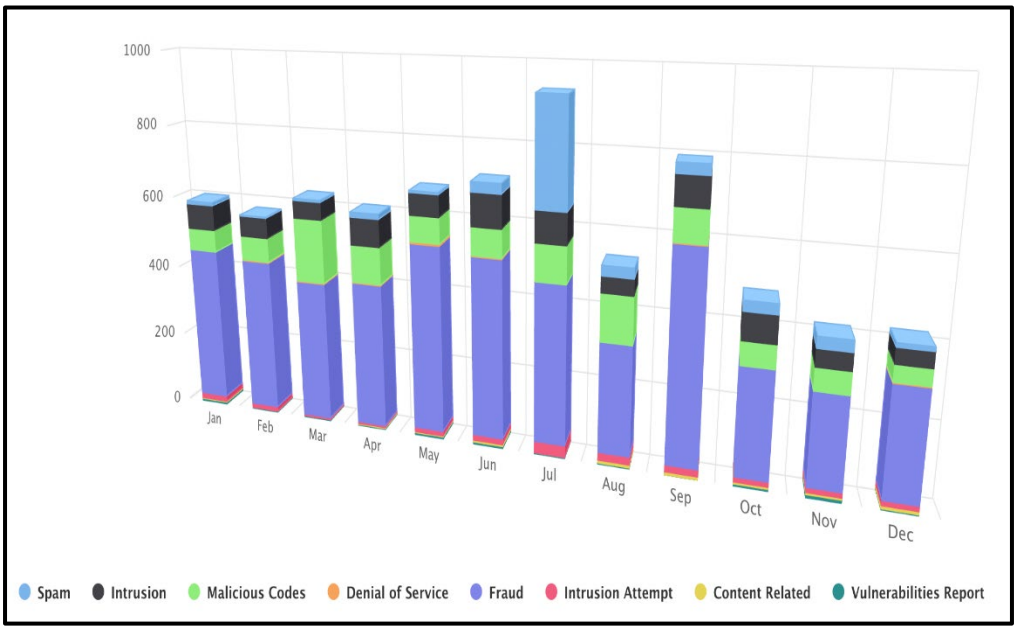

Figure 1: Reported Incidents Based on General Incident Classification Statistics 2022 (MyCert, 2022)

Based on **Figure 1**, it is evident that fraud is the main cyber-crime that is happening in Malaysia, followed by malicious codes. The latter is much more dangerous to the Malaysian Army as malicious codes enables malicious actors or hackers to develop a backdoor code to the computers used in the Army. Malicious codes could easily be embedded within a certain software and saved into a USB flash disk. If the USB flash disk is sticked in to the computer, the malicious codes can infect the computer and spread wide into the internal system and interrupt the cyber defence system. Malware that primarily impact individual users or organizations may spill over and have effects at the national level, especially when a large number of individuals are affected. As an example, the Conficker worm was first identified in November 2008, had infected more than 12 million computer uses worldwide had a national security impact in several countries. The French Navy had to ground several aircraft as their flight plans could not be downloaded into the cockpit system and the Germans had to replace their computers since it could not be used anymore. Hence, that's why public awareness is important for the citizens including military personnel so that incidents like this can be avoided.

FORCE READINESS IN MALAYSIA

Cyber security is not the job of a single organisation but a collection of effort from multiple organisations with the same aim. The Army in the Army 4nextG plan has laid out the development of Network Centric Operations (NCO) and the MAF has established the Cyber Defence Operations Center (CDOC). The CDOC is a one-stop center to handle mitigation towards national cyber security incidents and also ensure confidentiality, integrity and availability of information are achieved. The CDOC has equipped itself with the global cyber warfare and cyber defense grade vulnerability management, security management and network management. The network management aims to provide unify CDOC facilities monitoring and the security management will provide web and portal traffic monitoring. The vulnerability management is the most crucial as it will perform vulnerability assessment, penetration testing, offensive and defensive cyber warfare/ security operations that covers network, server, wireless, database and web application. This shows that the MAF takes cyber security seriously and constantly prevents attacks from malicious actors.

The government has also been making significant efforts to improve its cybersecurity posture in the last two decades. Malaysia has established Cyber Security Malaysia (CSM) in 2007 which is an agency responsible for developing and implementing policies and strategies related to cyber security in Malaysia. This agency also provides training and education programs to raise awareness about cyber security among government agencies, businesses and the general public. Under CSM, it also operates the Malaysian Computer Emergency Response Team (MyCert) which consists of specialists and analysts in the areas of incident handling and malware research. MyCert acts as an independent reference and coordination point for affected Malaysian hosts in a security incident. Rapid response through incident detection allows MyCert to defend national interests, organisations, and companies from further unauthorised activities and minimising the damage sustained from computer security attacks.

The National Security Policy which was formulated in 2006 was specifically developed to address the risks to the Critical National Information Infrastructure (CNII). There are 10 CNII sectors which are National Defence and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; and Food and Agriculture. All of these sectors are highly interdependent between another which makes it important that a comprehensive programme and frameworks are

installed in place. This will ensure the effectiveness of cyber security controls over vital assets and the CNII sectors are protected to an adequate level.

In February 2017, the government established the National Cyber Security Agency (NASCA) as the national lead agency for cyber security matters. The main objective of this agency is to secure and strengthen Malaysia's resilience in facing the threats of cyber-attacks, by coordinating and consolidating the nation's best experts and resources in the field of cyber security. This agency launched the Malaysia Cyber Security Strategy (MCSS) 2020 – 2024 in October 2020 to achieve Malaysia's goals of protecting government and CNII networks, system and data, as well as businesses and citizens, while at the same time combating cyber-crime. This strategy outlines five pillars as its main key area:

- **1st Pillar**: Effective Governance and Management.
- **2nd Pillar**: Strengthening Legislative Framework and Enforcement.
- **3rd Pillar**: Catalysing World Class, Innovation, Technology, R&D and Industry.
- **4th Pillar**: Enhancing Capacity and Capability Building, Awareness and Education.
- **5th Pillar**: Strengthening Global Collaboration.

These five pillars have a broader objective of transforming Malaysia into a global cybersecurity powerhouse by cultivating local talent. In order for this strategy to be realised, the needs to be a sense of inclusiveness among all stakeholders. All roles within the cyber security ecosystem that are outlined by the strategies are all connected and interdependent, which shows that cooperation will always be a key to aspect in ensuring success, security and peace.

CONCLUSION

In a nutshell, cyber warfare is no longer a stranger in today's day and age, and it is a constantly growing threat to Malaysia and other countries around the world. The cyber domain is a man-made domain that still has no clear operational boundaries and clear agreed definitions. This is a challenging task as military planners cannot only rely on their own cyber security policy alone but have to work hand in

hand with other government agencies to fully equipped themselves with the best comprehensive defence against any cyber threat. The last two decades has shown that information warfare through the cyberspace can bring about devastating effects. To make it worse, this attack can be launched by both state and non-state actors, which makes identifying the threat much more difficult.

The three main challenges that Malaysia faces are lack of awareness, shortage of skilled personnel and limited resources. All of these challenges are actually interdependent among one another whereby all of this challenge needs to be treated equally the same instead of just focusing on one of it. The MAF and government have already taken significant steps to improve its force readiness through the establishment of CDOC and various governmental agencies. The MCSS is a sound strategy that covers all aspects of cyberspace and at the same time aims to protect the CNII. Realising this strategy is not only the government's effort all alone but a collective effort from every stakeholder. Hence, it is important that this strategy is executed in line with the objectives that has been laid out so that Malaysia can always stay ahead of the constantly evolving threat of cyber warfare.

REFERENCES

Bernama. (2020, December 29). Rangkaian Data Angkatan Tentera Malaysia digodam. Harian Metro.

Bernama. (2021, June 10). Cyber Security Awareness still low among Malaysians — zahidi - the sun. The Sun Daily.

Bernama. (2023, March 17). Malaysia faces increasing cybersecurity threats -. News Straits Times.

Davies, D. (2019, September 19). Edward Snowden speaks out: 'I haven't and I won't' cooperate with Russia. NPR.

Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. CSO Online.

Gazula, M. B. (2017, June). Cyber Warfare Conflict Analysis and case studies. https://cams.mit.edu/wp-content/uploads/2017-10.pdf.

Herzog, S. (2011). Revisiting the Estonian cyber-attacks: Digital Threats and multinational responses. Journal of Strategic Security, 4(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Meikeng, Y. (2021, September 19). Online threats continue to spike. The Star.

MyCERT. (2022.). Incident statistics. MyCERT

National Cyber Security Agency. National Cyber Security Agency (NACSA), Malaysia. (2020, October). Retrieved March 20, 2023, from https://www.nacsa.gov.my/

Othman, N. Z. (2022, July 6). #TECH: Cybersecurity skills gap contributes to security breaches in Asia. News Straits Times.

Robinson, M., Jones, K., & Janicke, H. (2014, November 29). Cyber warfare: Issues and challenges. Computers & Security.

The Associated Press. (2009, July 8). A look at Estonia's cyber-attack in 2007. NBCNews.com.

Watts, S. (2011, February 3). Proposal for Cyber War Rules of Engagement. BBC News.

CYBER WARFARE – CHALLENGES AND FORCE READINESS

By LT KOL MOHAMAD FAIZAL BIN ABDULLAH
ROYAL SIGNAL REGIMENT

INTRODUCTION

Any Army organisation must be properly equipped and organised. Equipment is not the only important to be procure but the Army's organisation is far more crucial. Organisation is the precise delivery of the right information at the right time and size. Every Army requires an information and communication network, is reliant on logistics, and is required to understand its adversaries. The information age is evident on the battlefield as much as in business. Faster intelligence dissemination, more accurate communication of enemy movement, more precise unit deployment, and more accurate information-based decision-making are all required. This demonstrates how armies are relying more and more on information, yet they are unaware that this information is a valuable resource that must be safeguarded. Physical security was the focus of all efforts to protect information, such as limiting access, but with the enhancement of networking and internetworking, other threats must now be taken into account.

In the current state of conflict, protecting the sovereignty of digital and cyberspace is just as important as protecting the sovereignty of our region. A breach in cyberspace and digital security could cost people their lives and their political, economic, and social standing. The task of making sure the threat to the country is appropriately defeated has been given to the Malaysian Armed Forces (MAF), who serve as the main forces in preserving the nation's sovereignty. The released of Malaysia Defence White Paper (DWP) makes give the significance role of the MAF's in securing cyberspace because cyberthreats are seen as a non-traditional security threat to both national security and geopolitics. Military operations are now visible to cyber threats thanks to the development of disruptive technologies like artificial intelligence, machine and deep learning, big data, and cloud computing (MinDef, 2021).

WHAT IS CYBERSPACE AND CYBER WARFARE DEFINITION

Before examining what is cyber warfare, a clear understanding of cyberspace is a must. According to (Daniel Kuehl, 2009), he concludes that cyberspace is more than just computers and digital

information, and that there are four aspects of cyberspace that a definition should reflect:

- **An Operational Space** - People and organisations use cyberspace to act and create effects, either solely in cyberspace or across into other domains.

- **A Natural Domain** - Cyberspace is a natural domain, made up of electromagnetic activity and entered using electronic technology.

- **Information Based** - People enter cyberspace to create, store, modify, exchange and exploit information.

- **Interconnected Networks** - The existence of connections allowing electromagnetic activity to carry information.

Kuehl provides his own definition of cyberspace, which he says is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

There are many different meanings of cyber warfare, which is a word that is frequently used in mainstream media. Cyberwarfare, according to (Alford, 2004), is "any act intended to compel an opponent to fulfil our national will, executed against the software controlling processes within an opponent's system." This description from Alford represents the idea that states will use cyberwarfare to further a national agenda. However, one could argue that modern warfare does not necessarily attempt to further such a cause. Possibly, the objective of modern warfare is to spread non-national philosophies and religious convictions. Therefore, it is important to limit a definition of cyberwarfare to having that goal as its primary objective. The idea that cyberwarfare won't result in casualties, however, needs to be called into doubt. Losses of life could happen from a cyberattack on vital national infrastructure, including the electrical grid. It states that cyberwarfare is merely "another term for cyberwar" in the Oxford English Dictionary's definition of the term. The term "cyber war" is defined as "the use of computer technology to interfere with the operations of a state or organisation, particularly the intentional attack of communication systems by another state or organisation."

According to (MAFJD 3-04.5 Cyber Op, 2018), much of cyberspace is located outside of MAF control and crosses geographical and geopolitical boundaries. It is integrated into the management of crucial infrastructure as well as business operations, governmental operations, and national security. Adversaries with internet access have the ability to directly and indirectly threaten the integrity of MAF's essential infrastructure, posing a threat to our Centre of Gravity (COG). Despite the fact that cyber operations can generate independent tactical, operational, and strategic effects to accomplish goals, they must be integrated with the other capabilities of the Joint Task Force to produce synergistic effects in support of the joint operational strategy. While this is going on, cyber operations are taking place in a difficult environment where most of cyberspace is ungoverned. There is a huge variety of both state and non-state actors. Entry barriers are low, and technology is quickly evolving and frequently unpredictable. On the other hand, the MAF cyber troops must be ready to execute operations in a compromised cyberspace environment. They need to create mitigation and recovery plans, Defensive Cyberspace Operations (DCO) priorities, primary, secondary, and tertiary communication channels, as well as safeguards to assure the reliability of essential data.

