Sorotan DARAT

Volume 1, Number 84, June 2024

THE JOURNAL OF MALAYSIAN ARMY

THE VAST EXPANSION OF 5G NETWORK AND INTERNET OF THINGS (IOT) – SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM

SOROTAN DARAT
JURNAL TENTERA DARAT MALAYSIA
THE JOURNAL OF MALAYSIAN ARMY

DITERBITKAN OLEH
JAWATANKUASA 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.

Sebagai sebuah jurnal eksklusif TD, Sorotan Darat berperanan sebagai sebuah platform perbincangan berkenaan isu-isu kontemporari yang boleh menimbulkan minat profesional ketenteraan. Bermula tahun 2020, penerbitan bagi setiap siri Sorotan Darat adalah berdasarkan kepada tema-tema penulisan yang tertentu hasil cadangan dan persetujuan daripada MK TD – Cwg OPLAT serta MK TD – Cwg P&P.

Isu-isu kontroversi biasanya menjadi nadi penggerak bagi sesebuah jurnal profesional yang mana ia dapat menjadi asas pemikiran dan perbincangan yang sihat. Artikel-artikel seperti ini akan lebih diberikan keutamaan, manakala artikel-artikel mengenai operasi, idea-idea latihan atau kegunaan peralatan adalah antara topik-topik yang sangat dialu-alukan untuk diterbitkan.

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

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 would also like to thank the Editorial Board for maintaining the 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 84th edition is featuring articles related to **The Vast Expansion of 5G Network and Internet of Things (IoT) – Significance of the Army Future Soldier System**. This theme is quite current in nowadays security environment where a thorough discussion and analysis on this aspect will cultivate knowledge and perspectives of Army Officers on the said matter. Hopefully that the ideas and information highlighted by all writers would enhance the readers' knowledge, thus supporting the objective to develop Malaysian Army as a knowledge-based organization.

Last but not least, let us pray to Allah SWT for the well-being of all Army personnel. May the Almighty Allah continue to give us the guidance and strength to bring this organization excel in every aspect. 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 2024, Edition 84 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 will be discussing on '**The Vast Expansion of 5G Network and Internet of Things (IoT) – Significance of the Army Future Soldier System**'. As widely discussed, the rapid expansion of 5G networks and the proliferation of IoT devices have significantly transformed modern military operations. The strategic integration of these technologies within the Malaysian Army Future Soldier System has enhance the situational awareness and operational effectiveness, thus ensuring the more agile and responsive forces which are crucial in dealing with the uncertain environment of the future.

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 MOHD RASHID BIN ANANG
Chief Editor

ARTICLE CONTRIBUTORS

Brig Jen Rosli bin Bahrun was commissioned into the Royal Ranger Regiment on 4th April 1987. He holds a Master in Social Science (UKM 2017) and Diploma in Strategic & Defence Studies (UM 2004). He has served in various units and positions in the Army including as the Deputy Director at Infantry Directorate. He has also served at MAF Headquarters, MINDEF and ESSCOM. He is currently the Deputy Inspector General at MAF Headquarters.

Brig Jen Mohamad Ismail bin Kamarudin was commissioned on 15th August 1987 into the Royal Service Corps. He has served in various units and formations such as 11th Transport Company, 932nd Transport Company, PULMAT, RSC Directorate and also HQ of the Logistic Command. Apart from that, he has also served with MALCON V - SFOR in Bosnia & Herzegovina and MALCOY 8 in Lubnan. Currently, he is the Head of Admin and Logistic Department at East Sabah Security Command (ESSCOM).

Kol Badrul Hisham bin Nasir Nordin was commissioned on 7th September 1996 into the Royal Signals Regiment through Cadet Scheme. He holds a Master Degree in Social Sciences (2023). He also held various appointments throughout his career and among those significant appointments are Commanding Officer of 73rd Royal Signal Regiment (Electronic Warfare), SO 1 CDOC in DSID and SO 1 Training at Signals Directorate. He is currently the AKS J6 in Joint Forces Headquarters.

Kol Dr Samhasri bin Samah was commissioned into the Royal Malay Regiment on the 22nd July 1995. He has obtained his Doctor of Management Degree from the University of Malaya in 2022. Throughout his career, he has served with various units such as the 9th RMR (Para), the International Monitoring Team in Mindanao, PUSPAHANAS, 503rd TA Regiment, MAF Staff College, MK TD – CSM and currently serves at MiDAS as the Director of Regional Relations Affairs.

ARTICLE CONTRIBUTORS

Kol Zaidi bin Hj Omar joined the service in 1992 and later was commissioned into the Royal Malay Regiment. He has held numerous appointments such as Pl Cmdr of 24th RMR, OC of 19th RMR (Mech), SO 2 Ops of HQ 4th Bde (Mech) and 2IC of 18th RMR. He also served as a Directing Staff for G2 Course in Army College, Deputy Commander of the 516th TA Regiment and COS of 6th Bde HQ. In addition, he served with the United Nations Interim Force in Lebanon under MALBATT 4 from 2011 until 2012. Currently he is the COS of the 2nd Inf Div.

Lt Kol Alif Aiman bin Mohamed was commissioned on 11th January 2010 into the Royal Intelligence Corps. He holds a Master Degree in Management from UNITAR (2017) and Bachelor Degree in Mechanical Engineering from UTM (2009) as well as Post Graduate Diploma in Strategic and Studies from NDUM (2023). He has served various appointments as Intelligence Staff in the Army formations, instructor at Malaysian Armed Forces Staff College and also member of the International Monitoring Team Mindanao in 2020. He is currently serving at MDIO – Directorate of Strategic Intelligence.

Lt Kol Ts. Ir. Arjun Gopinathan was commissioned on 17th December 2005 with a bachelor's degree in Electrical and Electronic Engineering. In 2010, he obtained his master's degree in Engineering Management from University of Wollongong, Australia. He graduated with a Post Graduate Diploma in Strategic dan Defence Studies from UPNM in 2020 where he was awarded the best academic achievement with a CGPA of 4.00. He has served in various units notably at the Army Institute of Engineering, REME Directorate and Army Logistic Command HQ - EME Gp. He is currently the SO 1 Strategy and Concept at the Defence Logistics Division, MAF HQ.

ARTICLE CONTRIBUTORS

Lt Kol Mohamad Hazri bin Hamzah was commissioned into the General Service Corps (Pay) in 2003 after graduating from Akademi Tentera Malaysia (ATMA) with Bachelor of Science (Computer). He has served in various units such as MAF Staff Service Division, Seremban Staff Station HQ, 511 TA Regiment, 3rd Brigade Infantry, RMAF Base Butterworth, AFCW, 13th Infantry Bde, 12th Infantry Bde and OPLAT. He earned his Master of Business Administration (MBA) from UUM and Master of Cybergovernance and Management from Macquarie University, Sydney. Currently he is the SO 1 Finance of Defence Engineering and Service Department.

Lt Kol Mohd Rizam bin Zulkifli was commissioned on the 4th of July 2006 into the Royal Engineer Regiment from Universiti Pertahanan Nasional Malaysia (UPNM). He holds a Master in Structural Engineering and Construction (2017) and a Bachelor in Civil Engineering (2006). He has served in various units and positions in the Army, including as the Geospatial Officer in Eastern Sabah Security Command (ESSCOM). He is currently the SO 1 CIMIC at Army Headquarters – Directorate of Royal Engineer Regiment.

Lt Kol Ahmad Rosdi bin Rahim was commissioned on the 3rd of September 2001 into the Royal Electrical & Mechanical Engineer Corps. He holds a Master in Public Management – Development and Security (2016) and a Diploma in Mechanical Engineering (Aeronautic) (2000). He has completed his Staff College course in 2016 at Philippines Armed Forces Staff College, Manila. Throughout his career, he has served in various REME units, headquarters and training centres including Army School of Logistic Operation (ASLO), Australia as a Seconded Officer under Malaysian Australian Joint Defence Programme (MAJDP). Currently, he holds the appointment as SO 1 Technical Management at Army HQ – REME Directorate.