According to a review of the literature, there isn't a common definition of cyberwarfare. Some scholars provide very wide definitions, which are likely to capture the majority of hypothetical instances of cyberwarfare but may be overly inclusive. Others provide highly detailed explanations that could be more helpful but leave out other aspects of what might be termed cyber warfare. We provide a definition approach based on actor and purpose identification to address this issue.

CYBER WARFARE CHAOS

Given the contemporary climate, where everyone relies completely on the internet, it is imperative to comprehend and learn more about cyberwarfare. Any format or technique will be used to attack the network. What would be safeguarded or defended is still another crucial component of defence. To secure information processes from theft, for instance, as well as information dissemination from assault and protection of networking as a whole. Most often, technological advancement has led to progressive developments, particularly in the area of information sharing and innovation in defence systems around the world, but in today's globalised world, this innovation has also led to vulnerability. Cyber weapons are modern weapons of war, individuals or nations can pick from a variety of

cyberweapons, including syntactic, semantic, and hybrid weapons (Swanson, 2010). They attack computer operating systems that include harmful code, such as viruses, worms, Trojan horses, distributed denial of service (DDoS), and spyware, by utilising syntactic weapons. Using DDoS attacks, a cyber attacker can bring down a website by flooding it with massive amounts of traffic. During the semantic attack, information entered into the computer system will be converted in order to prevent any errors from being made without the handler's knowledge. In other words, the semantic weapon was directed against the accuracy of data that a computer user has a legal claim to.

The term "mixed weapon" refers to a weapon that combines syntactic and semantic weapons. It is also known by the term "blended weapons." With this weapon, an even more sophisticated attack will be made on both the information and the computer's operating system. For instance, according to Swanson (2010), a "bot network," which is a growing number of "bots" secretly installed on other computers, is a variety of weapons. Bots are automatic computer programmes that harm other computers, according to one definition. Anyone with access to its control can use a swarm attack against specific machines to find, copy, and transfer sensitive data. We referred to this guy as a hacker. The attacked computers or networks will thereafter be managed by an attacker from a remote-control location once they have been infected with malicious software (Swanson, 2010).

According to the Global Information Assurance Certification Paper from 2004, information is the most important component of any firm's success. Lack of information security puts us at risk to a certain extent. When it comes to Malaysia's present cyberwarfare concerns, the Critical National Information Infrastructure (CNII)'s adaptability as a defense against cyberthreats is always at the forefront. CNII is characterized as essential national infrastructure, including crucial real and virtual assets, systems, and operations. Their incapacity or damage will have a startling effect on the nation's economy, reputation, defense, ability to run the government, and public health and safety. The confidence of the country's main growth region to be able to compete successfully in the global market while maintaining decent standards of living is a sign of national economic strength. It's crucial to maintain a positive national image in order to increase the nation's stature and sphere of influence.

In contrast to government competence, which is to operate and keep order while performing and delivering the bare minimum essential to public services, national defense and security are to ensure sovereignty and independence while ensuring internal security. All

citizens must get and remain in the best possible condition of health care, according to public health and safety. National Defense & Security, Banking & Finance, Information & Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services, and Food & Agriculture are among the ten sectors that make up CNI. The National Cyber Security Policy (NCSP) was designed to improve the resilience of our CNII because the security of any country against cyberattacks is only as strong as its weakest link or point. The National Cyber Security Policy was created to help Malaysia progress toward a knowledge-based economy (K-economy).

Based on the National Cyber Security Framework, a policy was created. Its topics include laws and regulations, technology, public-private sector cooperation, and institutional as well as institutional features. The systems that don't have an internet connection and have a backup power source, like a generator, are secure from cyberwarfare attacks. On the other hand, every electronic gadget is susceptible to a weapon that uses electromagnetic pulses (EMF). Since information theft is a constant worry and unlawfully obtained information could have a severe effect on the economy of the country, government papers have also been impacted by cyberwarfare. Additionally, from a national perspective, CNII organisations are the targets of cyberattacks, and from an economic standpoint, it may be a company that has significant trade secrets. When systems that are not sufficiently secured are at risk, cyberwarfare can undermine the security system. The sole distinction is how these systems are affected or implicated when they are compromised. Due to Malaysia's reliance on these "foreign" technologies, all systems are susceptible.

CHALLENGES AND FORCE READINESS

Establishing a Security Operation Center (SOC) is one solution for continuously monitoring the quick response to reducing the cyber threat. Since the recent cyberattack, its function in security operations has become more crucial. Organizations are starting to understand how to defend themselves against the growing threat of cyberattacks while also saving money. The majority of organizations have set up a SOC in recent years to address security-related issues and solve security-related problems (White, 2016). Many organizations, including the military, the government, the corporate sector, and even private businesses, use SOC. An efficient SOC operates information security functions, which can serve as the framework for safeguarding an organisation’s network, network infrastructure, and information systems. This enables them to react more swiftly to dangers like cyberattacks, data breaches, and other sorts of attacks.

The security operation centers also monitor network endpoints for vulnerabilities while safeguarding sensitive data and abiding by industry and government standards. SOC keeps an eye on and assesses the network's security, including network traffic, activity, and connections, and searches for unusual activity that might point to a security event or danger. SOC could shorten the gap between attacks and detection while also assisting the organization in staying vigilant against threats. According to the severity of security incidents (ranging from Level 1 to Level 4), **Figure 1** shows how SOC categorizes risk alerts.

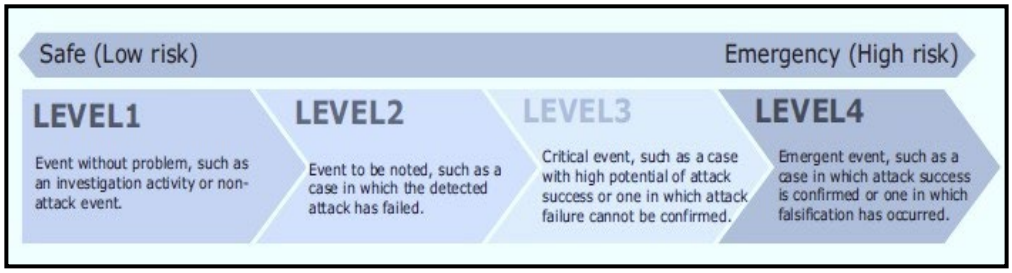

Figure 1: Levels of Security Events (NEC, n.d.).

According to a report from the Center for Cyber Security Research and Development (Petters, 2020), SOC has decreased the frequency of security incidents by assisting organizations to stay at the forefront of all threats. Setting up a SOC is an expensive investment, but if it is designed correctly to give the organization enough protection, it pays off. The typical SOC setup is less efficient and calls for the analyst to have prior knowledge and experience. It is therefore suggested that this task be automated using artificial intelligence technologies to increase the system's effectiveness and efficiency.

A Network Operations Center (NOC) is a frequently used phrase in the realm of network management and network security. Network operations personnel often provide and actively support network monitoring, control, and management services across the whole network at the NOC, according to Wu and Buyya (2015). The NCO carries out the responsibilities of network control, incident response, and upholding uninterrupted service. An essential part of the overall network operation and management system is the NOC.

The NOC team is in charge of overseeing, controlling, and administering the whole network. Since all active networks are present at the NOC's location, it is common for one NOC to oversee and manage a number of geographically scattered sites. In addition to providing network maintenance and management services for

networks affected by network issues both on and off the network, monitoring of servers and services can be carried out at multiple locations to address network issues affecting the network, not just on the servers but also on other components of the system, such as network security, network performance, and performance management (Livinjo, 2020).

A NOC should, in general, make it easier for organizations with vast networks, like MAF, to keep track of their network history without having to handle each component manually and one at a time. Given the limited precision, users who rely on network data should feel confident knowing that security and operations centers are always monitoring networks. The organization's network can be better understood through the use of surveillance software, which may also give valuable information about the network's state and ability to sustain health.

There are a few benefits to having a NOC in services, such as data backup storage on network devices, patch management, software installation, updating, and troubleshooting, antivirus support, report generation on network performance, health, and optimization, management and monitoring of network security software and firewalls, and lastly, attack on the network from inside detection and analysis.

The creation of Network Security Monitoring Center (NESMOC) lead by Bahagian Siber dan Elektromagnetik Pertahanan (BSEP) is a centralized system will benefit MAF in many ways, including cost effectiveness and efficiency. A dependable monitoring system enables MAF to find issues more quickly and with fewer system failures. A unified approach to network monitoring helps the company cut downtime and the amount of time it takes to investigate issues. Employing network monitoring tools to track bandwidth and resource utilization is also a wonderful way to improve network performance. As a result, the MAF can concentrate on optimizing network consumption to allot the necessary and appropriate bandwidth for the associated system. The NOC's use of network monitoring technologies can be used to provide studies and give crucial information for precisely identifying network issues such as network traffic, network performance, and network security.

NESMOC typically keeps command and control of communication between various organizational parts in the hands of a small number of individuals, which helps to improve the organization's communication and, at the same time, reduce the need for human resources, increasing the effectiveness of command and control.

Because the system is automated utilizing machine learning and artificial intelligence, this technology will also limit human engagement with the system, necessitating the use of a minimal number of human resources. A centralized system will offer a reliable, user-friendly solution for network security and MAF system monitoring.

To allow for the seamless integration of new components into the infrastructure, monitoring systems must be agile and flexible enough. Additionally, the network can establish specific monitoring standards, and organizations frequently need the flexibility to modify and enhance the system to meet their objectives. The MAF's modern infrastructure and environment are incompatible with the previous NOC monitoring system's antiquated design. The MAF will struggle to achieve the performance required to guarantee the security and availability of systems and networks inside the MAF environment if the present network management system in use is not adaptable.

CONCLUSION

This article has offered a survey of current ideas regarding the difficulties posed by cyberwarfare. It started by examining the terms already used to describe cyberwar and cyberwarfare and identifying two issues that needed to be fixed. First, it was discovered that neither cyberwarfare nor cyberwarfare have a generally agreed-upon meaning. This is problematic because it is impossible to debate the more complicated concerns or even identify when cyberwarfare is taking place without a common definition. Second, we discovered that the terms "cyber war" and "cyber warfare" are regularly used synonymously. We contended that this was equally problematic because war and warfare have different definitions. By establishing the actor and intent definition model, which more clearly characterised both cyberwarfare and cyberwar, we attempted to address these issues.

Although steps are being taken to address these issues, there are still important research gaps that require filling, some of which have been noted in this work. The most important finding is that there is no one field that can adequately address all of the problems brought by cyberwarfare. For instance, attribution and cyber defence are undoubtedly technical concerns, but effective resolution of these and other problems necessitates political, legal, and societal participation. Similar to this, developing a set of laws for cyberwarfare calls for input from the technical and military on what would be possible to enforce, in addition to legal experts.

In light of this, it is necessary to draw the conclusion that the ideal strategy for future research is a multidisciplinary one. Securing information and networks is the best defence against cyberwarfare threats. All systems, even those not regarded as vital, should have security upgrades installed because any system that is weak can be taken over and used to launch attacks. Comprehensive disaster recovery planning that takes into account potential damage from an attack is necessary, along with contingencies for prolonged outages.

In conclusion, cyberwarfare has a negative influence on national security since it makes it more vulnerable to assault from outsiders. Given that attackers may easily access technology in the modern world, national security should be tightened. The government must ensure that this happens as technology advances.

REFERENCES

Minister of Defense (MinDeF). (2019). Malaysia Defense White Paper, 2020 – 2030.

D. T. Kuehl. (2009). Cyberpower and National Security, Potomac Books and National Defense Univerity, 2009, Ch. From Cyberspace to Cyberpower: Defining the Problem, pp. 24–42.

L. Alford. (2001). Cyber warfare: A new doctrine and taxonomy

Malaysian Armed Forces Joint Doctrine (MAFJD) 3-04.5. (2018). Cyber Operations

Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. Digital Commons at Loyola Marymount University and Loyola Law School.

Petters, J. (2020, June 17). What is a Security Operations Center (SOC)? Retrieved from Varonis:https://www.varonis.com/blog/security-operations-center-soc/

Buyya, C. W. (2015). Data Center Facilities. Cloud Data Centers and Cost Modeling. In C. W. Buyya, *Cloud Data Centers and Cost Modeling* (pp. 153-191). Chicago: Morgan Kaufmann.

CHALLENGES OF THE ARMY TO FACE CYBER WARFARE

By LT KOL DENIS ANAK INGGANG
ROYAL ARTILLERY REGIMENT

INTRODUCTION

Cyber war refers to conducting and preparing to conduct military operations according to information-related principles, primarily against or in defence of military connectivity. It means disrupting, if not destroying, information and communication systems. It also means timing the balance of information and knowledge' in one's favour, especially if the balance of force is not equal. The special characteristics of cyber war are low cost, precision, standoff and stealth.

For many, the term cyber war brings up images of deadly, malicious programmes causing computer systems to freeze, weapon systems to fail, and enemy's technological prowess being neutralized to bring about a bloodless conquest. This picture, in which cyber war is isolated from the broader conflict, operates in an altogether different realm from traditional warfare and offers a bloodless alternative to the dangers and costs of modern warfare, is attractive but unrealistic. Such a scenario is not beyond the realm of possibility, but it is unlikely, at least in the foreseeable future, as of now, cyber warfare will almost certainly have very real physical consequences as well.

Cyber war may have broad implications for military organization and doctrine. It may imply developing new doctrine about the kinds of forces needed, where and how to deploy them, and what and how to strike on the enemy's side. Similarly, questions such as, how and where to position what kinds of computers and related sensors, networks, databases and so forth, are also of utmost relevance. Cyber war would also have implications for strategy, tactics and weapons design. It may be applicable in low and high intensity conflicts, in conventional and non-conventional environments, and for defensive or offensive purposes.

Many have sought to answer this question during the last decade as the internet emerged as a new battlefield in conflict. It is tempting to simply define cyber war as when a nation state engages in cyber operations. However, a definition that restricts actions to a nation state is likely incomplete. Governmental organizations from the more traditional actors such as Hamas and Hezbollah to newer organizations

such as Anonymous and Lulz Sec continue to play an increased role in conflict. However, in extending the range of actors in cyber warfare beyond nation states, it would not make sense to include every two-bit criminal sending out spam e-mails and high-school kids conducting Web defacements as cyber warriors. On the other hand, we cannot make an arbitrary decision based on the size of the organization conducting the attacks.

Clearly, cyber war is difficult to pin down with a definition. Based on Clausewitz's definition of war "an extension of policy (or politics) by other means." Then we can create a corollary for cyber war "an extension of policy (or politics) by actions taken in cyber space." But we also want to avoid considering every politically motivated Web site defacement as an act of cyber war. Perhaps we should also account for capability and add the condition that the actions pose a "serious threat" to national security. However, we still cannot account for cases in which a state uses cyber operations against non-state actors. Cyber war is an extension of policy by actions taken in cyber space by state or non- state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security.

CYBER WARFARE METHODS

The increasing number of internet users resulted in the fact that propaganda is spread more efficiently in cyber space than through leaflets airdropping. The spreading of malware is easier, more available and faster with the increasing number of users. Therefore, the threats of cyber-attacks are also more likely. There are various methods of cyber-attacks in cyber space ranging from the moderate to the merciless ones, such as follows:

- **Vandalism** - common attacks on government web sites. Such attacks are usually fast and do not cause serious damage.

- **Propaganda** - dissemination of political news mainly through internet.

- **Collection of data** - collection of classified information which is not sufficiently protected.

- **Access denial** - attacks against armed forces which use computers and satellites for communication. Orders and reports may be intercepted and altered, which may result in dangerous situations for the army.

- **Network attacks against infrastructure** - attacks on transmission systems of the companies in power engineering, gas industry, heating industry, oil industry and communication infrastructure, which are sensitive to cyber-attacks.

- **Non-network-based attacks against infrastructure** - abuse (or rather utilization) of common computer software and hardware used in internet operation and security. Virus is hidden in hardware, software, or maybe even in microprocessors.

DEFENSIVE CYBER WARFARE

In case of defensive cyber war, it will be important to determine strategically important installations. At present such installations are buildings and the decisive criteria are their geographical locations, equipment, etc. These installations may also be virtual in case of cyber war. In order to prevent an attack or reduce loses and damage it is necessary, prior the attack itself, to minimize the number of input access spots, introduce multiple software security, hardware security and properly screen and train the personnel with network access permits.

Cyber attackers have got a clear goal within easy plan. The key to success is the moment of surprise during attack. The earlier the defender responds to the attack, the easier it may be to stop or repulse it. If such an attack with the moment of surprise is conducted, it is first necessary to stabilize the whole system and thus deal with the surprise.

Second, it is necessary to detect the attack and try to understand the attacker´s plans and intentions. Then the attack may be repulsed. It must not be forgotten that the attack analysis always has to follow. Based on acquired information, the protection of critical infrastructure (hardware and software) has to be increased in order to prevent possible subsequent cyber-attacks.

OFFENSIVE CYBER WARFARE

Firstly, we have to be aware of the aspects of offensive cyber warfare and compare them with traditional aspects. Such a type of war may be more acceptable for public than employing the means of conventional war. Although a cyber-warfare may avoid direct casualties, there are still indirect dangers. Critical infrastructure is somewhere between state and private sectors. It includes water distribution network, electric energy network, air traffic control, and other systems critical for the functioning of a particular country.

Enemy may take advantage of our dependence on cyber space and gain strategic advantage in a possible conflict. It is assumed that a cyber-war would precede a convention. Future possible cyber warfare is reasons for our serious concerns. Unlike tradition situation requiring a vast amount of sources, such as weapons, personnel and equipment, cyber wars require somebody who has got appropriate know-how, computers, and willingness to create chaos. Enemy may be everywhere, even inside the country or organization.

An intense attack may be carried out by only a few hackers with the help of standard computers. Another terrifying aspect of cyber war is the fact that cyber-attack may be either part of a coordinated attack, or it may only be an idea of a malicious hacker with a funny idea. No matter what the attacker motive is, cyber-attacks may cause big financial losses. And many countries are pitifully unprepared to manage such unexpected cyber-attacks.

THE REALITY OF CYBER WARFARE

- **Cyber War is Real**. What we have seen so far is far from indicative of what can be done. Most of these well-known skirmishes in cyberspace used only primitive cyber weapons. It is a reasonable guess that the attackers did not want to reveal their more sophisticated capabilities

- **Cyber War Happens at The Speed of Light**. As the photons of the attack packets stream down fiber-optic cable, the time between the launch of an attack and its effect is barely measurable, thus creating risks for crisis decision makers.

- **Cyber War is Global**. In any conflict, cyber-attacks rapidly go global, as covertly acquired or hacked computers and servers throughout the world are kicked into service. Many nations are quickly drawn in.

- **Cyber War Skips the Battlefield**. Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defenses.

- **Cyber War Has Begun**. In anticipation of hostilities, nations are already "preparing the battlefield." They are hacking into each other's networks and infrastructures, laying in trapdoors and logic bombs – now, in peacetime. This on-going

nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability.

THE BATTLE SPACE

Cyberspace it sounds like another dimension, perhaps with green lighting and columns of numbers and symbols flashing in mid-air. Cyberspace is actually much more mundane. It's the laptop you or your kid carries to school, the desktop computer at work. It's a drab windowless building downtown and a pipe under the street. It's everywhere, everywhere there's a computer, or a processor, or a cable connecting to one. And now it's a war zone, where many of the decisive battles in the twenty-first century will play out.

Cyberspace is all of the computer networks in the world and everything they connect and control and not just the internet. Let's be clear about the difference. The internet is an open network of networks. From any network on the Internet that able to communicate with any computer connected to any of the Internet's networks. Cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the internet. It includes private networks look just like the internet, but they are, theoretically at least, separate. Other parts of cyberspace are transactional networks that do things like send data about money flows, stock market trades, and credit card transactions. Some networks are control systems that just allow machines to speak to other machines, like control panels talking to pumps, elevators, and generators.

In the broadest terms, cyber warriors can get into these networks and control or crash them. If they take over a network, cyber warriors could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send a platoon into an ambush, or cause a missile to detonate in the wrong place. If cyber warriors crash networks, wipe out data, and turn computers into doorstops, then a financial system could collapse, a supply chain could halt, a satellite could spin out of orbit into space and airlines could be grounded.

CYBER WARFARE AND ARMED FORCES

The Indian Army way back in 2004 had identified cyber warfare as a means of waging an unconventional war. Despite this, not much effort has gone into developing the capabilities for cyber warfare either by the army or by the other two services.

Strategic cyber warfare targets CII of a nation while operational cyber warfare aims to target battlefield targets. While the former would be undertaken by a strategic force after a clear national mandate has been established and a go ahead has been given by the Government of India, the latter will be undertaken by Field Force Commanders and will form part of any future conflict. It is therefore essential that Armed Forces equip themselves with the knowledge of this form of warfare and also organise themselves for it so that enemy's cyber capabilities do not take us by surprise.

Armed Forces of certain developed nations such as the USA, Russia, NATO and China are well organised for undertaking cyber warfare both offensive and defensive operations. We may follow any of their models for organising our Armed Forces. The United States Cyber Command (USCYBERCOM) is an armed force subordinate to United States Strategic Command (USSTRATCOM) that is one of the nine Unified Combatant Commands of the US Department of Defense. The mandate of the USCYBERCOM is to fuse the Department's full spectrum of cyberspace operations and plan, coordinate, integrate, synchronise, and conduct activities to lead day-to-day defense and protection of Department of Defense (DoD) information networks; coordinate DoD operations providing support to military missions; direct the operations and defense of specified DoD information networks and prepare to, and when directed, conduct full spectrum military cyberspace operations.

The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronising war fighting effects to defend the information security environment. Over 6000 personnel both uniformed and civilians who are working under the USCYBERCOM. A large number of them have undergone training at the United States Army Cyber School, Fort Gordon, Georgia.

CASE STUDY

Cyber warfare can be seen clearly based on case studies reported abroad as follows:

- The cyber-attack suffered by the Japanese Government. That is, on August 4, 2004, there was an attack on the Japanese Government's computer that caused eight Japanese government agencies to experience a simultaneous disruption known as a jamming barrage. It affects the network so that it cannot be accessed for several hours.

- In August 2005, a group of hackers managed to block US Customs computers for several hours. it happened when a computer virus entered the US Customs system and severely affected the computers at the airport in Miami, New York, San Francisco, Los Angeles, Houston and Dallas.

- In May 2007, Estonia was attacked by hackers who disabled internet communication systems and targeted government, banking, media and police websites for three weeks and caused huge economic losses due to disrupted online transactions.

LOCAL ATTACK

In 2001, Malaysia's internet infrastructure was attacked by the Code Red worm. This was a classic example of infrastructure attack in which the worm spread very fast and brought our national communication network to a standstill. It was reported that the relevant agencies took three months to eradicate this worm and the estimated minimum losses was RM 22 million, not inclusive of the losses to the business fraternity and other sectors as well.

Other incidents of cyber-attacks were caused by the Blaster and Naachi worms in 2003. The incident started with the propagation of the Blaster worm through the scanning of vulnerable machines via the network, followed by Naachi worms. These worms exploited the vulnerability found in the Windows NT, 2000 and XP software. The estimated cost to eradicate this worm was about RM 31 million, not including lost productivity and the cost of lost opportunity.

OVERVIEW OF CYBER WARFARE THAT AFFECTED MALAYSIAN SYSTEM SECURITY

In Malaysia, current issues related to cyber warfare are always about the elasticity of the Critical National Information Infrastructure (CNII) as provision for any cyber threats. CNII is defined as properties (real and virtual), systems, and functions that are vital to the nation. Their incapability or damage will give shocking impact to the nation such as economic strength, image, defense and security, impact on government functionality, public health and safety.

The National economic strength is where the self-assurance of the nation's key growth area can able to compete successfully in the global market while preserving satisfactory standards of living.

To enhance national stature and sphere of influence, it's important to maintain a good national image.

National defense and security are to guarantee sovereignty and independence while maintaining internal security whereas Government capability is to functions and maintains order while performing and deliver minimum crucial to public services. Public health and safety, they are responsible for bringing and maintaining optimal health care to all residents. There are ten sectors under CNII, which include National Defence & Security, Banking & Finance, Information & Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services and Food & Agriculture.

The strength of any nation's security, against cyber-attacks, is as strong as its weakest link/point, and the National Cyber Security Policy (NCSP) was established to increase the resiliency of our CNII. To assists Malaysia moving forward to a knowledge-based economy (K-economy), National Cyber Security Policy has been designed. A policy that formulated is based on National Cyber Security Framework. Its covers legislation and regulation, technology, collaboration between the public and private sector, institutional as well as institutional aspects. NCSP seeks to address the risks to the 41 CNII, which comprises the networked information systems often critical sectors.

The issue affected Malaysian system security is any CNII system that is compromised is capable of disrupting the well-being of the nation. It is always a catch-up scenario, as cyber threats are always evolving. The Malaysian system needs to continuously enhance. The knowledge and adopt more IT-savvy in order to stay ahead of cyber threats practices in securing the CNII operations. Besides, the table also explained what would be attacked in the cyber warfare which the Cyber Security stated that if the attack intention is to disrupt the national economy, therefore, any of the CNII organizations are a potential target. When the cyber warfare attacked, the things that are protected are systems that do not have an internet connection and have their independent power supply such as its generator. In contrary, all electronic devices are vulnerable to an Electro-Magnetic Pulse (EMP) type of weapon.

Government documents have also been affected by cyber warfare as information theft is always a concern as the illegally obtained information could have a negative impact on the economic fortune of the nation. On top of that, from the country perspective, the victims that usually attacked by cyber warfare is CNII organizations while from economic perspectives; it could be the business with

valuable trade secrets. Cyber-warfare can harm the security system when any systems that are not adequately secured are at risk. The only differences are in the impact or implication when these systems are compromised. All systems are vulnerable as Malaysia is dependent on these “foreign” technologies.