EXPANDING APPLICATIONS OF THE INTERNET OF THINGS (IOT) IN MILITARY DEFENCE: TECHNOLOGICAL INTEGRATION AND STRATEGIC IMPLICATIONS

By **BRIG JEN ROSLI BIN BAHRUN**
ROYAL RANGER REGIMENT

INTRODUCTION

The swift progress and incorporation of the Internet of Things (IoT) technology in military defence systems offer exceptional prospects as well as notable difficulties. With militaries around the world increasingly using IoT, there is a need to carefully analyse the strategic consequences of this technological transformation. Military operations use the IoT to enhance situational awareness, process real-time data, and enhance logistics. This paper will look into the increasing use of IoT in military defence, with a specific focus on the technology integration and strategic consequences, seeking to comprehensively comprehend the enhancement of IoT technologies for military applications, guaranteeing operational efficiency and security. This will be achieved by analysing existing implementations, evaluating the strategic advantages and risks, and exploring future possibilities (Darwish et al., 2017; Lin et al., 2017).

The integration of IoT technologies into military defence systems entails the deployment of an extensive range of sensors, wearable devices, and autonomous systems that communicate and function flawlessly in real-time. Several applications such as unmanned aerial vehicles (UAVs), smart uniforms, and improved logistics management systems are utilising these technologies (Ray, Chowdhury, & Roy, 2016). The IoT enables greater battlefield intelligence and operational efficiency through the provision of real-time information on adversary actions, environmental circumstances, and equipment conditions (Singh, Tripathi, & Jara, 2014; Alaba, Othman, Hashem, & Alotaibi, 2017). Nevertheless, the integration of IoT in military environments has significant concerns around cybersecurity, data privacy, and the capacity of multiple systems and platforms to function effectively together (Baig, Khan, & Ibrahim, 2017; Zeadally, Adi, Baig, & Khan, 2020). It is evident during the Ukraine-Russia's unfolded since 2022 where IoT technology integration into military operations has totally changed the battlefield dimension and started to draw new compassion to warfare in the past.

The strategic implications of IoT significantly impact the military's operations. The implementation of IoT technology has the potential to significantly enhance command and control (C2) systems, resulting in improved coordination and expedited decision-making processes (Darwish et al., 2017). The IoT enables military commanders to have a greater awareness of their surroundings, leading to more accurate and rapid decision-making. This capability is particularly important in rapid and high-risk situations (Lin, Yu, Zhang, Yang, & Zhang, 2017). In addition, the IoT enables the development of intelligent bases and automated logistics systems, which enhance the effectiveness and dependability of supply chains (Gubbi et al., 2013; Singh et al., 2014).

Although the advantages of IoT in military defence, such as enhanced operational efficiency and real-time data gathering, are substantial, it is crucial not to disregard the associated risks. The widespread utilisation of IoT devices creates opportunities for cyber-attacks and data breaches, which can have severe effects in conflict situations (Zeadally et al., 2020; Lin et al., 2017). Furthermore, it is necessary to deal with the challenges involved in achieving interoperability among various IoT devices and platforms in order to ensure effortless integration and operation (Baig et al., 2017; Alaba et al., 2017). This study seeks to look at the integration of IoT technology into military defence systems, evaluate the strategic consequences of IoT on military operations and tactics, and estimate the advantages and hazards linked to the implementation of IoT in military defence.

The IoT is revolutionising military operations by using modern technologies to enhance awareness of the situation, improve operational efficiency, and raise strategic decision-making abilities. The integration of IoT technology in military settings encompasses a diverse array of applications, including unmanned aerial vehicles (UAVs), intelligent uniforms, self-governing systems, and sophisticated logistics management. This part will examine the correlation between these applications and the goals of this paper: analysing the integration of IoT technology in military defence systems, evaluating the strategic consequences of IoT on military operations and tactics, and assessing the advantages and risks associated with the implementation of IoT in military defence. In the latest part of writing, several challenges will be discussed to examine the range of impact of the development of IoT in public and defence sectors.

TECHNOLOGICAL INTEGRATION OF IOT IN MILITARY DEFENCE SYSTEMS: THE CASE OF UKRAINE-RUSSIA WAR

IoT technology enables the implementation of a multitude of sensors and devices that gather and transfer data instantly. For instance, IoT-equipped unmanned aerial vehicles (UAVs) can collect vital data about enemy positions, environmental conditions, and battlefield topography. Command centres then receive this data for analysis (Darwish et al., 2017). Biometric sensors integrated into smart uniforms possess the ability to monitor the physical well-being of soldiers, record their activities, and transmit real-time information to medical personnel and commanders. This technology improves situational awareness and enables prompt responses in critical situations (Lin et al., 2017).

In addition, IoT enables seamless integration of self-governing systems, including robotic vehicles and drones, which are capable of independently performing duties including reconnaissance, surveillance, and logistics. These systems mitigate the risk to human soldiers and enhance operational efficiency by carrying out operations that are too hazardous or time-consuming for humans (Gubbi et al., 2013; Singh et al., 2014). The successful integration of these technologies into existing military infrastructure emphasises the capacity of IoT to transform military operations by delivering extensive and uninterrupted battlefield intelligence (Baig et al., 2017).

The advent of IoT technology is ostensibly demonstrated in the battlefield of Ukraine-Russia's war since 2022 where armed drones were widely used for reconnaissance, surveillance, targeting and even to create destruction toward the enemy. In the early stage of conflict, Ukraine, who is much inferior in terms of military personnel and hardware, was heavily relying on drones such as Turkish made TB2 Bayraktar, the US made Switch-blade and improvised commercial drone to locate and destroy much more superior Russia forces. Certainly, this tactical manoeuvre cannot be achieved without seamless IoT Technology. As the result of it, it's compelled the Russian to employ jamming equipment to hunt down the Ukraine's drones. This clearly demonstrates the evolution of military technology which has been tested to be effective in the battlefield where devices to be wildly used in substituting physical human involvement in combat situation.

In truth, Ukraine's success in early stage of the campaign comes with no surprise. The battlefield evolved rapidly when the adversary struggled to get its air defence and electric warfare

capabilities in-place which created favourable condition for Ukraine to make tactical gains. Turkey's Bayraktar TB2 weapon is capable of carrying a variety of air-to-ground munitions and loitering for long periods. This allowed Ukrainian troops to penetrate Russian air defenses and attack heavy targets (Thompson, 2024). However, this never took too long for Russia to respond by jammed and downed Ukrainian drones by disrupting their Global Positioning System links (Angevine et al 2019). On Russia's side, models such as the Lancet, Eleron-3, Orlan-10, and Orion were widely deployed against Ukraine's defence position, but shredded due to the shortage of production. Instead, Russia had turned to Iranian-made Shahed-136 drones which has better payload and can operate in longer distance (Thompson, 2024).

In essence, it is clear that this conflict has demonstrated the battlefield advantages of drones that largely credited to the advent of IoT technology. It is smaller, more lethal, easier to operate, and availability provides enabling medium to make targeting to destroy processes faster and more precise. Drones with longer endurance profiles are able to effectively conduct hours of reconnaissance, allowing other, more advanced drones to conduct precision strikes deep inside and even until the behind enemy territory. Another advantage of this model is that it allows individual soldiers to monitor enemy movements without risking lives or exposed the soldier's position (Thompson, 2024).

❖ Strategic Implications of IoT on Military Operations and Tactics

The IoT presents a multitude of strategic implications for military operations and tactics, revolutionizing the way armed forces gather intelligence, conduct operations, and engage with adversaries. Military operations may greatly benefit from the strategic implications of IoT, especially in improving command and control (C2) systems. The use of IoT technologies enables rapid data gathering and examination, allowing commanders to make well-informed decisions in a timely and precise manner. IoT-enabled command and control (C2) systems have the capability to combine data from many sources, including unmanned aerial vehicles (UAVs), ground sensors, and troops' wearable devices, in order to generate a complete operational overview (Ray et al., 2016). Among of the advantages from IoT-enabled devices such as drones and smart munitions can be used for precise targeting of enemy assets, minimizing collateral damage and civilian casualties while maximizing the

effectiveness of military strikes. Enhanced situational awareness enables military commanders to efficiently coordinate movements, allocate resources, and implement strategies (Lin et al., 2017).

Furthermore, the IoT enables the development of intelligent facilities and automated logistical systems. Smart bases utilise IoT sensors to oversee and control resources, including energy usage, security systems, and supply stocks. This results in improved efficiency and sustainability in operations (Alaba et al., 2017). Automated logistics systems employ the IoT to monitor the real-time whereabouts and condition of items, guaranteeing prompt delivery and minimising the possibility of shortages during crucial operations (Zeadally et al., 2020). These strategic improvements highlight the potential of the IoT to enhance the efficiency and effectiveness of military operations. This aligns with the purpose of evaluating the strategic impact of the IoT on military operations and tactics.

❖ Benefits and Risks Associated with the Adoption of IoT in Military Defense

The advantages of IoT in military defence are substantial, encompassing higher operational efficiency, improved situational awareness, and enhanced decision-making capabilities. Real-time data collection and analysis allows military forces to promptly and efficiently address threats, potentially resulting in the preservation of lives and resources (Darwish et al., 2017). The IoT also enables the implementation of predictive maintenance for military equipment, which helps to minimise time and prolong the lifespan of crucial assets (Gubbi et al., 2013).

Nevertheless, the implementation of IoT in military environments presents significant risks. The vulnerability of IoT devices to hacking and cyberattacks poses a significant threat to cybersecurity, potentially compromising key military data and operations (Zeadally et al., 2020; Lin et al., 2017). To protect military IoT systems from potential threats, we must overcome vital challenges such as safeguarding data privacy and fortifying communication channels. Lack of compatibility between different IoT platforms and devices can also make it harder for them to work together smoothly. This shows how important it is to have standardised protocols and strong

security measures (Baig et al., 2017; Alaba et al., 2017). To summarise, the use of IoT applications in the military has the ability to completely transform defence operations through the enhancement of technical integration, the improvement of strategic decision-making, and the provision of substantial advantages. Still, it is crucial to confront the related risks and difficulties in order to effectively exploit the capabilities of IoT in military defence.

ASSESSING THE STRATEGIC IMPLICATIONS OF IOT ON MILITARY OPERATIONS AND TACTICS

The strategic consequences of IoT in military operations are significant and diverse, radically altering the way military forces carry out operations, make decisions, and accomplish strategic objectives. IoT technologies provide heightened awareness of the situation, increased command and control (C2) systems, and more efficient logistics management. These improvements collectively improve the effectiveness and responsiveness of military operations.

An important strategic consequence of the IoT in military operations is an improvement in situational awareness. IoT devices and sensors gather huge amounts of real-time data from the battlefield. This data includes information regarding enemy activities, environmental circumstances, and the condition of military resources (Darwish, Hassanien, Elhoseny, Sangaiah, & Muhammad, 2017). Command centres receive the transmitted data, examine it, and combine it into a detailed operational overview, empowering commanders to make well-informed decisions efficiently and precisely (Lin, Yu, Zhang, Yang, & Zhang, 2017). Improved situational awareness empowers the armed forces to anticipate possible risks, adjust to evolving circumstances, and synchronise activities with greater efficiency, ultimately enhancing their operational effectiveness.

The integration of IoT technology greatly enhances Command and Control (C2) systems by facilitating uninterrupted communication and efficient data exchange across different military units and platforms. The integration of IoT devices into C2 systems enables the seamless and synchronised interchange of real-time data among soldiers on the ground, UAVs, and command centres, hence establishing a cohesive operating environment (Ray, Chowdhury, & Roy, 2016). As a result, IoT-enabled autonomous systems, such as UAVs and unmanned ground vehicles (UGVs), have the potential to revolutionize military tactics by providing persistent surveillance,

reconnaissance, and strike capabilities without putting human operators at risk. The improved connectivity enables commanders to efficiently coordinate actions with higher accuracy and swiftness, thereby lowering the time needed to carry out strategic decisions. Enhanced Command and Control (C2) skills are especially crucial in dynamic and high-risk contexts, where prompt and precise decision-making can significantly impact the outcome of military conflicts (Zeadally, Adi, Baig, & Khan, 2020).

The integration of IoT technology into military logistical systems also carries substantial strategic ramifications. Logistics management systems that utilise IoT technology monitor the real-time position and condition of supplies, guaranteeing the timely and accurate delivery of essential resources to their designated destinations (Gubbi, Buyya, Marusic, & Palaniswami, 2013). This feature decreases the likelihood of running out of supplies and improves the effectiveness of logistical operations, which is essential for ensuring operational readiness and supporting military forces during prolonged deployments (Alaba, Othman, Hashem, & Alotaibi, 2017). In addition, the use of IoT sensors allows for predictive maintenance, which helps to anticipate equipment breakdowns and schedule maintenance in advance. This proactive approach has extended the lifespan by reducing downtime of military assets. The use of IoT technologies also improves armed forces' strategic adaptability and flexibility. Military forces can rapidly adjust to changing threats and operational conditions by gathering and examining real-time data from several sources. IoT-enabled unmanned aerial vehicles (UAVs) can offer up-to-the-minute reconnaissance and surveillance data, enabling commanders to adapt their tactics and strategies according to the most recent intelligence (Darwish et al., 2017). In contemporary battles, the ability to move quickly and accurately is essential, as it can offer a significant advantage in determining battle outcomes.

While using IoT in military operations offers significant strategic advantages, it also presents substantial challenges and factors that require careful consideration. The vulnerability of IoT devices to hacking and cyberattacks poses a significant risk to cybersecurity, potentially compromising important military data and operations as adversaries may attempt to exploit weaknesses in networked systems to disrupt military operations or steal sensitive information (Zeadally et al., 2020; Lin et al., 2017). It is crucial to safeguard IoT-enabled systems to prevent potential risks and maintain their security and integrity. Furthermore, the lack of compatibility across various IoT devices and platforms can impede seamless integration and

functioning. This highlights the importance of implementing standardised protocols and strong security mechanisms (Baig, Khan, & Ibrahim, 2017). Standardizing communication protocols and data formats can help overcome these challenges and facilitate seamless integration of IoT technologies into military operations.

The use of IoT in military operations has significant strategic consequences, as it brings about transformative changes. It provides improved situational awareness, expanded command and control capabilities, the efficient administration of logistics, and increased strategic agility. However, it is crucial to deal with the related risks and difficulties in order to effectively exploit the capabilities of IoT in military defence, as adversaries may attempt to disrupt IoT networks through electronic warfare tactics such as jamming or spoofing, thus, developing countermeasures to defend against these threats is essential to maintaining the reliability and integrity of IoT-enabled military systems.

IOT APPLICATIONS IN MILITARY DEFENCE: STRATEGIC IMPLICATIONS AND FUTURE SOLDIER SYSTEMS IN MALAYSIA

IoT is transforming military operations by augmenting situational awareness, enhancing command and control (C2) systems, and optimising logistics. The integration of this technology is not only revolutionising military operations around the world, but it also has important consequences for Malaysia's future military systems. The discussion will focus on the strategic implications and their relevance to the Malaysian context. The use of IoT technologies enables the immediate gathering and analysis of data, giving armed personal an in-depth understanding of their surroundings. Sensors and gadgets integrated into UAVs, smart uniforms, and ground sensors can gather data on enemy movements, surrounding circumstances, and equipment status. Command centres receive this data for immediate analysis (Lin et al., 2017). This skill enables commanders to quickly make well-informed decisions, thereby improving the efficiency and responsiveness of military operations. Integrating IoT into the Malaysian Armed Forces in Malaysia has the potential to greatly enhance their capacity to promptly monitor and address threats in real time, namely in the South China Sea and other strategically important regions (Alaba et al., 2017).