RECOMMENDATIONS

❖ National Level

The following recommendations are made in the light of the threat that Cyber Warfare poses to Pakistan:

- Formulation of a committee under central government, responsible for monitoring and coordinating information warfare activities, is needed without further delay. This body may be placed under the Defence Minister and could include Chairman Joint Chiefs of Staff Committee, representatives from the three services, intelligence agencies, secretaries from ministries of foreign affairs, communications, science and technology, information and broadcasting, commerce and defence production division, this governing body may be mandated to make national policy to evolve comprehensively in short and long term programmes, procure funds, make allocations to the assigned agencies and monitor progress.

- In the realm of offensive Cyber warfare, and as part of the national ‘TW' policy, there would be a need to determine the desired thresholds by way of stipulating the magnitude and intensity of an offensive application.

- Most countries with advanced TTW' programmes have established a central ‘Computer Emergency Response Team' (CERT) to combat emergencies caused by Hackers. The Ministry of Science and Technology may also be directed to set up such a team in line with American CERT. This would enable control of cyber-crime and fight cyber threat from hackers.

- Making use of the 'Trusted Computer System Security Criteria’, the proposed central IW1 committee may evaluate and determine minimum security levels for all vital military and civilian establishments.

- There is a dire need to introduce and sustain a new (stricter and uncompromising) work place security culture in all departments and functions of the government which would eliminate possibility of action by insiders'' or data loss through theft or neglect.

- Institute measures for increasing education levels of the public and development of human resource in IT. Awareness of policy makers, information system managers and general public on information and cyber security aspects needs to be promoted at the national level.

- Advance training in cryptology to be imparted to selected personnel in-country, and cryptographic software and hardware be developed and procured, as far as possible, through expertise available in country.

❖ **Armed Forces Level**

The recommendations that been suggested are as follows:

- An Information Warfare directorate is set-up at the Joint Services Headquarters, to co-ordinate on Information Warfare activities at national level. A comprehensive Cyber Warfare strategy be evolved based on military and defence policy.

- Information and Cyber Warfare be recognized as the fifth dimension in warfare. Towards this end, may issue required policy directives to all service HQs to initiate development and employment planning.

- Computer literacy of officers and men may be enhanced. At junior levels, competency in computer skills may be made a part of the promotion examinations for officers and men.

- A comprehensive and practicable module be integrated into all single and joint service war gaming and exercises in the armed forces.

- Training and awareness on IW' be enhanced through orientation courses and seminars for officers and men of the three services.

- Protection of Defence Communication Networks, communication systems (exchanges) and operational networks be maximized through the use of fire walls, access codes, multi-layered defences and data encryption. Implementation be monitored through individual services 'IW' Directorates.

- All sensitive establishments be equipped with TEMPEST proof equipment, or specially coated building walls.

- Hiring of civilian computer professionals be encouraged.

- Use of non-licensed software is strictly discouraged.

Recommendations offered in this paper are by no means conclusive and exhaustive because of the nature of the subject and ever emerging new threats and technologies to counter the threats. However, these can serve as a starting point for developing Cyber Warfare strategies at all tiers in a national effort to master this new paradigm in warfare.

CONCLUSION

Military Information Operations have a tremendous cost-effect advantage. Even with limited military resources at its disposal, a nation can launch these operations virtually against any nation of the world with devastating effects. In today's cyberspace, not even institutions of the stature of Microsoft are safe anymore. The break-in of hackers into Microsoft in February, 2000 was just once example of the threat that organizations faced. But the most worrying aspect was that if a company such as Microsoft, which probably has the densest concentration of intellectual firepower, which could fall prey to hackers.

Communication systems in the Third World have been built around borrowed or imported software and hardware. These may possess several loopholes that an adversary could exploit. Pakistan has indeed found itself at the receiving end of cyber vandalism in the past, and with growing computerization and automation in Pakistani

Armed Forces and other strategic organizations, the magnitude of our vulnerability is bound to increase, This, coupled with the fact that only about 5% of cyber ingresses are detected by organizations, justifies a strong case for an effective and comprehensive ‘IW 'programme of our own without further delay.

Understanding 'IW' correctly requires a mind-set change. Cyber warfare has to be understood at the grassroots as well as the highest levels. A coterie of young, energetic and intelligent officers with an aptitude for computers, networking, encryption and internet applications has to be cultivated as an ‘IW' asset in our Armed Forces, Government departments and civilian institutions of strategic significance. That would serve as a crucial clement towards ensuring the sanctity and safety of our decision-making processes.

Amidst the concern on cyber warfare however, an important point to consider for the decision makers would be to determine the extent to which the enemy, particularly a nuclear capable adversary, is to be taken out or blinded, so that an unintended of the ante is prevented.

REFERENCES

Brig Saleem, Muhammad Ashraf,“Infomation Warfare”, Pakistan Defence Review,26. Summer 1999.Thomas, Timothy L. “Deterring Information Warfare: A New Strategic Challenge”.

Parameters, Winter 1996-97, pp 81-91. Cdr Clemmons, Byard Q and Maj Brown. Gary D, “Cyberwar fare: Ways, Warriors”.

Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence-Building as available at http://www.unidir.org/ programmes/emerg-ing-secu-threats/threats/

Strategic Analysis, Oct-Dec 2003. Joshi, Akshay,“The Scourge of Cyber Terorism', Stmtegic Analysis, July 2000

Title Jr, John H and Gerhardt, William P. “Information-Age Warfare: Solving Threat SOF.

UN General Assembly, A/RES/66/24, 13 December 2011 as available at http://www.un.org/ga/search/viewdoc.asp?symbol=A/RES/66 /24

U.S. Talks to Russia on Internet Security by J. Markoff and A. Kramer, N.Y. Times December 12, 2009, as available at http://www.nytimes.com/2009/ 12/13/sci-ence/13cy-ber.html

Weapons of Mass Destruction'. Military Review, Sep-Oct 1999, pp 35-45.

CHALLENGES AND THE ROLE OF THE MALAYSIAN ARMY AS PART OF A JOINT FORCE IN COUNTERING CYBER WARFARE THREATS IN A MULTI-DOMAIN OPERATIONAL ENVIRONMENT

By MEJ MOHD QAZZEEM BIN IBRAHIM
ROYAL MALAY REGIMENT

INTRODUCTION

"The Army must be agile to change and avoid being exposed to exploitation in cyberspace that can cripple infrastructure and infostructure capabilities," – **Jen Tan Sri Dato' Seri Zamrose bin Mohd Zain, Chief of Army (2021)**.

As stated by Ibrahim et al., (2019), cyber warfare can be defined as cyber-attacks provide the terrorists a chance of bigger safekeeping and flexibility in operational. Ideally, it used a computer to attack from anywhere in the worldwide, avoid revealing the assailant to physical injury. In other words, this cyber warfare can have hacked the system of the computer without the owner of the computer knows that their computers been hacked by those cyber-attackers. They can attack the computer from one location to another location just by one click of the mouse. Software is a key component in nearly every critical system used by every people in the world especially government agency. Attacking the software in a system of cyber warfare is a revolutionary method of pursuing war.

Karl von Clausewitz in Shuurman (2010) defined war as "...an act of violence intended to compel our opponent to fulfil our will... In order to attain this object fully, the enemy must be disarmed, and disarmament becomes therefore the immediate object of hostilities...." At the end of the second millennium, this definition no longer describes the full spectrum of modern warfare. In the future, we will have the potential to make war without the use of violence and fulfill the second half of von Clausewitz's definition with software alone. Today's software-intensive systems make this possible.

Cyber warfare is the conduct of military operations according to information-related principles (Arquilla and Ronfeldt, 1992). This does not define the full degree of capabilities now possible in cyber warfare. Cyber-attacks can be used to disrupt or destroy critical infrastructure, such as power grids, water systems, and transportation networks. This can have a devastating impact on the economy and public safety.

The Defence White Paper (DWP) states that cyber warfare is "the use of computer networks and information systems to attack or defend against an adversary". It goes on to say that, cyber warfare can be used to disrupt or destroy critical infrastructure, steal sensitive information, or influence public opinion. Cyber warfare has emerged as a significant and increasingly prevalent threat in the modern operational environment. As technology continues to advance, the reliance on digital infrastructure and interconnected systems has grown exponentially, making nations vulnerable to cyber-attacks. It is crucial to understand the challenges associated with countering cyber warfare threats and the role of the Malaysian Army as part of a joint force in this Multi-Domain Operational Environment (MDOE).

This article will examine the challenges encountered by the Malaysian Army in countering cyber warfare threats. These challenges include the constantly evolving nature of cyber threats, the interconnectedness of the operational environment, the asymmetric nature of cyber warfare, legal and policy challenges, and the need for advanced technological capabilities. Furthermore, we will delve into the force readiness of the Malaysian Army, encompassing the development of robust cyber defense mechanisms, training, and education for personnel, collaboration with other branches of the military and relevant agencies, and research and development activities. By analyzing these challenges and the role of the Malaysian Army in countering cyber warfare threats, we can gain valuable insights into the importance of force readiness and the overall national security framework required to combat this ever-evolving threat.

NATURE OF CYBER WARFARE

The Volatile, Uncertain, Complex, and Ambiguous (VUCA) nature of cyber warfare poses a significant challenge to the Malaysian Army. The nature of cyber warfare is constantly changing as volatility. New threats are emerging all the time, and existing threats are evolving. The outcome of a cyber-attack is often uncertain. The cyber domain is complex and interconnected. Cyber-attacks can have a ripple effect, impacting multiple systems and networks. The intent of a cyber-attack is often ambiguous. It is difficult to determine who is behind a cyber-attack, and it is difficult to understand their motives (Stein, 2021).

According to Kim et al. (2021), a cyberattack is an offensive operation that is conducted to compromise or disrupt enemy computer systems and networks. These attacks can take various forms, leveraging different techniques and strategies to achieve their

objectives. Cyber attackers exploit vulnerabilities in software, hardware, or human behavior to gain unauthorized access, steal sensitive information, disrupt services, or cause physical damage.

One common form of cyber-attack is malware attacks. Malware, short for malicious software, refers to software programs that are designed to infiltrate systems and perform unauthorized actions. This can include activities such as stealing sensitive data, modifying, or deleting files, or controlling the compromised system remotely. Malware can be delivered through various means, including email attachments, infected websites, or removable media drives. Another type of cyberattack is Distributed Denial-of-Service (DDoS) attacks. In DDoS attacks, the attacker overwhelms a targeted system or network with a flood of traffic or requests, rendering it unavailable to users. By overloading the system's resources, the attacker disrupts the normal functioning of the target, causing inconvenience, financial losses, or reputational damage.

Phishing attacks are another common form of cyberattack. Phishing involves tricking individuals into divulging sensitive information, such as passwords or credit card details, by posing as a trustworthy entity. Attackers often send deceptive emails or create fake websites that resemble legitimate ones, luring unsuspecting users into disclosing their confidential information. Ransomware attacks have also become prevalent in recent years. Ransomware is a type of malware that encrypts the victim's files, making them inaccessible. The attacker then demands a ransom in exchange for decrypting the files. These attacks can have severe consequences for individuals, businesses, and even critical infrastructure, as they can cause data loss, financial harm, and disruption of essential services.

Cyber espionage is the covert use of cyber tools and techniques to gain unauthorized access to classified or sensitive information from target entities (Bederna & Szadeczky, 2020). It is typically conducted by state-sponsored actors or intelligence agencies to gather intelligence on adversaries' capabilities, plans, or vulnerabilities. Unlike traditional espionage, which involves physical infiltration or human intelligence gathering, cyber espionage leverages technology to infiltrate networks, systems, and databases. This allows the perpetrators to access and extract valuable information remotely, without direct physical contact.

Sophisticated techniques, such as Advanced Persistent Threats (APTs), are commonly employed in cyber espionage operations. APTs are stealthy and prolonged cyber-attacks that specifically target high-

value entities, such as government agencies, defense contractors, or critical infrastructure providers. These attacks often involve a combination of social engineering, zero-day exploits, and malware to gain initial access and establish a persistent presence within the target's network.

Information warfare in cyberspace refers to the deliberate manipulation or influencing of information to achieve strategic objectives (Ventre, 2016). It encompasses a range of activities aimed at shaping public opinion, undermining adversaries, or gaining an information advantage. These activities often take place in the digital realm and leverage cyberspace as a battleground. One aspect of information warfare is the spread of disinformation or misinformation. This involves the deliberate dissemination of false or misleading information to deceive or confuse the target audience. Disinformation campaigns can be carried out through social media platforms, websites, or other online channels, to shape public opinion, create division, or undermine trust in institutions.

Propaganda is another key component of information warfare. It involves the systematic dissemination of biased or misleading information to promote a particular viewpoint or ideology (Starbird et al., 2019). Propaganda can be used to influence public opinion, rally support for a cause, or delegitimize adversaries. In cyberspace, propaganda can be disseminated through various online platforms, including social media, news websites, or blogs. Psychological Operations (PSYOPs) are also part of information warfare (Bakshi, 2018). PSYOPs involve the use of psychological techniques and tactics to influence the emotions, beliefs, and behaviour of target audiences. In the context of cyberspace, PSYOPs may include the manipulation of online discussions, the creation of fake personas or accounts to spread specific narratives, or the use of targeted messaging to exploit psychological vulnerabilities.