The integration of sophisticated technologies in Military Defence Future Soldier Systems (FSS) using the Internet of Things (IoT) aims to enhance the operational capabilities, situational awareness, and survivability of military personnel, thus modernising

their approach. These systems encompass a variety of technologies, including wearable sensors, augmented reality (AR) devices, advanced communication systems, autonomous vehicles, and AI-driven logistics and decision-making tools. The primary objective of FSS is to establish a unified and compatible network of soldiers and equipment that operates effectively in diverse combat situations. The main elements of the FSS consist of the Integrated Visual Augmentation System (IVAS), the Enhanced Night Vision Goggle-Binocular (ENVG-B), and the Nett Warrior system. These elements interact in order to enhance the soldier's capability to communicate, navigate, and engage with the adversary in a highly efficient manner. These technologies utilise recent advances in virtual reality, thermal imaging, GPS technology, and secure communication networks to deliver real-time data and practical insights on the battlefield (News - European Security & Defence) (SMG Conferences).

- **Improved Command and Control (C2) Systems**

The integration of IoT technology into C2 systems allows for seamless and effective communication and data exchange among various military units and platforms. This improved connection provides more effective coordination and expedited decision-making, which is essential in rapid and high-risk situations (Ray, Chowdhury, & Roy, 2016). The Malaysian military might strengthen their operational capabilities by implementing IoT-enabled C2 systems to achieve more precise and efficient coordination during joint operations and peacekeeping missions (Zeadally et al., 2020).

- **Efficient Logistics Management**

The IoT also plays an important role in military logistics administration. IoT systems provide the capability to monitor and track the precise position and condition of supplies in real time. This guarantees the prompt and precise delivery of essential resources. This feature minimises the likelihood of supply deficits and improves the effectiveness of logistical activities. Integrating IoT technology into military logistics in Malaysia has the potential to enhance the efficiency of supply chain management and equipment maintenance, guaranteeing the preparedness of the armed forces for deployment (Darwish et al., 2017).

❖ Future Soldier Systems in Malaysia

The use of IoT technologies could significantly improve future Malaysian Armed Forces Soldiering systems. Biometric sensors integrated with smart uniforms have the capability to monitor the physical well-being and effectiveness of soldiers, offering immediate data to medical personnel and commanders (Lin et al., 2017). Wearable devices have the capability to monitor and record the whereabouts and activities of soldiers, thereby improving their awareness of the surrounding circumstances and ensuring their safety. In addition, autonomous systems equipped with IoT technology, such as drones and robotic vehicles, have the capability to carry out reconnaissance and surveillance missions. This reduces the risks faced by human soldiers and enhances the efficiency of operations (Ray et al., 2016).

To date, there are several IoT technology related systems have been used in the MAF services. For instance, the C4ITAC system which provides secured real-time communication facility to MAF for routine monitoring and reporting procedures. ScanEagle Drone used by the Royal Malaysian Navy (RMN) for maritime surveillance at South China Sea and the Royal Malaysian Air Force (RMAF)'s purchase of Turkish made Anka-S UAV which provides better durability than the ScanEagle are the current inventory of IoT devices in the MAF. It is anticipated that there will be more procurement in the future, which is proven to be effective and efficient in both financial and human security consideration.

❖ Challenges and Considerations

While IoT offers significant advantages in military defence, it also presents various challenges that require resolution. The vulnerability of IoT devices to hacking and cyberattacks poses a significant threat to cybersecurity, potentially compromising key military data and operations (Zeadally et al., 2020). Addressing major concerns about data privacy and safeguarding communication networks is critical. Moreover, the lack of compatibility across various IoT devices and platforms can impede seamless integration and functioning, emphasising the importance of standardised protocols and strong security mechanisms (Baig et al., 2017).

The use of drones by military, particularly in carrying out surveillance, mapping, logistics and intelligence gathering is

aimed to reduce the numbers of personnel being deployed in carrying out these activities as well as dangerous activities such as combating the enemy in the battlefield. However, it carries residual risk where legal and ethical issues following with the increased use of drones in combat mission. Besides that, the usage of public and commercial drones is expected to impact significantly upon the security and safety of the public, and not to forget the serious implications for public privacy (Anawar, S. et al.,2019). An uncontrolled public privacy breaching will create public unrest and damaging human values.

On the use of airspace, it is crucial for the government to control the numbers of military drones and civilian aircrafts to fly at the same times to avoid unnecessary air mishap. This conflict needs to be resolved, through devising policy and rules to safeguard the drones whilst upholding military and commercial priorities. In Malaysia's context, drones may not be flown in Class A, B, C or G airspace; within an aerodrome traffic zone; or more than 400 feet above the ground and drone pilots must maintain a direct visual line of sight with their drones during operations (Noor, N. M. et al., 2018).

With largely relying on foreign technology due to lack of domestic Research and Development (R&D) in defence IoT, this phenomenon had compelled MAF to procure equipment from foreign Original Equipment Manufacturer (OEM) or transfer of equipment from friendly countries such as U.S. This encompasses design, supply and maintain the IoT platforms by the foreign entity which is seen to be able to compromise the security at certain extent. In addition, it is expected to cost more and implicitly affect the financial sustainability and flexibility in long terms. As such, it is crucial for Malaysia to double up high-end technology development in order to meet the commercial and defence sector demand. A self-sustain policy will definitely ensure to continuous supply of defence IoT without reliance of foreign support.

CONCLUSIONS

The integration of IoT technologies in military defence systems has exceptional possibilities for expanded situational awareness, evolved command and control (C2) capabilities, and streamlined logistics management. IoT devices and sensors gather real-time data from the battlefield, giving commanders a comprehensive operational

overview and allowing for immediate and well-informed decision-making. These technologies also enable seamless interaction across different military units and platforms, enhancing coordination and decreasing the time needed to carry out strategic decisions. It is proven in the case of Ukraine-Russia's war where the inclusion of drone devices changes the whole landscape for the battlefield. Despite unconventionally use of drone in undermining adversary fighting capability, it is undeniably the proper use of drone may deliver instant tactical results and contribute to the strategic ends.

Military operations derive considerably from the strategic implications of IoT, as IoT technologies allow for increased situational awareness, enhanced C2 systems, and more effective logistics management. The Malaysian military may significantly improve their operational capabilities by implementing IoT-enabled devices. This would help them to achieve more accurate and efficient coordination during joint operations and peacekeeping missions. Integrating IoT into military logistics could improve supply chain management and equipment preservation, ensuring constant readiness for armed troop deployment.

Although there are significant advantages, the implementation of IoT in military environments also presents considerable risks. The vulnerability of IoT systems to hacking and cyberattacks poses a significant security risk, potentially compromising key military data and operations. Preserving data confidentiality and fortifying communication channels are imperative to safeguarding military IoT systems against potential hazards. Furthermore, the lack of compatibility across various IoT devices and platforms might impede effortless integration and functioning, emphasising the importance of standardised protocols and strong security measures. Other challenges may include the safety of airspace, public privacy and personal data breaching and lastly the financial flexibility in sustaining IoT in the defence sector will certainly impact the use of IoT in the future.

In a nutshell, Malaysia's proficiency in managing IoT for military defence is improving, indicating significant potential for expansion and advancement. The nation's allocation of resources towards advanced technology and infrastructure, along with the establishment of strategic relationships and cooperative efforts, can expedite the seamless integration of IoT into military endeavours. To fully use the potential of IoT and strengthen national security, Malaysia must confront and overcome the risks and challenges associated with it.

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

Anawar, S., Zakaria, N. A., Masu'd, M. Z., Muslim, Z., Harum, N., & Ahmad, R. (2019). IoT technological development: Prospect and implication for cyberstability. *International Journal of Advanced Computer Science and Applications*, *10*(2).

Angevine, R., Warden, J. K., Keller, R., & Frye, C. (2019). Learning lessons from the Ukraine conflict. *Alexandria, VA: Institute for Defense Analyses, document NS D-10367, May*, *1*.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.

Baig, Z. A., Khan, F. A., & Ibrahim, A. A. A. (2017). Internet of Things (IoT): Security and privacy issues and challenges. Future Internet, 9(4), 77.

Bakar, K. A., & Islam, M. D. (2019). The impact of the Internet of Things on military operations in Malaysia. Journal of Emerging Technologies and Innovative Research, 6(6), 239-244.

Bala, A., & Singh, P. (2018). Emerging applications of Internet of Things in military: An overview. International Journal of Computer Applications, 179(30), 1-6

Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2017). The impact of the Internet of Things on the future of intelligent transportation systems: A survey. IEEE Transactions on Intelligent Transportation Systems, 20(5), 1823-1841.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors*, *16*(10), 1644.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

Lin, J., Yu, W., Zhang, N., Yang, X., & Zhang, H. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

Noor, N. M., Mastor, I. Z., & Abdullah, A. (2018). UAV/drone zoning in urban planning: Review on legals and privacy. In *Proceedings of the Second International Conference on the Future of ASEAN (ICoFA) 2017–Volume 2: Science and Technology* (pp. 855-862). Springer Singapore.

Puthal, D., Ranjan, R., Nanda, P., Mohanty, S. P., & Obaidat, M. S. (2018). Secure and sustainable load balancing of edge data centers in fog computing. IEEE Communications Magazine, 56(5), 60-65.

Ray, P. P., Chowdhury, C., & Roy, A. (2016). Internet of Things for military applications: A review. International Journal of Future Computer and Communication, 5(1), 21-27.

Singh, S., Tripathi, R., & Jara, A. J. (2014). A survey of Internet-of-Things: Future vision, architecture, challenges and services. Internet of Things Journal, 1(1), 10-21.

Wahab, A. W. A., & Pengiran, A. R. R. A. (2019). Smart defense with IoT for Malaysian armed forces: Challenges and opportunities. Defence Science Journal, 69(1), 83-89.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing the power of Internet of Things based services for military operations. IEEE Communications Magazine, 58(4), 74-79.

Zhou, W., Zhang, Y., & Liu, P. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2), 1606-1616.

THE VAST EXPANSION OF 5G NETWORK AND INTERNET OF THINGS (IOT) – SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM

By BRIG JEN MOHAMAD ISMAIL BIN KAMARUDIN
ROYAL SERVICE CORPS

"Any sufficiently advanced technology is indistinguishable from magic"
Arthur C. Clarke (2001)

INTRODUCTION

Over the past 40-decade, generation was introduced with something new that we can transmit with our life especially in Internet Information Technology (ICT). The development of ICT started in 1980s, they gave us a technology so call sound, in early 1990s, they gave us texts, in early 2000s, world received the mobile web and from 2010s, 4G made our live more interesting with live video streaming. Today the 5G promises us to be ultra-fast, with peak data rates of up to 100 times faster than 4G. More interesting, it supports near-zero latency, which means there will be practically no delay in sending and receiving information between devices. With a lag of just one millisecond, the devices can talk to each other in almost real time.

WHAT IS 5G AND IOT

5G is fifth-generation wireless (5G) is the latest iteration of cellular technology. Alexander S. Gillis in his article 5G: Guide to Planning, Architecture and Benefits explained 5G was engineered to greatly increase the speed and bandwidth of wireless networks while also reducing latency when compared to previous wireless standards. Now, 5G is a very significant gadget for development in the field of telecommunications, while IoT is a platform that will use these facilities to increase and expand ICT dominance in all fields. For example, cellular companies began deploying 5G networks in 2019 as the successor to fourth-generation wireless (4G). Alexander S. Gillis also highlighted in his article, with 5G, data transmitted over wireless broadband connections can travel at multigigabit speeds, with potential ideal peak download speeds as high as 20 gigabits per second (Gbps). These speeds exceed wire line network speeds and can provide latency below 5 milliseconds (ms) or lower than iut. This is especially true for applications that require fast time response in multiple domains. Today's 5G is able to accommodate a dramatic increase in the amount

of data transmitted over wireless systems due to more available bandwidth and advanced antenna technology.

According to IBM, Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data. It also known as “smart gadget” which can range from simple “smart home” devices such as smart thermostats, to everyday hardware such as smart watches, industrial machinery and a complex network of transport systems. Technologists also envision a whole "smart city" based on IoT technology to be adopted in the near future. IoT allows these smart devices to communicate with each other and other devices with a wide network by using the capabilities of the internet. IoT is also seen in completely taking over the defence system of a country within a few decades.

- **Monitoring Environmental Conditions**. This technology called clean technology which able to support the detection of noxious substances, chemical spills, harmful pollutants and more, enabling governments and industries to clean and protect our air, soil, and water.

- **Managing Traffic Patterns**. These devices in our city infrastructure provide us with real-time data on traffic conditions, vehicle counts and pedestrian movements.

- **Controlling Machines and Processes in Industries**. IoT is an ever-evolving network embedded with advanced sensors. These sensors exchange data with other systems and devices across the internet allowing industry management to be shared globally. Data in this vast communication allows action or response, making orders, optimizing processes and making the equipment attached to them more accessible and convenient for users without limit.

- **Tracking Inventory and Shipments in Warehouses**. Devices and sensors that use IoT capabilities allow inventory or stock tracking to be done quickly and accurately. Stock storage management, the ability to monitor warehouse environment conditions and the ability to detect anomalies immediately are among the characteristics of IoT capabilities. In general, this transformative technology is able to improve efficiency, accuracy and profitability in the warehousing industry.

- **Security and Safety**. IoT is able to improve combat effectiveness including logistic support to frontline forces.

SECURITY vs IOT

The potential of IoT applications is vast and has spanned various industries such as manufacturing, transportation networks, health, agriculture and security. Along with the development of the internet nowadays, it is believed that IoT will play a role in shaping the way of life, the way of working and interacting. For example, in agriculture and manufacturing, IoT is able to monitor temperature, humidity, air quality and energy use including machine performance. In terms of safety and security, IoT plays a major role in today's warfare. It not only focuses on the sophistication of assets that military personnel need to have but also covers how IoT works in all forms of conflict and threats.

In this context, as a modern-day soldier, the roles and responsibilities assigned to military personnel are broader than before. Mission can vary from deployments in harsh conditions and environments combating hostile threats in both rugged and urban situations, to military and humanitarian support to provide aid and clean up after natural disasters. The tools and equipment they need to perform tasks are based on tasks and threats and these requirements change depending on the current development of the IoT. Technically advanced products that use the latest technology are very helpful for military personnel to perform tasks effectively to achieve the assigned mission. This includes provision of communications networks, detection, protection, real-time situational awareness and enhanced data analysis.

The importance of IoT is not only limited to military personnel conducting operations. IoT is also needed by the Malaysian Army in logistics management. In this context, the logistics management of the Malaysian Army needs to focus more broadly including SMART stores, centralized control of land, sea and air movements as well as integrated management of personnel assets and equipment.

HOW 5G AND IOT EFFECTED OUR MALAYSIAN ARMY FUTURE SOLDIER SYSTEM ENVIRONMENT

As we all know, the vast ability of 5G and IoT which promise of evolutionary change in network performance. Here there are four areas which significantly affected our military live and work system.

- **Enhanced Mobile Broadband**. Faster speed, lower latency and greater capacity of 5G is highly needed in the Malaysian Army. Nowadays, the use of mobile phones as a means of communication whether in peace or conflict is an important priority for the Malaysian Army. The occurrence of major floods on the East Coast of Malaysia in 2022 proves the importance of this smart communication tool to ensure that rescue operations can be carried out effectively. The use of sophisticated communication tools was also proven during the implementation of the Movement Control Order implemented by the Malaysian Armed Forces when the country was dealing with the COVID-19 virus.

- **IoT**. Todays, the existing cellular networks are unable to keep up with the rapid growth in the number of connected devices. Therefore, the Army needs a platform that is capable and powerful to provide a wide, fast and efficient communication system with low power consumption. The national borders that include the north and south of the Peninsula as well as in Kalimantan require constant surveillance. The method of patrolling on foot or by vehicle needs to be strengthened to be more effective. The use of drones that are capable of exploring unexplored areas is important to ensure the security of national borders is not invaded. The use of IoT is not only focused on national border control but is also capable of impacting rescue operations carried out by the Army.