Cyber defence activities encompass a range of measures taken to protect computer systems, networks, and infrastructure from cyber threats (Von Solms & Van Niekerk, 2013). In today's interconnected digital landscape, where cyberattacks are becoming increasingly sophisticated and prevalent, a strong cyber defence strategy is crucial to safeguard sensitive information, maintain operational continuity, and protect the integrity of critical infrastructure. One of the key components of cyber defence is the development and implementation of robust cybersecurity measures. This includes deploying technologies like firewalls, intrusion detection systems, and secure communication protocols to establish strong barriers and protect against unauthorized

access. Encryption techniques are employed to secure sensitive data both in transit and at rest, ensuring that even if intercepted, the information remains unreadable to unauthorized individuals.

Incident response is another critical aspect of cyber defence. Organizations must have well-defined and tested incident response plans in place to swiftly detect, contain, and mitigate cyber threats (Auffret et al., 2019). This involves establishing procedures and protocols for identifying and analysing security incidents, as well as coordinating the appropriate response actions. Incident response teams work to minimize the impact of cyberattacks, restore systems and services, and collect evidence for forensic analysis and future prevention. Threat intelligence plays a vital role in cyber defence. It involves gathering, analysing, and sharing information about potential and emerging cyber threats. By monitoring and staying informed about the latest tactics, techniques, and procedures used by threat actors, organizations can proactively strengthen their defences and identify vulnerabilities in their systems. This intelligence enables the development of proactive strategies and the implementation of preventive measures to mitigate potential risks.

Continuous monitoring is an integral part of effective cyber defence (Senol & Karacuha, 2020). It involves the real-time monitoring of networks, systems, and applications to detect and respond to potential security incidents promptly. This includes the use of Security Information and Event Management (SIEM) tools, intrusion detection systems, and log analysis to identify unusual or suspicious activities. By constantly monitoring and analysing network traffic and system logs, organizations can identify potential threats and take timely action to prevent or minimize damage. In addition to technical measures, cyber defence also relies on the human element. This involves training and educating personnel about cybersecurity best practices, promoting awareness about common threats like phishing and social engineering, and instilling a culture of security within organizations. By fostering a cyber-aware workforce, organizations can reduce the risk of human error and improve overall cyber resilience.

CHALLENGES IN CYBER WARFARE

The constantly evolving nature of cyber threats presents significant challenges in countering cyber warfare (Sobb et al., 2020). Rapid advancements in technology and attack methodologies require continuous monitoring and adaptation to stay ahead of the threat landscape. Technology is evolving at an unprecedented pace, providing new opportunities for cyber attackers. Advancements such

as artificial intelligence, machine learning, and quantum computing can be harnessed by both malicious actors and nation-states to develop sophisticated cyber-attack tools and techniques. These innovations enable attackers to exploit vulnerabilities more effectively and launch attacks with greater precision and speed.

Attack methodologies are continually evolving to bypass existing defence measures. Cyber attackers frequently develop new tactics, techniques, and procedures to exploit vulnerabilities in systems and networks. They adapt their approaches to evade detection, enhance their ability to infiltrate target systems, and maximize the impact of their attacks. This agility makes it challenging for defensive measures to keep up and effectively mitigate emerging threats.

INTERCONNECTED OPERATIONAL ENVIRONMENT

The interconnected operational environment refers to the extensive interdependence and reliance on critical infrastructure and interconnected systems within various domains, including military, governmental, commercial, and societal sectors (Rinaldi et al., 2001). This interconnectivity offers numerous benefits, such as improved efficiency, communication, and coordination. However, it also introduces vulnerabilities that can be exploited by malicious actors, including in the context of cyber warfare. The dependence on critical infrastructure and interconnected systems makes them attractive targets for cyber-attacks. Disrupting or compromising these systems can have far-reaching consequences, impacting not only military operations but also essential services such as transportation, energy, communication, and finance.

In the military context, the interconnected operational environment requires comprehensive defence strategies that account for cyber threats. This involves integrating cyber capabilities into overall defence planning, establishing dedicated cyber defence units, and fostering collaboration and information sharing among different branches of the military and relevant agencies. Joint exercises and training programs that simulate cyber-attacks can help improve preparedness and enhance coordination in responding to cyber threats.

ASYMMETRIC NATURE OF CYBER WARFARE

The asymmetric nature of cyber warfare refers to the fact that cyber-attacks can be carried out by non-state actors, such as hacker groups or individuals, as well as state-sponsored entities (Sigholm,

2013). This creates challenges in terms of attribution and response, as it can be difficult to identify the perpetrators and determine the appropriate countermeasures. Non-state actors, including hacker groups, hacktivists, and cybercriminals, have increasingly become involved in cyber-attacks. They may have varying motivations, ranging from financial gain to political activism or personal gratification. These actors often operate with a certain degree of anonymity, making it challenging to attribute attacks to specific individuals or groups. The use of various techniques, such as proxy servers, encryption, and obfuscation, further complicates the task of attribution. State-sponsored cyber-attacks are another aspect of the asymmetric nature of cyber warfare. Nation-states may employ cyber capabilities to achieve their strategic objectives, such as intelligence gathering, disrupting critical infrastructure, or conducting espionage. These attacks are often carried out by highly sophisticated and well-resourced actors, making attribution even more complex. State-sponsored attacks can be conducted with plausible deniability, employing tactics to mislead investigators and deflect responsibility.

The challenges in attribution and response to cyber-attacks by non-state actors and state-sponsored entities pose significant dilemmas for affected nations. It becomes crucial to gather sufficient evidence and conduct thorough investigations to attribute attacks accurately. Attribution is vital to determine the appropriate countermeasures, including diplomatic, economic, or legal actions, as well as possible offensive cyber operations in response.

LEGAL AND POLICY CHALLENGES IN CYBERSPACE

Cyberspace presents unique legal and policy challenges in countering cyber warfare (Stahl, 2011). The rapid evolution of technology often outpaces the development of comprehensive legal frameworks and policies to address cyber threats adequately. This creates a gap in international and domestic laws, making it difficult to enforce cyber norms, prosecute cybercriminals, and coordinate responses to cyber-attacks. Addressing these jurisdictional challenges requires international cooperation and coordination among law enforcement agencies. Mutual legal assistance treaties and agreements can facilitate information sharing, evidence collection, and extradition of cyber criminals. Additionally, capacity building efforts aimed at enhancing the capabilities of law enforcement agencies and fostering international collaboration can help overcome these challenges.

TECHNOLOGICAL CHALLENGES AND THE NEED FOR ADVANCED CAPABILITIES

Countering cyber warfare requires defence forces to possess advanced technological capabilities. This includes advanced detection and monitoring systems, robust encryption algorithms, secure communication protocols, and the ability to rapidly respond to emerging threats (Colbaugh & Glass, 2012). However, acquiring and maintaining these advanced capabilities can be a significant challenge due to the constant evolution of technology, high costs, and the need for specialized expertise. Furthermore, capacity building programs, training, and education initiatives should be prioritized to ensure that cybersecurity personnel possess the necessary skills to operate and manage advanced technologies effectively. Continuous professional development and knowledge sharing within the cybersecurity community are vital to keep pace with the rapidly evolving cyber threat landscape.

CASE STUDY – RUSSIA-UKRAINE WAR

According to Bateman et al., (2022), the Russian invasion of Ukraine has revealed several important lessons about the future of cyber warfare. First, cyber warfare is now a central component of modern warfare. Russia used cyber warfare to support its invasion of Ukraine in several ways, including launching cyberattacks against the Ukrainian government and military networks, spreading disinformation and propaganda, and disrupting critical infrastructure. Second, cyber warfare is becoming increasingly sophisticated. Russia used a variety of sophisticated cyberattacks against Ukraine, including using wiper malware to destroy data on Ukrainian computers, DDoS attacks to disrupt Ukrainian websites and services, and using social media to spread disinformation and propaganda. Third, cyber warfare is becoming increasingly globalized. Russia's cyber-attacks against Ukraine have had a significant impact on countries around the world, including the United States. This is because the internet is a global network and cyber-attacks can easily spread from one country to another. Fourth, cyber warfare is becoming increasingly difficult to defend against. Russia's cyber-attacks against Ukraine were very effective, and the Ukrainian government and military were largely unable to defend themselves. This is because cyber warfare is a very complex and rapidly evolving field, and it is difficult for governments and businesses to keep up with the latest threats. Fifth, cyber warfare is becoming increasingly likely to lead to armed conflict. The Russian invasion of Ukraine is a clear example of how cyber warfare can escalate into armed conflict. This is because cyber-attacks can be used

to disrupt critical infrastructure, such as power grids and communications networks, which can have a significant impact on a country's economy and security.

The lessons learned from the Russian invasion of Ukraine have important implications for the future of cyber warfare. The Russian invasion demonstrated that cyber warfare can be employed as a means to weaken an adversary's military capabilities or economy. It can be used to gain an advantage in a conflict by disrupting or disabling key systems. The invasion highlighted how cyber-attacks can complement conventional military operations. Cyber tactics can be integrated with conventional warfare to gain an edge in conflicts. The Ukrainian invasion revealed that cyber-attacks can be utilized to manipulate public opinion and influence political decisions. Disinformation campaigns and propaganda disseminated through cyber means can shape perceptions and create divisions. The Ukrainian case demonstrated that cyber-attacks lead to significant economic consequences. By targeting critical infrastructure, financial systems, or businesses, adversaries can cause disruption and financial losses. The invasion by Russian revealed the vulnerability of critical infrastructure to cyber-attacks. Adversaries can target power grids, transportation systems, communication networks, and other essential services, causing widespread disruption and chaos.

MALAYSIAN ARMY'S FORCE READINESS IN CYBER WARFARE

Force readiness is of utmost importance in countering cyber threats effectively. A well-prepared and proactive approach enables defence forces to anticipate, detect, and respond to cyber-attacks promptly and efficiently. Force readiness ensures that the necessary resources, capabilities, and strategies are in place to protect critical systems, networks, and infrastructure from cyber threats. It also enhances the ability to mitigate the potential damage caused by successful cyber-attacks and facilitates a swift recovery process.

Collaboration and information sharing among different branches of the military and relevant agencies are essential for the Malaysian Army's readiness in countering cyber threats. The Malaysian Army works closely with other branches of the MAF, such as the Royal Malaysian Navy, Royal Malaysian Air Force, Defence Cyber and Electromagnetic Division (BSEP), and Cyber Defence Operations Centre (CDOC), to develop integrated cyber defence capabilities. Sharing information on emerging threats, tactics, and vulnerabilities can enhance the overall cyber readiness of the joint force.

Furthermore, collaboration with relevant government agencies, such as the National Cyber Security Agency (NACSA), intelligence agencies, and law enforcement, is crucial for effective coordination and response to cyber threats. Joint exercises, table top simulations, and information-sharing platforms should be established to facilitate seamless collaboration and ensure a coordinated and swift response to cyber-attacks. Additionally, international cooperation and collaboration with partner nations, industry experts, and academia can provide valuable insights and best practices for enhancing force readiness in cyber warfare. Sharing lessons learned, conducting joint research and development activities, and participating in international cyber defence exercises can contribute to the overall readiness and effectiveness of the Malaysian Army in countering cyber threats.

MALAYSIAN ARMY'S RESPONSIBILITIES IN COUNTERING CYBER THREATS

The Malaysian Army plays a crucial role as part of a joint force in countering cyber threats (Ibrahim et al., 2019). While traditionally focused on land-based operations, the Malaysian Army has recognized the need to adapt to the changing nature of warfare and the increasing significance of cyber warfare. As part of their responsibilities, the Malaysian Army is tasked with establishing and maintaining robust cyber defence mechanisms, participating in joint exercises, and training programs, engaging in research and development activities, and collaborating with other branches of the military and relevant agencies.

In March 2021, the Malaysian Armed Forces (MAF) set up a Cyber Warfare Signals Regiment (99 RSPS) to strengthen its cyber defence capabilities (Malay Mail, 2021). The regiment was established in response to the growing threat of cyber warfare and the increasing sophistication of cyber-attacks. The regiment is equipped with the latest cyber warfare assets and systems, and its personnel are trained in cyber warfare operations. The establishment of the 99 RSPS is a significant step in the MAF's efforts to strengthen its cyber defence and protect Malaysia's national interests in cyberspace. The Malaysian Army's focus on cyber warfare is a sign of the growing importance of this domain in modern warfare. Cyber-attacks can disrupt critical infrastructure, steal sensitive information, and even cause physical damage. By strengthening its cyber warfare capabilities, the Malaysian Army is better positioned to defend Malaysia against these threats.

CONCLUSION

In conclusion, countering cyber warfare threats poses significant challenges in the Multi-Domain Operational Environment. The constantly evolving nature of cyber threats, the interconnectedness of the operational environment, the asymmetric nature of cyber warfare, legal and policy challenges, and technological complexities all contribute to the complexity of the task. However, force readiness plays a crucial role in mitigating these challenges and effectively countering cyber threats. The Malaysian Army has recognized the significance of cyber threats and has taken proactive measures to enhance force readiness. They have responded to specific incidents, learned valuable lessons, and implemented measures to strengthen their cybersecurity posture. Collaboration, training, research and development, and integration with other branches and agencies have been key in their approach. The ongoing commitment to enhancing force readiness and capabilities is vital in the face of the ever-evolving nature of cyber threats.