- **Mission Critical Control**. Connected devices are increasingly used in applications that require absolute reliability, such as in logistics system. As reminded by Napoleon "*An army marches on its stomach*". The logistics management of the Army, for example, is in dire need of 5G Network and IoT so that logistic planning in line with needs of Army 4nextG, formations and units. Accurate, integrated data with prioritizing real time data is needed by our Army today, especially at the Army Logistics Headquarters. Issues such as head to toe shortages, vehicles without spare parts, damage to military quarters and camps need to be integrated with the use of IoT under one Mission-critical control platform. In fact, it would be more efficient if all the movement of vehicles in the Malaysia Army could be monitored in one control.

- **Fixed Wireless Access**. The speed of data provided by the IoT is much needed by the highest leadership of the Army. Accurate and fast data will definitely allow deployment of troops

and logistic support to be planed effectively. Therefore, speed in decision-making is very necessary for the leadership of the Army in an effort to form Army personnel who are capable of facing any threat in the future.

ARMY FUTURE SOLDIER SYSTEM

We consider the Army Future Soldier System to be a modern-day soldier. There are various roles that must be performed by military personnel who are titled Future Soldiers. This is because the first responder that needs to be given is more extensive than before. Respondents also vary in terms of threat level, environmental conditions, weather and type of operation. At the same time the development of the current conflict that the world is facing also has an impact on changes to asset technology.

Technically advanced products that have adopted the latest technology are greatly capable of protecting of people and helping them do their jobs better. These products can provide enhanced communication, detection, protection, real time situational awareness, and data analysis. The soldier can now be more capable and confident and becomes a greater value as an asset in his environment. Imagine how advanced IoT can help soldiers on the battlefield where they can flip their transparent screens from their helmets to scan the landscape to identify their own troops or enemies. In fact, not only for identification and location, but with a visual scan allows military personnel to know their health status and readiness to be on the battlefield. In this contest, biometric sensors embedded in uniforms and equipment can detect more than just the above vital signs.

Soldiers of the future need to be provided with quick and accurate information regarding how much rest they need, hydration, concentration, alertness, blood sugar, metabolic status and energy reserves, altitude adjustment, how many bullets are needed to face the threat, battery level communication tools and potential exposure to chemicals and toxic substances by simply scanning the visuals provided. This is what the military of the future will need and it will depend heavily on 5G and IoT. On the other hand, availability of real-time answers to questions such as: Where is the enemy? In what location are our troops? Are our troops prepared to engage? Do they require combat supplies? Should they take a break, change shifts, need other supplies? Another question that needs to be thought about, are military personnel who are in the battlefield exposed to chemical or biological hazards? and how the advantage of IoT in overcoming these threats. This is because, the role of the future soldier will continue to

evolve from a tactical combat operator and combat role to a complex human sensor with greater cognitive capabilities.

HOW MIGHT 5G AND IOT TECHNOLOGIES IMPACT TO MALAYSIAN ARMY FUTURE SOLDIER SYSTEM?

If 5G is deployed in Army Future Soldier System across these four commercial domains, namely the Deployment, Asset, Logistic Support and Healthcare it will be captured with creative applications of advanced connectivity. Here are the four domains with some of the biggest potential to impact the Army Future Soldier System:

- **Deployment of Troop**. With the 5G architecture and the deployment of Networks and the Internet of Things (IoT) occurring worldwide, electronic warfare (EW) requirements and spectrum management applications are also impacting the Army's operations. Intelligence, Surveillance, and Reconnaissance (known ISR) systems can change the way our military gathers intelligence data that can help commander make the right decisions in any conflict. As discussed, the use of drones in controlling national border security can not only have a major impact on border security, but can also increase the level of intelligence and surveillance, especially in areas that are beyond the reach of patrolling personnel. Real time data provided is very important to ensure the deployment of troops is at the right time and location. This proved that the use of drones was effectively used during Operation BENTENG during the Movement Control Order - COVID 19. In other contexts, the data obtained needs to be processed quickly to allow real time to be provided. Therefore, the Army Future Soldier System needs to be equipped with a platform capable of storing and analysing the data received. It functions as mission-critical control and needs to be established in two formations, namely the Army's Western Command Headquarters and the Army's Eastern Command Headquarters before being consolidated at the Army Headquarters and the Malaysian Armed Forces Headquarters.

- **Asset**. Although Malaysia still adheres to the ASEAN principle - non-interference is the original core foundation upon which regional relations between ASEAN member-states and the alliance with The Five Power Defence Arrangements (FPDA), in terms of asset acquisition, the Malaysian Army cannot deny the existence of technology that needs to be aligned with the development of global and regional conflicts today. China's presence in the South China Sea,

security in the Straits of Malacca, current developments on the Kalimantan border, Thailand's desire to build the Kra Canal and security in East Sabah are among the aspects that require the Malaysian Army to provide members and forces that are truly capable of dealing with various threats. and conflict.

- **Hypersonic Weapons**. The geography of Malaysia, which has a long coastline and is equipped with extensive space and two landmasses separated by a vast ocean, requires an effective defence system. Therefore, the Malaysian Army Future Soldier System requires hypersonic weapons that provide the best weapons equipment to all soldiers. In this context, hypersonic defence systems need to be developed within the Malaysian Army so that they meet the needs of the Army Future Soldier System. It includes weaponry, training systems and equipment based on conflict and threat. In short, a large amount of real-time data processing powered by artificial intelligence on targets and trajectories will be required by the Malaysian Army to face any threat both from abroad and within the country. This strength is what the Malaysian Army needs in order to ensure that they deserve the title of Malaysian Army Future Soldier and this is where 5G and IoT play a role.

- **SMART Military Training Facility**. The best moral for a soldier is training. In shaping the Future Soldiers of the Malaysian Army who are truly professional, the Army needs a training facility complete with sophisticated facilities. 5G and IoT capabilities should be empowered such as the use of simulators in all training conducted prior to field training. A training system integrated with real-time logistical support, realistic troop deployments and conflict environments will be able to provide efficient military personnel in the face of all threats. In other contexts, changes to the training system used should be adopted in line with the needs of the Solider Future Army. This includes the ability of Malaysian Army personnel to master the field of ICT. Without fail, all members must be proficient in all systems used in the Army. At the same time, the Malaysian Army needs to focus on developing a SMART Army Base by adopting 5G and IoT. For example, the use of CCTV for camp security and adopting 5G in effective unit administration system.

- **Battle Network**. Speed is everything on the battlefield, and 5G's lower latency and higher capacity will allow the military to share more data, such as real-time maps and photos of battlefield scenarios, as well as computer simulations. The true potential of 5G will impact the battle networks of the future. Undoubtedly, this network will continue to increase to include a large number of systems that are more and cheaper, more connected and more resilient to function in the face of threats or conflicts. the Malaysian Army needs to find a way to ensure that 5G and IoT become a strength in the Army War Gaming Centre (POP TD). Today's systems need to be integrated with all threats and conflicts including logistics support systems. The Battle Network facility at POP TD is important in building Army personal who are capable of performing duties as Army Future Soldier.

- **Artificial Intelligence**. Unmanned aerial vehicles (UAVs) – AKA drones – are already used by the Malaysian Army. However, they don't transmit and share real-time 4K video and other data across command-and-control centre, and units in the battlefield. With 5G comes 4K video, object recognition, faster data processing and artificial intelligence which will help reconnaissance missions and giving Army units' information on what they're about to come up against. 5G could also help in more accurately and intelligently targeting weapons. In the future, drones in the Army are an important asset. Therefore, drone acquisition planning is no longer limited to Combat Forces, Combat Support and Service Support units are deserving attention. This is because the deployment of both units during conflict or war requires aerial surveillance and protection. In another context, monitoring the movement of logistic vehicles also needs to adopt 5G and IoT. This is because with the presence of a platform equipped with 5G and IoT facilities, the movement of assets in the Army will be easy to regulate.