REFERENCES

Alford Jr, L. D. (2000). Cyber warfare: Protecting military systems. *Acquisition Review Quarterly*, *7*(2), 101-107.

Arquilla, J., & Ronfeldt, D. (1992). Emergent modes of conflict. *Cyberwar is coming*, 1995- 1996.

Auffret, J. P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., & Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks*, *17*(01), 17-40.

Bakshi, B. (2018). Information warfare: Concepts and components. *IJRAR- International Journal of Research and Analytical Reviews*, *5*(4), 178-185.

Bateman, J., Beecroft, N., & Wilde, G. (2022, December 19). What the Russian invasion reveals about the future of cyber warfare. Carnegie Endowment for International Peace.https:// carnegieendowment.org/2022/12/19/what-russian-invasion reveals-about-future-of-cyber-warfare-pub-88667

Bederna, Z., & Szadeczky, T. (2020). Cyber espionage through Botnets. *Security Journal*, *33*(1), 43-62.

Colbaugh, R., & Glass, K. (2012, October 14). Predictability-oriented defense against adaptive adversaries. In *2012 IEEE international conference on Systems, Man, and Cybernetics (SMC)* (pp. 2721-2727). IEEE.

El-Muhammady, A. (2021). Malaysia: Balancing national development, national security, and cybersecurity policy. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 325-336). Routledge.

Hassan, A. G. A. (2019). Malaysia's Defence Policy: A Future Not Dictated By The Past. *The Journal of Defence and Security*, *11*(2), 9-20.

Ibrahim, A., Mahmud, N., Isnin, N., Dillah, D. H., & Dillah, D. N. F. (2019). Cyber Warfare Impact on National Security-Malaysia Experiences. *KnE Social Sciences*, 206-224.

Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cyber-attack scoring model based on the offensive cybersecurity framework. *Applied Sciences*, *11*(16), 1-21.

Liaw, J. O. H., Ahmad, F., Ibrahim, N., Ismail, A., & Zainol, N. A. M. (2021). The Readiness of Malaysian Government in Total Defense (HANRUH) on the Social Media Usage. *Journal of Southwest Jiaotong University*, *56*(2).

MalayMail. (2021, March 2). Malaysian Army to set up cyber warfare regiment to strengthen the cyber defense says army chief. Malay Mail. https://www.malaymail.com/news/malaysia/2021/03/02/malaysian-armed-forces-to-set-up-cyber-warfare-regiment-to-strengthen-cyber/1954285

Persadha, P. D., Waskita, A. A., & Yazid, S. (2015, October). Comparative study of cyber security policies among Malaysia, Australia, Indonesia: A responsibility perspective. In *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)* (pp. 146-150). IEEE.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, *21*(6), 11-25.

Schuurman, B. (2010). Clausewitz and the “new wars” scholars. *The US Army War College Quarterly: Parameters*, *40*(1), 89-100.

Senol, M., & Karacuha, E. (2020). Creating and implementing an effective and deterrent national cyber security strategy. *Journal of Engineering*, 2020(1), 1-19.

Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1-37.

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), 1-31.

Stahl, W. M. (2011). The uncharted waters of cyberspace: applying the principles of international maritime law to the problem of cybersecurity. *Ga. J. Int'l & Comp. L.*, *40*, 247.

Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1-26.

Stein, S. (2021). Reimagining global citizenship education for a volatile, uncertain, complex, and ambiguous (VUCA) world. *Globalisation, Societies and Education*, *19*(4), 482-495.

Stevenson, W. R. (2013). Cyber planning And Cyber Defense: A Malaysian Perspective. *The Journal of Defence and Security*, *3*(2), 117-127.

Tan, O. S. L., Vergara, R. G., Phan, R. C., Khan, S., & Khan, N. (2020). Cybersecurity laws in Malaysia. In *Encyclopaedia of Criminal Activities and the Deep Web* (pp. 435-448). IGI Global.

Ventre, D. (2016). *Information warfare*. John Wiley & Sons.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102.

CYBER WARFARE – CHALLENGES AND FORCE READINESS

By MEJ ABDUL KADIR BIN USAMAH
ARMED FORCES RELIGIOUS CORPS

INTRODUCTION

The emergence of cyber warfare in contemporary conflicts has significantly reshaped the landscape of modern warfare, posing new challenges to national security. With the increasing interconnectedness and reliance on advanced technology, protecting against cyber threats has become a top priority. Cyber warfare involves using digital tools and techniques to gain unauthorised access and disrupt or damage information systems and networks through hacking, data breaches, espionage and sabotage. This type of warfare can affect governments, military organisations, critical infrastructure and individuals alike. It requires understanding within multi-domain operational environments to fully comprehend its impact across various domains, including land, sea, air, space and cyberspace (Shakarian et al., 2013). The Army plays a crucial role in countering these evolving threats within this framework as part of the joint force effort. However tackling these seemingly complex issues requires strategic adaptations involving cross-domain collaboration to defend against potential attacks by having effective intelligence gathering capabilities coupled with seamless offense-defence strategies improving force readiness.

This article focuses on analysing the challenges confronting Army personnel in their attempts to counteract such constant looming attacks stemming from increased cyber intrusions into interlinked information systems used for logistics functions like procurement, defence communications, public and command control. It seeks to examine traditional military operations alongside a technological system that directly affects Active Duty service members because, given its impact on modern battlespaces, which means lack of prepare-dness might have far-reaching effects on troops participating in such scenarios (Brose, 2012). Through careful consideration, necessary measures will be suggested aimed at fortifying military preparedness for both present and future adversaries while fostering joint efforts amongst all services.

UNDERSTANDING CYBER WARFARE

Cyber warfare is a rapidly evolving form that utilises digital technologies and networks to target adversaries' computer systems,

networks and infrastructure. It is characterised by its covert nature, where attacks are conducted virtually to gain unauthorised access, cause disruption, steal sensitive information or compromise targeted systems' integrity (Butler, 2013). The nature of cyber warfare is multi-faceted, with diverse objectives and tactics employed by various actors. The primary objective of cyber warfare is to gain a strategic advantage by exploiting vulnerabilities in the digital infrastructure of adversaries. This advantage can be achieved through different tactics, including reconnaissance, infiltration, exploitation and manipulation. Reconnaissance involves gathering information about the target's networks, systems and vulnerabilities. It enables the attacker to identify potential entry points and weaknesses that can be exploited (Hills, 1997).

Infiltration is gaining unauthorised access to the target's systems, often through phishing, malware, or social engineering. Once inside, the attacker can execute various tactics, such as data theft, system disruption, or malicious code implantation. The objectives of cyber warfare can range from disrupting critical infrastructure, sabotaging military operations, stealing sensitive information, influencing public opinion or even conducting psychological operations (Lal & Chavan, 2019). It offers attackers the advantage of anonymity, as they can hide behind layers of encryption and proxies, making it difficult to attribute the attacks to a specific actor.

Furthermore, cyber warfare tactics can be executed through different means, including Distributed Denial of Service (DDoS) attacks, malware deployment, zero-day exploits and social engineering techniques. DDoS attacks overload targeted networks or websites with a flood of traffic, rendering them inaccessible. Malware deployment involves using malicious software to infiltrate systems, steal information or cause damage (Tira, 2018). Zero-day exploits take advantage of unknown vulnerabilities in software or systems, giving attackers a significant advantage. Social engineering tactics exploit human vulnerabilities, such as manipulating individuals into divulging sensitive information or clicking on malicious links.

The scope of cyber warfare extends beyond traditional military conflicts. It has become a tool utilised by nation-states, non-state actors and individuals with varying motivations. State-sponsored cyber warfare campaigns have gained prominence, with governments investing significant resources in developing cyber capabilities to protect their interests, gather intelligence or engage in offensive operations (Grange, 2014). Non-state actors, such as hacktivist groups or criminal organisations, also engage in cyber warfare for political,

financial or ideological reasons. Cyber warfare encompasses various objectives and tactics that exploit vulnerabilities in digital systems. Its scope extends beyond traditional warfare, affecting national security, critical infrastructure and global stability. Understanding the nature of cyber warfare and its diverse objectives and tactics is crucial in formulating effective strategies to defend against and respond to cyber threats.

Cyber warfare poses a severe threat to national security and critical infrastructure. With the ability to disrupt essential services, steal sensitive information and compromise government institutions, it demands attention from military and defence organisations. National security concerns primarily surround the potential for cyber-attacks to interfere with government agencies, military networks and defence systems (National Cyber Security Agency, 2020). These breaches could lead to compromised classified data and create communication disruptions that hinder trustworthiness when addressing physical threats. Worryingly, many aspects of fundamental infrastructure rely on interconnected computer networks susceptible to cyber-attack (Diamond, 2014). For example, a calculated move against power grids can cause prolonged blackouts that negatively impact the economy or diminish public safety capabilities. Financial institutions are not immune in such cases either since an unmitigated risk scenario that targets them leads to economic disruption - something which seriously erodes both financial data accuracy as well as public trust in banks' credibility.

Furthermore, nation-states using cyber espionage pose greater risks by stealing trade secrets or intellectual property that provide significant advantages baring long-lasting consequences if firms do not stay protected with robust cybersecurity frameworks in place through solid encryption protocols or incident response plans (Robinson et al., 2015). Mitigating cascading effects of these situations is critical across all sectors since one organisation's breach might have impacts on multiple closely connected systems - making containment much more challenging when dealing with a transportation system shutdown, causing havoc among supply chains lowering functionality among various other vital sectors nationwide. Governments must invest heavily in proactive cybersecurity measures to ensure comprehensive defence strategies while fostering public-private partnerships coupled with international cooperation as new emerging threats keep coming up regularly, so vulnerability assessments needs equal attention for maintaining digital preparedness ongoingly.

Cyber warfare is a complex arena encompassing numerous threats and actors, each with its objectives, tactics and capabilities. Recognising these various cyber threats and understanding the actors involved is essential in developing effective defence strategies to counter cyber warfare successfully. One of the most common forms of cyber threats is malware, which includes viruses, worms and Trojans designed to infiltrate computer systems to steal sensitive information or disrupt operations (Tan et al., 2021). Malware spreads through email attachments, infected websites or compromised software primarily. Another significant threat is DDoS attacks that overwhelm targeted systems with excessive traffic rendering them inaccessible to legitimate users causing disruptions leading to financial losses and damaged reputation-wise. They pose a severe national security concern by necessitating advanced techniques and resources in defence mechanisms against such sophisticated breaches. Cybercriminal organisation that operate for financial gain by engaging in identity thefts, ransomware attacks, data breaches and selling stolen information make it equally crucially crucial for companies conducting online business always to have impenetrable security measures set adequately.

Various non-state actors, like hacktivist groups, engage in ideological and political causes while terrorists utilise fear-inducing means-online terror tactics for disruption and damage public services being their prime targets (Gazula, 2017). Comprehending of wide assortment of cyber threats and their sources is critical to creating practical defence systems and response tactics. Achieving this obligation mandates continual monitoring, threat intelligence sharing and cooperation between governing bodies, intelligence agencies, law enforcement groups and private corporations. Mitigating the risks posed by these perils and ensure national security, along with safeguarding crucial infrastructure, requires robust cybersecurity measures, user education programs and technological upgrades.

Cyber-attacks have become more frequent and sophisticated in recent years. Many high-profile examples show that these incidents can have damaging consequences across various sectors. In 2013, the Carbanak Group stole over $1 billion from financial institutions through highly advanced hacking methods revealing the vulnerability of banks to cybercrime threats (White, 2018). The WannaCry ransomware attack in 2017 affected hundreds of thousands of computers worldwide, highlighting potential risks to public safety and infrastructure (Dar, 2019).

Moreover, Russian hackers attacked the DNC during the 2016 US presidential election leading to political turmoil and raising concerns about cyber manipulation of democratic processes (Lal & Chavan, 2019). The SolarWinds supply chain attack discovered in 2020 compromised numerous government agencies and private organisations worldwide, showcasing software supply chain vulnerabilities (Tan et al., 2021). These cases emphasise that cyber-attacks can result in immense damage, including physical harm, financial losses, service disruption, reduction of public trust, among others. Policymakers must implement proactive cybersecurity measures such as system updates or enhanced employee training programs to mitigate these risks effectively. International collaboration between governments, intelligence agencies and cybersecurity entities has become crucial for exchanging information and best practices toward collective defence against cyber warfare threats, given cyberspace's interconnectivity.

THE MULTI-DOMAIN OPERATIONAL ENVIRONMENT

The concept of a Multi-Domain Operational Environment acknowledges that modern warfare has expanded beyond traditional land, sea and air domains to include cyberspace. It highlights the interconnectivity and interdependence of these domains and underscores the importance of integrated operations to achieve military objectives. Military operations are conducted simultaneously or coordinated across multiple domains with this approach (Harris III, 2018). By leveraging the unique capabilities of each domain, commanders gain a competitive advantage over adversaries. Modern conflicts are intricate and dynamic, requiring a comprehensive understanding of battlespace for effective operation across multiple domains.

Military forces utilise ground troops for land operations, while naval forces such as surface ships, submarines and maritime aircraft conduct sea operations. Air forces provide air superiority support through close air assistance and strategic bombing while space-based satellites enhance communication and navigation surveillance via reconnaissance activities. This integration aims at creating synergies between domains by exploiting their distinguishing traits for achieving military objectives efficiently. However, incorporating cyber operations into these multi-domain environments presents unique challenges due to its virtual nature with remote operating capabilities, anonymity features and additional layers of complexities not present in other physical domains (Gady & Stronell, 2020). This obstacle necessitates continuous innovation in adapting new techniques promptly amidst

emerging threat vectors ensuring maximal interoperability without comprising traditional military objectives giving them an extra economic edge over adversaries.

Integrating cyber operations into traditional military operations is challenging due to the interconnectedness of different domains in the Multi-Domain Operational Environment. This interconnectivity creates both opportunities and challenges for military planning and execution. Integrators of cyber need to have a comprehensive understanding of these domains, their interdependencies and how cyber activities can impact traditional military capabilities. One challenge faced when integrating cyber operations with other domains is the complex nature of interconnections between them; actions in one domain have immediate effects on others, disrupting critical infrastructure that would obstruct ground forces' ability to coordinate with air support or access satellite intelligence networks (Rantapelkonen & Salminen, 2013). Moreover, interoperability and coordination between cyber forces require specialised knowledge and expertise in network security systems, computer architectures and information warfare – which may be hard to integrate into existing structures. The agility required from cybersecurity experts makes it necessary also to work with civilian organisations such as industry partners or government agencies intensively.

Additionally, legal and ethical considerations must be properly addressed as the use of cyber abilities during periods of conflict raises questions concerning protecting civilians' infrastructure while avoiding collateral damage called ransomware payments or any money laundering involved by hackers who might attack financial sectors during this period (Robinson et al., 2015). Overcoming these challenges requires effective communication channels and shared situational awareness across several fields, such as land, space and sea, including cyberspace. Developing suitable guidelines about governance structures while enhancing investment strategies such as research development areas emphasising policy development, training education technology advancements enhanced information sharing robust collaboration between various public-private institutions will prove essential for overall effectiveness but maintaining a competitive edge at modern conflicts gives an added advantage over adversaries who find little time adapting changes quickly

Cyber warfare has significant implications for overall force readiness in today's Multi-Domain Operational Environment. Integrating cyber capabilities into traditional military operations brings new dimensions of warfare that require careful consideration of their

effects on the effectiveness and preparedness of our military forces. With increasing connectivity between critical infrastructure and military systems, they become potential targets for cyber-attacks, making them more vulnerable to risks across all domains. Successful cyber-attacks can disrupt vital military capabilities, compromising situational awareness, communication networks and command and control systems (Diamond, 2014). This significantly hampers a force's ability to respond effectively to threats. It is crucial that we ensure the resilience and security of our military networks and systems so that we maintain force readiness.

Cyber warfare also highlights the importance of intelligence gathering and information superiority. Information is vital in decision-making and situational awareness in today's operational environment. Cyber operations provide an avenue for reconnaissance activities like surveillance or obtaining adversary data; however, adversaries may also use this means to collect sensitive information or manipulate data leading to compromised decision-making frameworks. Maintaining adequate cybersecurity capability ensures authentic information flow becomes necessary as it helps adopt agile methods in addressing new challenges quickly with sophisticated workarounds.

The fast-changing environments of cyberspace require flexibility from our armed forces' current operation mindset by embracing a dynamic defence plan comprising continuous monitoring threat hunting exercises vulnerability assessments, among others, through red teaming approach (Shakarian et al., 2013). Cyber-attacks blur the line between civilian-infrastructure businesses owned by civilians and those belonging to the military; thus, close collaboration between stakeholders, including government agencies and private sector entities, becomes crucial when ensuring the protection and resilience of critical infrastructures. Private-public partnerships have proven advantageous in building enhanced collective defence postures, thus proving instrumental in disseminating threat landscapes shared among various partners both domestic overseas, through information-sharing initiatives.

The 2015 cyber-attack on Ukraine's power grid is a grave example of the implications of cyber warfare in modern-day multi-domain operations (Dar, 2019). The hackers easily infiltrated the control systems of multiple electricity distribution companies, resulting in excessive power outages and disrupting normal life across the country. This highlighted the significance and potential impact of targeting critical infrastructure through cyberspace and underlined the interconnectedness between physical domains and the cyber domain.

It also emphasised the need for military forces to develop strategies that consider cybersecurity threats as a significant factor towards maintaining overall force readiness, including preparing for attacks with adequate defence measures and response plans to ensure operational effectiveness.

CHALLENGES OF CYBER WARFARE

The Army and joint forces face several challenges in countering cyber threats. One of the key obstacles is the ever-changing nature of cyber warfare as attackers adapt their tactics and techniques regularly, leaving defence systems struggling to keep up. In addition, it is difficult to attribute attacks to specific actors due to cyberspace's anonymous and global nature. Cyber threats are complex, taking various forms such as malware, ransomware, DDoS attacks and social engineering each requiring specific countermeasures (Tira, 2018). Interconnected systems add another challenge; protecting them requires collaboration between different entities including military operations and civilian networks - a tall order. There is also a significant shortage of skilled cybersecurity experts globally, with recruitment also challenging. Lastly, technological advancements bring opportunities and risks necessitating proactive measures against potential cyber threats for comprehensive defence strategies that require continuous adaptation to stay ahead of evolving risks.

The Army and the joint force face technical challenges in cyber warfare that must be addressed to counter cyber threats effectively. Three key challenges include attribution, Advanced Persistent Threats (APTs) and emerging attack vectors. Attribution is difficult as attackers can hide their identities in various ways, making it challenging to respond effectively and deter future attacks. Combatting APTs involves using sophisticated tools and technologies for threat detection and implementing proactive defence measures through continuous monitoring and threat hunting. The emergence of new attack vectors with advancements in technology requires continuous research and development to safeguard against evolving threats (Robinson et al., 2015). To address these technical difficulties, investing in advanced technologies for identification and response capabilities, collaborating with industry partners on research and development and sharing intelligence across academia and international boundaries while promoting a cybersecurity mindset among personnel are essential.

Operational challenges in cyber warfare require agile and adaptable defence strategies and cyber capabilities integration into military planning to counteract evolving cyber threats. Traditional static

defence approaches are not enough against modern sophisticated tactics used by attackers. Therefore, a proactive approach that emphasises continuous monitoring, threat intelligence sharing and rapid response are necessary to mitigate and control cyber-attacks effectively. The use of machine learning and artificial intelligence can also enhance real-time threat detection and response (Gady & Stronell, 2020). The integration of cyber operations into strategic planning presents additional operational challenges for joint forces to coordinate seamlessly between military domains like land, sea, air and space while considering critical elements such as intelligence-sharing targeting processes.

Skilled personnel with expertise in various cyber disciplines are essential to building a competent workforce for the Army and joint forces. It is pertinent to embrace training programs actively alongside educational courses as valuable investments for workers' career development. A comprehensive approach is vital to overcoming these operational challenges amidst rapidly evolving cyber threats. Integrated defence mechanisms leveraging advanced technologies accompanied by reliable threat intelligence reinforces our readiness against potential risks arising from a cybersecurity breach within military domains. In cyber warfare, one operational challenge is exemplified by the Stuxnet attack on Iran's nuclear facilities. This intricate malware was specifically designed to target the industrial control systems used in these highly secure and isolated facilities. It caused extensive physical damage to centrifuges by exploiting multiple system vulnerabilities. The Stuxnet attack demonstrated the level of expertise, resources and coordination required to successfully execute a target cyber operation with significant operational impact while remaining covert (Kanwal, 2009).

ROLE OF THE ARMY IN CYBER WARFARE

The role of the Army in a joint force framework is critical to address the challenges of cyber warfare effectively. With cyberspace becoming increasingly contested, the Army plays a vital part in contributing to a nation's overall cyber defence and resilience. While traditionally focused on land-based operations and its role has expanded to include cyber warfare capabilities. The Army is responsible for developing and deploying cyber measures to defend national interests, protect critical infrastructure and support joint force operations. Military branches collaborate with intelligence agencies and government entities while respecting legal parameters and policy guidelines for strategic objectives (Tira, 2018). This collaboration is

essential as threats extend beyond traditional boundaries requiring expertise from multiple domains.

Additionally, proactive engagement through offensive cyber operations further enhances defensive measures disrupting or degrading adversary capabilities within set limits applying minimal collateral damage techniques minimising escalation wherever possible. Furthermore, critical activities performed by armed forces involve intelligence gathering and analysis in cyberspace, which provides situational awareness to both trace and adversaries besides identifying potential risks early enough stressing promptness in response mechanisms. The workforce plays an invaluable role here; highly trained personnel equipped with technical knowledge conduct specialised courses enable them to handle sophisticated systems used during such missions successfully (Brose, 2012). Through these efforts aimed at meeting modern digital battlefield challenges head-on, the Army remains dedicated to enhancing its evolving position within a joint force cybersecurity framework, assuring resiliency amidst ever-increasing threats online that might impact severe consequences otherwise.

The Army plays a critical role in safeguarding a nation's cyber infrastructure. Its tasks and responsibilities encompass defence, offence and intelligence gathering. In terms of defence, the Army implements robust cybersecurity measures to protect sensitive information and infrastructure against cyber threats (Harris III, 2018). It works closely with other branches of the military, government agencies and private sector partners to share threat intelligence and coordinate response efforts. Offensive operations involve leveraging cyber capabilities to weaken an adversary's networks and support military operations in other domains. The Army conducts these activities within legal guidelines while adhering to strategic objectives. Intelligence gathering is another crucial responsibility for understanding adversary capabilities, intentions and tactics through advanced surveillance techniques. For fulfilling such roles successfully, the Army invests significantly in training personnel with the technical expertise required for dynamic fields like cybersecurity while promoting an innovation culture among its workforce constantly.

Collaboration and cooperation across various military branches, government agencies and international partners are fundamental to effectively countering cyber threats in today's complex technological environment. Cyber warfare operates in a densely interconnected space where activities undertaken in one domain can have significant implications across other domains (Hills, 1997). The Army cannot

address such challenges alone and must work together with intelligence agencies, law enforcement bodies and other military branches to gather timely information on emerging trends, share threat assessments and analyse cyber intelligence data accurately so that it can keep ahead of adversaries. Integrated coordination facilities allow the Army to synchronise its strategies with conventional military actions seamlessly while sharing expertise across various domains. Additionally, it lets them develop a unified approach toward cybersecurity operations by establishing common doctrines and standard operation procedures for consistent practices across different environments. Collaborating beyond traditional military realms is crucial for leveraging technological advancements, innovative ideas from research institutions and insights from cybersecurity organisations. The joint force framework enables the Army to counter evolving cyber threats effectively, enhancing overall situational awareness simultaneously. Pooling resources through cross-domain collaborations that create collective situational awareness enhances proactive response rates by acting swiftly against potential crises (Butler, 2013).

The participation of the Army in cyber warfare primarily involves joint cyber exercises. These simulations recreate real-life cyber-attacks and require military branches, government entities and global partners to coordinate their efforts. For instance, the Army may collaborate with the air force, navy and cyber command to work on a joint project focused on safeguarding critical infrastructure from coordinated attacks (Dinniss, 2012). By coordinating with other domains through these drills, the Army can gain valuable experience in identifying weaknesses in its operations and implementing effective defensive strategies. The insights gained from such simulations also aid the military's ongoing development of strategies, tactics and capabilities needed for successful engagements in cyberspace.

ENHANCING FORCE READINESS

It is imperative for the Army to enhance force readiness in cyber warfare so that they can effectively defend against and respond to cyber threats. A multi-faceted approach involving different strategies and initiatives must be implemented. Firstly, comprehensive training programs should be developed to equip military personnel with the necessary knowledge and skills in cyber operations. By providing ongoing training and education, the Army can ensure its personnel is well-equipped to handle evolving cyber threats (Grange, 2014). Conducting realistic and dynamic cybersecurity exercises can significantly enhance force readiness by allowing soldiers to practice

their response capabilities in controlled environments. Investment in cutting-edge technology, such as intrusion detection systems and threat intelligence platforms, is another crucial aspect of enhancing force readiness. Furthermore, establishing strong partnerships with industry and academia allows access to the latest expertise, technologies and best practices that facilitate knowledge sharing innovation for developing tailored solutions against emerging cyber threats. Incorporating a proactive risk-based approach prioritises continuous monitoring, identifying vulnerabilities and potential threats and reducing the impact of potential attacks while fostering a culture of cybersecurity awareness throughout all levels helps mitigate internal risks ensuring strict adherence to best practices.

Military personnel involved in cyber operations must prioritise training, education and skill development to be fully prepared to counter complex cyber-attacks and enhance force readiness. Technical skills such as network security, cryptography and incident response should be integrated into comprehensive training programs. Formal education in relevant fields like cybersecurity or computer science is also a critical investment for building solid foundations of knowledge that enable decision-making (White, 2018). The rapidly evolving nature of technology requires continuous professional development opportunities for military personnel, including advanced training courses, certifications, competitions and interdisciplinary collaborations across various fields, including legal frameworks and intelligence analysis. Creating a culture of continuous learning by encouraging research and development will foster innovation and adaptability, helping the Army to stay ahead of emerging threats. By prioritising these initiatives in personnel development through practical collaborative efforts within the military community, we can ensure that our forces ensure are well-equipped to tackle ever-changing cybersecurity challenges with distinction.