❖ **Logistic Support**. In order to provide effective and efficient logistics support, every logistician need a system that is able to provide the data needed by formations and units in the right time, the right quantity or in other words real time data. Therefore, 5G and IoT are platforms that are able to provide those needs. 5G and IoT will enable a reduction in the time

between data capture and decision-making that allows the supply chain to respond to changes in real-time allowing the necessary logistics assistance to be delivered at the right time, in the right quantity and cost effectively. In this context, the need to strengthen the Army Future Solider is not only focused on the combat forces but also involves the logistics forces.

- **Army Supply Chain Automation**. In logistic principle, the supply chain consists three major elements. The first one is the stocking of appropriate quantities of supplies within a distribution zone. Second is the movement of supplies within distribution zone, including to and from drop points for interfacing with delivery vehicles and last elements is transportation of goods from the distribution zone until to end users. In all these elements, 5G and IoT play an important role as a key platform to ensure that deployed forces will be equipped with combat supplies. As mentioned above, logisticians need accurate data based on conflict situations. The accuracy of this data can only be transmitted to the Army Logistics Headquarters if 5G capability is available at all levels of command. Therefore, the logistics platform of the Malaysian Army needs to be developed based on 5G and IoT. This is important to ensure that the needs of empowering the future soldiers of the Malaysian Army can be implemented in an integrated manner, taking into account all aspects including logistical requirements.

- **Movement and Logistical Systems**. Transportation and logistics systems are also impacted by the development of IoT. Fleets of military cars, trucks, ships, and trains that carry military asset can be rerouted based on weather conditions, vehicle availability or driver availability. By using IoT sensor data all movements can be controlled by higher levels. The inventory itself can also be outfitted with sensors for track-and-trace monitoring and temperature control. Additionally, the food and beverage and pharmaceutical industries that often carry temperature-sensitive inventory are sure to benefit greatly from IoT application developments. In nut shell, IoT is also needed in the supply and preparation of food in the Malaysian Army. In another context, the use of this IoT sensor is not only effective during war/conflict but can also be used as a gadget to reduce the rate of road accidents in the Malaysian Army if it is widely integrated

with the Movement Control Centre and vehicle drivers. IoT Sensors will easily provide information to the Movement Control Centre on the endurance level of the driver, the distance travelled and fuel consumption. And then 5G will play a role in regulating vehicle movements accordingly.

- **Malaysian Army 4th Line Support**. The 4th line support units of the Malaysian Army are in dire need of a system capable of providing front line units with their logistical needs in the right place, quickly, in the right quantity and cost effectively. In this context, the Malaysian Army needs to be equipped with efficiency systems to ensure that the principles of directed, push and pull can be implemented.

- **SMART Store**. In this context, the Army Logistics Headquarters, needs to be equipped with the best management system. The use of SMART stores should be adopted in all Malaysian Army stores in both regions. Integrated controls need to be built into the system to benefit all personal of the Army. The use of IoT should be adopted in asset inventory management from receipt to disposal that includes all classes of asset. For example, in 'Head to Toe' management, it needs to be supervised at the highest level so that the acquisition of equipment can be implemented based on the current needs of the Army. In this context, control using BAT L 117 which has been a practice for a long time needs to be replaced with a system that adapts to IoT. It strongly believed, by adopting this concept, it will help the Army in the preparation of the annual budget and will be able to ensure that all military personnel can be supplied with equipment correctly and accurately.

- **Movement Control Centre**. In accordance with the principle of movement held by the Malaysian Army, movement control at the highest level should be present in the Malaysian Army system. The Malaysian Army needs to adapt the concept of IoT in the Future Solider System. This system must adapt to IoT to provide a system that is able to centrally control land, sea and air movement. It would be good if the control of this movement could be integrated in both regions.

- **Healthcare**. The transformative nature of technology in healthcare provided by 5G and IoT is also an important element in the development of the Army's Future Soldier. The development of the Army's Future Soldier is not only focused on advanced military equipment, but also on the health care needs by military personnel. Clinical applications, education and research in field medicine and surgery are essential for military personnel whether in peacetime or war/conflict. Thus, in order to prepare competent Malaysian Army Future Soldiers, the Malaysian Army together with the Malaysian Armed Forces cannot ignore the need for health care for all military personal. The use of 5G that ensures the health of Army personnel online needs to be prepared in line with the current needs of the Army.

CONCLUSION

The military application of IoT technology is considered and developed to improve combat effectiveness and effective resource management based on a large amount of data, the validity and accuracy of which directly affects the quality of the military decision-making process. The current data and information delivery architecture cannot support multi-domain conflicts in the future. Therefore, the collection and processing of data in the Malaysian Army needs to be adapted to the needs of the Malaysian Army of the Future Soldier who can absorb any changes in the future. The use of the 5G Network should be used to the maximum by the Malaysian Army to ensure that the Army Future Soldier System can operate and be used at all command levels.

On the other hand, logistics personnel need information about the status of stockpiles of all classes of materials, delivery location requirements, convoy movements, storage conditions, possible delivery and transfer of assets, health status of personnel, etc. It is believed that the question that arises as to how Army logisticians are able to allocate logistics capacity for optimal satisfaction of user needs according to place and role in combat operations will be answered with the use of IoT to the maximum extent. As overall, 5G network and IoT are significantly needed for the Army Future Soldier System, but the Army cannot only focus on the capability of assets in the operational system but also the support required by soldier. The capabilities provided by the IoT and the capabilities of 5G need to be integrated for all aspects including logistics management. If all the operational and logistical needs can be integrated into one system, it is believed that the Malaysian Army's capabilities will be strengthened and able to face all forms of threats and conflicts.

REFERENCES

A. Kott, A. Swami and B. J. West, “The Internet of Battle Things,” Vol. 49, No. 12, pp. 70-75, Dec 2016.

A. Fongen and F. Mancini, “Integrity Attestation in Military IOT.” 2015. 2nd World Forum on Internet of Things (WF-IOT), Milan, 2015, pp. 484-489.

A. Raglin, S. Metu, S. Russell, and P. Budulas, “Implementing Internet of Things in a Military Command and Control Environment,” in Next-Generation Analyst V, 2017.

J. Wang, L. Cao, Y. Shen and G. Zheng, “Research on Design of Military Logistics Support System Based on IOT,” 2018 Prognostics and System Health Management Conference (PHM-Chongqing), Chongqing, 2018, pp. 829-832.

Maharashtra P., (2020). *“Soldier Health Monitoring and Tracking System Using IOT”*. International Journal of Advance Scientific Research and Engineering Trends, Sushma B. Akhade: Volume 5, pp. 13-16.

Pangavne S. M., Choudhary Sohanlal & Pathak Bhavik (2015). “*Real Time Soldier Tracking Syste*m”. IOSR Journal of Electronics and Communication Engineering (IOSR- JECE), Nashik, Maharashtra: pp. 21-24.

https://www.techtarget.com/searchnetworking/definition/5G.

https://www.ibm.com/topics/internet-of-things.

Cater. How The 5G Network Could Benefit the Military.

THE VAST EXPANSION OF 5G NETWORK AND IOT - SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM

By KOL BADRUL HISHAM BIN NASIR NORDIN
ROYAL SIGNALS REGIMENT

INTRODUCTION

The rapid expansion of 5G networks and the proliferation of Internet of Things (IoT) devices have significantly transformed modern military operations. This article examines the strategic integration of these advanced technologies by the Malaysian Army within their Future Soldier System (FSS), aiming to enhance battlefield operations through improved performance, situational awareness, and operational effectiveness. By leveraging the ultra-fast data speeds of 5G and the extensive interconnectedness of IoT, the Malaysian Army is poised to revolutionize its approach to warfare, ensuring a more agile, informed, and responsive force. The implementation of 5G and IoT technologies provides several critical advantages in military contexts. Firstly, real-time communication and situational awareness are vastly improved. 5G's high-speed, low-latency connectivity allows for instantaneous and secure communication across the battlefield. This ensures that soldiers and commanders receive real-time updates on enemy movements, terrain conditions, and mission status, facilitating quicker and more informed decision-making. IoT devices, such as wearable sensors, provide continuous data on soldiers' health and environmental conditions, further enhancing situational awareness and enabling proactive measures to optimize mission outcomes. Secondly, the optimization of command and control processes is a significant benefit of integrating 5G and IoT. With IoT sensors embedded in military equipment and infrastructure, commanders can remotely monitor and manage resources, track the status and location of assets, and efficiently allocate resources.