Enhancing force readiness in cyber warfare requires a comprehensive approach that includes technological advancements, investment in cyber capabilities and strong partnerships with industry and academia. The rapidly evolving nature of cyber threats necessitates the adoption of cutting-edge technologies, the developing of robust cyber capabilities and collaboration with external entities to stay ahead of adversaries (Kanwal, 2009). First and foremost, technological advancements play a crucial role in enhancing force readiness. The Army must invest in state-of-the-art cybersecurity technologies, tools and infrastructure to detect, prevent and respond to cyber threats effectively. This includes advanced threat detection systems, network monitoring tools, secure communication channels

and secure hardware and software solutions. By staying at the forefront of technological advancements, the Army can better defend against sophisticated cyber-attacks and minimise vulnerabilities. Simultaneously, investment in cyber capabilities is essential to improve force readiness. This involves allocating resources and personnel to develop and maintain dedicated cyber units within the Army. These units should have specialised skills and expertise in offensive and defensive cyber operations. By investing in cyber capabilities, the Army can proactively identify and neutralise threats, conduct cyber intelligence operations and launch practical offensive actions against adversaries when necessary (Tan et al., 2021). Partnerships with industry and academia also play a pivotal role in enhancing force readiness in cyber warfare. Collaboration with industry allows the Army to leverage the expertise and cutting-edge technologies developed in the private sector. The Army can access advanced threat intelligence, innovative tools and collaborative research and development opportunities.

Similarly, collaborating with academia enables the Army to tap into academic institutions' knowledge and research capabilities. This collaboration can lead to advancements in cyber defence strategies, the development of new technologies and the recruitment of talented individuals. Furthermore, partnerships with external entities provide opportunities for joint training exercises, information sharing and mutual support during cyber incidents (Gady & Stronell, 2020). These collaborations foster a more assertive cyber defence ecosystem, enabling the Army to benefit from a broader range of perspectives, resources and expertise. Enhancing force readiness in cyber warfare requires a multi-faceted approach that includes technological advancements, investment in cyber capabilities and partnerships with industry and academia. By embracing cutting-edge technologies, developing specialised cyber units and leveraging external collaborations, the Army can effectively counter cyber threats and maintain a high level of readiness. These efforts contribute to a more robust cyber defence posture and ensure the Army is prepared to safeguard critical assets and infrastructure in an increasingly interconnected and digitised world.

Enhancing force readiness in cyber warfare has been the US Army's partnership with leading technology companies. These collaborations have resulted in specialised cyber training centres, where the soldiers receive hands-on coaching in simulated attack scenarios. One such instance is the Cyber Training Centre of Excellence, created by partnering with cybersecurity firm FireEye (Gazula, 2017). This centre provides cutting-edge tools and realistic

environments to enhance the soldiers' skills to defend and respond against cyber threats. By leveraging industry expertise and resources, these partnerships ensure that soldiers are well-prepared to handle complex challenges as they arise in real-world situations.

FUTURE TRENDS AND IMPLICATIONS

Several key trends and potential developments will shape the landscape of conflicts in the future of cyber warfare. One significant trend is the increasing sophistication of cyber threats, which are likely to become more advanced with the advancement of technology. Artificial intelligence and machine learning algorithms will be used to automate and enhance adversaries' capabilities. The integration of cyberspace with physical systems, such as critical infrastructure, will introduce new vulnerabilities since IoT devices are becoming ubiquitous (Butler, 2013). Nation-states and non-state actors, such as hacktivist groups and cybercriminal organisations, are investing heavily in offensive cyber capabilities development; they have become prominent players in cyber warfare and can cause disruptive attacks.

Moreover, military forces must integrate cyber capabilities into joint operations while coordinating traditional kinetic operations effectively to achieve mission success. Information warfare will be a central focus area: Manipulating information or spreading disinformation can significantly impact public opinion, political stability and international relations, causing strategic implications (Rantapelkonen & Salminen, 2013). Effective monitoring measures should be developed for social media manipulation campaigns not limited to spreading fake news or shaping narratives. Therefore, ingenious adaptation through continuous investment in advanced defensive measures enhancing situational awareness is necessary across nations against this evolving landscape. Robust international cooperation, together with legislative frameworks, crucially deals with the global nature rooted within cyberspace while establishing behaviour norms for effective control against these consistently emerging threats.

The evolving trends in cyber warfare have significant implications for force readiness and the Army's role in countering cyber threats. As the cyber landscape becomes increasingly complex and sophisticated, the Army must adapt its strategies, capabilities and operational doctrines to respond to these challenges effectively (Shakarian et al., 2013). Firstly, the Army must prioritise cyber readiness as a core component of overall force readiness. This includes ensuring that personnel receive comprehensive training in

cyber operations, equipping them with the necessary skills to defend against and respond to cyber threats. Additionally, the Army should invest in advanced technologies and tools to enhance its cyber capabilities, such as robust cyber defence systems, threat intelligence platforms and incident response capabilities. By prioritising cyber readiness, the Army can better protect its networks, critical infrastructure and sensitive information from cyber-attacks.

The role of the Army in countering cyber threats goes beyond defensive measures. It also includes the ability to conduct offensive cyber operations to deter potential adversaries and disrupt their capabilities. As the Army develops offensive cyber capabilities, it must ensure that these operations are conducted within legal and ethical frameworks, respecting international norms and avoiding unintended consequences (Tira, 2018). Additionally, the Army must actively partner with industry and academia to leverage their expertise, innovation and technological advancements. Collaboration with the private sector can facilitate access to cutting-edge technologies, threat intelligence and best practices. Academic partnerships can contribute to research and development efforts and the education and training of cyber personnel (Dinniss, 2012). The implications of future trends in cyber warfare highlight the need for the Army to prioritise cyber readiness, enhance collaboration and coordination within the joint force, develop offensive cyber capabilities within ethical boundaries and engage in partnerships with industry and academia. By doing so, the Army can effectively counter cyber threats, protect national security interests and maintain a state of readiness in the face of evolving cyber challenges.

Looking into the future of cyber warfare, it is evident that a joint force strategy becomes increasingly imperative in addressing complex and evolving challenges within this domain. As cyber threats surpass traditional military boundaries, multiple branches of armed forces, other government agencies and international partners collaborate to provide comprehensive and cohesive response (Kanwal, 2009). Adopting a joint force approach enables the Army to integrate cyber operations efficiently with other military components leading to an enhanced situational awareness that facilitates effective decision-making while maximising operational effectiveness. A shared pool of expertise and resources between different branches further ensures synchronised efforts across domains for developing robust defences against evolving cyber threats. This collaborative approach fosters information sharing, intelligence fusion, coordinated responses and joint exercises with allied nations, enhancing collective defence against emerging foreign actors affecting critical infrastructure beyond the military's scope.

CONCLUSION

The nature, scope, objectives, tactics and potential impact of cyber warfare are discussed, along with notable examples of cyber-attacks and their consequences. The author has also examined the different types of cyber threats and actors involved in cyber warfare while highlighting its relevance to a multi-domain operational environment. Considering force readiness as a primary concern, technical challenges such as advanced persistent threats and emerging attack vectors have been identified alongside operational obstacles such as agile defence strategies and integration issues in military planning. The role of the Army within a common force framework when confronted with evolving trends in Cyber Warfare was considered important for effective responses requiring cooperation, information sharing and coordination between relevant agencies while emphasising that investment in training development or acquisition technological advancements equipment partnerships were basic necessities too. Overall security and strengthening national infrastructure are crucial, demanding proactive measures affordable enough to security bureaus, whether it be investment incentives or ongoing research upgrades. Cyber defence measures must keep adapting these recognised principles yielding positive results buttressed by a resilient future.

REFERENCES

Brose, R. (2012). Cyber War , Netwar , and the Future of Cyberdefense. *National Intelligence United States of America*, *3*.

Butler, S. C. (2013). Refocusing cyber warfare thought. *Air and Space Power Journal*, *27*(1), 44–57.

Dar, Z. (2019). Cyber Warfare and International Law. *Jacobs University*, *April*. https://doi.org/10.13140/RG.2.2.24187.57129

Diamond, E. (2014). Applying International Humanitarian Law to Cyber Warfare. *Institute for National Security Studies*.

Dinniss, H. H. (2012). Cyber Warfare and the Laws of War. In *Cambridge University Press*. Cambridge University Press.

Gady, F.-S., & Stronell, A. (2020). Cyber capabilities and multi-domain operations in future high-intensity warfare in 2030. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, 151–176. https://www.ccdcoe.org/uploads/2020/12/Cyber-Threats-and-

NATO-2030_Horizon-Scanning-and-Analysis.pdf#page=158

Gazula, M. B. (2017). *Cyber Warfare Conflict Analysis and Case Studies* (Issue 10).

Grange, M. (2014). Cyber Warfare and The Law of Armed Conflict. *Victoria University of Wellington*.

Harris III, A. (2018). Preparing for multidomain warfare. Lessons from Space/Cyber operations. *Air & Space Power Journal*, *32*(Fall), 45–61.

Hills, A. (1997). Warfighting. *Department of The Navy*. https://doi.org/10.4324/9780203323120.ch6

Kanwal, G. (2009). China's Emerging Cyber War Doctrine. *Journal of Defence Studies*, *3*(3), 14–22. http://www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf

Lal, B., & Chavan, C. R. (2019). Analysis Report on Attacks and Defence Modeling Approach to Cyber Security. *International Journal of Scientific Research in Science and Technology*, *March*, 52–60. https://doi.org/10.32628/ijsrst196215

National Cyber Security Agency. (2020). Malaysia Cyber Security Strategy 2020-2024. *Malaysia Cyber Security*.

Rantapelkonen, E. J., & Salminen, M. (2013). *The Fog Of Cyber Defence*. National Defence University.

Robinson, M., Jones, K., & Janicke, H. (2015). *Cyber Warfare: Issues and Challenges*. *March*. https://doi.org/10.1016/j.cose.2014.11.007

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction To Cyber-Warfare A Multidisciplinary Approach* (C. Katsaropoulos & B. Rearick (eds.)). Elsevier.

Tan, J., Tee, W. X., Parsons, A., & Radlett, A. (2021). ASEAN cyberthreat assessment 2021. *Interpol*, 5. https://www.interpol.int/content/download/16106/file/ASEAN Cyberthreat Assessment 2021 - final.pdf

WINNERS OF BEST ARTICLES

SOROTAN DARAT VOLUME 2, NUMBER 81, DECEMBER 2022

1ST PLACE

ARMY 4NEXTG: CHALLENGES IN THE NEW HORIZON

Lt Kol Willie Anak Chahat
Royal Ranger Regiment

2ND PLACE

ARMY 4NEXTG: CHALLENGES IN THE NEW HORIZON

Brig Jen (Dr) Mohamad Asri bin Din
Royal Medical and Dental Corps

3RD PLACE

ARMY 4NEXTG: CHALLENGES IN THE NEW HORIZON

Lt Kol Azadlee Rafedzi bin Kamal Rafedzi
Royal Malay Regiment

INFORMATION FOR WRITERS

- The article length limit ranges from 4,000 to 6,000 words, which is around 8 to 11 pages. The writing should be in a size 12 Arial font. The text of the article should be typed at an interval of one and a half lines using the A4's paper format. Articles must be forwarded in both printed and soft copy versions to the *Bahagian Pembangunan Doktrin, MK PLDTD* (*UP: Editor Sorotan Darat*).

- The writing procedure must follow the APA standard or any procedure for writing academic articles which endorsed by the local public universities. The article must have several subheadings. Reference systems such as footnotes and bibliography/references are adopted and sorted alphabetically. An example of its writing method is as follows:

  - Flyod, K. (2009). Interpersonal Communication: The Whole Story. New York: McGraw-Hill

  - Mohd Radzi & Jusang Bolong. (2015). Komunikasi Pemimpin. Jurnal Komunikasi Malaysia , 45 (3), 89-102

  - Risya Zu. (12 Feb 2014). Etos Kepahlawanan Tentera Darat. Utusan Malaysia , ms 9

  - Rozman Malakan, (2011). Pembentukan jati diri insan. http:// www.open subscribe. com/ worldlibrarary /teks /7.html. Capaian pada 30 Mei 2016

- Diagrams, tables and pictures should be used on a limited basis and numbered as recorded in the text description.

- Requirements:

  - Each article must be forwarded together with a brief biodata/background and a softcopy of passport-sized photo of the writer.

  - A synopsis of the article not exceeding 100 words containing the main arguments/opinions discussed in the article.

REMINDER: ARTICLES MUST BE OF THE GENUINE THOUGHTS AND IDEAS OF THE WRITERS AND NOT FROM THE RESULT OF PLAGIARISM.

Bahagian Pembangunan Doktrin
Markas Pemerintahan Latihan dan Doktrin Tentera Darat
Kem Segenting
71050 Port Dickson
Negeri Sembilan