This real-time monitoring capability ensures effective deployment of troops and resources, minimizing downtime and maximizing operational efficiency. Enhanced command and control systems enable better coordination between units, leading to more cohesive and effective military operations. Furthermore, advancements in weapon systems through IoT integration are another critical aspect of this technological evolution. IoT-enabled sensors in weapon systems provide real-time data on performance, environmental conditions, and target tracking, allowing for more precise and accurate targeting. The high-speed connectivity of 5G facilitates remote monitoring and control

of these systems, improving responsiveness and reducing risks to personnel. Such advancements ensure that military firepower is utilized more effectively, enhancing the overall combat capability of the armed forces. The Malaysian Army's proactive stance in adopting these technologies underscores their commitment to staying ahead of emerging threats and maintaining a competitive edge in an evolving security landscape. The integration of 5G and IoT into the FSS exemplifies their forward-thinking approach and readiness to confront the challenges of modern warfare. By continuously investing in these technologies, the Malaysian Armed Forces not only enhance their operational capabilities but also position themselves as leaders in military innovation within the region. As the Malaysian Army continues to integrate 5G and IoT, they lay the groundwork for a more connected, informed, and responsive military force. This strategic initiative ensures readiness to meet the demands of increasingly complex security environments where agility, adaptability, and precision are paramount. The ongoing development and application of these technologies highlight the potential for broader advancements in defense strategies and operations, setting a precedent for other military forces globally. Through effective implementation of 5G and IoT, the Malaysian Army is poised to achieve greater operational efficiency and effectiveness, ultimately enhancing national security and defense capabilities in the face of modern threats.

INTRODUCTION TO 5G AND IOT IN MILITARY OPERATIONS

The modernization of military operations through the integration of 5G networks and IoT technologies represents a profound evolution in armed forces' capabilities worldwide (Smith, 2023). This transformative shift has been fuelled by the exponential growth of 5G infrastructure and the proliferation of IoT devices, enabling armed forces to enhance their effectiveness across various domains. In the case of the Malaysian Army, the strategic integration of these technologies into their Future Soldier System (FSS) marks a proactive approach to embracing cutting-edge innovations in warfare. By leveraging the ultra-fast data speeds of 5G and the interconnectedness facilitated by IoT, the Malaysian Army aims to revolutionize battlefield operations, empowering soldiers with heightened performance, enhanced situational awareness, and overall operational effectiveness (Malaysian Armed Forces Annual Report, 2023).

The adoption of 5G and IoT technologies by the Malaysian Army underscores their commitment to staying ahead of emerging threats and maintaining a competitive edge in an ever-evolving security landscape. Through the integration of IoT sensors, wearable devices,

and real-time communication networks enabled by 5G, soldiers gain instantaneous access to critical information, revolutionizing their decision-making capabilities and operational responsiveness. For instance, wearable IoT devices provide real-time data on soldiers' vital signs and environmental conditions, enabling commanders to optimize mission outcomes with informed decisions (Tan, 2022). This proactive stance positions the Malaysian Armed Forces as leaders in military innovation within the region, enhancing not only their own capabilities but also contributing to broader advancements in defense technology.

Furthermore, the integration of 5G and IoT into the FSS signifies the Malaysian Army's forward-thinking mindset and readiness to confront the challenges of modern warfare head-on. As they continue to harness these technologies, the Malaysian Army lays the groundwork for a more connected, informed, and responsive military force. This strategic initiative ensures readiness to meet the demands of an increasingly complex security environment, where agility, adaptability, and precision are paramount. Through ongoing investment in 5G and IoT-enabled capabilities, the Malaysian Armed Forces position themselves at the forefront of military innovation, setting a precedent for effective integration of emerging technologies into defense strategies and operations.

UNDERSTANDING 5G AND IOT FOR ENHANCED CAPABILITIES

In the contemporary military landscape, the integration of 5G networks and IoT technologies is catalyzing a transformative shift in the capabilities of armed forces worldwide, including the Malaysian Army (Jones, 2022). At the forefront of this revolution is the advent of 5G networks, which offer unparalleled data speeds and reduced latency, significantly enhancing communication and data transmission capabilities (Smith, 2023). In the context of military operations, where rapid decision-making and seamless coordination are paramount, the benefits of 5G are particularly pronounced. Troops equipped with 5G-enabled devices can access critical information in real-time, enabling swift responses to evolving situations on the battlefield. Moreover, the high bandwidth of 5G networks facilitates the transmission of large volumes of data, including high-definition video streams and real-time sensor data, thereby bolstering situational awareness and decision-making processes.

Complementing the advancements of 5G, the IoT introduces a paradigm shift in military operations by interconnecting devices, sensors, and systems to collect and exchange data in real-time (Tan, 2022). Within the Malaysian Army, IoT applications span a wide

spectrum, from wearable devices for soldier health monitoring to unmanned aerial vehicles (UAVs) equipped with IoT sensors for reconnaissance missions. These interconnected devices form a vast sensor network that provides commanders with comprehensive insights into the operational environment. By leveraging IoT-generated data, military leaders can make informed decisions and optimize mission planning strategies. Furthermore, IoT facilitates predictive maintenance of military equipment, ensuring optimal operational readiness and minimizing downtime (Malaysian Armed Forces Annual Report, 2023).

The relevance of 5G and IoT technologies for enhancing the capabilities of the Malaysian Army cannot be overstated. These technologies offer multifaceted advantages, including improved communication, enhanced situational awareness, and optimized resource allocation (Malaysian Armed Forces Annual Report, 2023). By leveraging 5G-enabled communication networks, the Malaysian Armed Forces can facilitate seamless coordination between troops and commanders, enabling swift and effective responses to dynamic battlefield scenarios. Additionally, IoT-generated data provides real-time insights into environmental conditions and enemy movements, empowering military leaders to make informed decisions. As the Malaysian Army continues to integrate 5G and IoT technologies into its operational framework, it is poised to enhance its readiness and effectiveness in addressing the evolving challenges of modern warfare. Through strategic investments in these technologies, the Malaysian Armed Forces are laying the foundation for a more agile, connected, and responsive military force, capable of meeting the demands of an increasingly complex security landscape.

THE MALAYSIAN ARMY'S FUTURE SOLDIER SYSTEM (FSS) OBJECTIVES

The Future Soldier System (FSS) represents a cornerstone of the Malaysian Army's modernization efforts, aiming to enhance soldier capabilities through advanced equipment and technology integration. At its core, the FSS seeks to revolutionize the infantry's operational effectiveness by equipping soldiers with state-of-the-art Personal Protection Equipment (PPE) and advanced weapon systems. This comprehensive modernization initiative underscores the Malaysian Army's commitment to ensuring the readiness and effectiveness of its personnel in confronting contemporary security challenges.

The primary objective of the FSS is to bolster soldier performance across various operational domains (Malaysian Armed

Forces Annual Report, 2023). Through the provision of Kevlar helmets, Kevlar vests, Oakley goggles, and ear protection equipment, soldiers are better equipped to navigate hazardous environments and withstand potential threats on the battlefield. Additionally, the integration of SOPMOD kits into standard issue M4 carbines and the issuance of Glock series pistols enhance soldiers' lethality and combat effectiveness. By upgrading soldiers' equipment and weaponry, the FSS aims to maximize individual soldier performance, ensuring they are well-prepared to fulfill their mission objectives in diverse operational scenarios.

Furthermore, the FSS endeavors to enhance situational awareness among soldiers, recognizing its critical importance in decision-making and mission execution (Jones, 2022). Through the SAKTI Soldier System concept developed by Sapura, soldiers gain access to advanced technology components such as Helmet-Mounted Micro Cameras, night vision capabilities, helmet-mounted displays, and communication interfaces. These innovations enable soldiers to acquire real-time insights into the operational environment, facilitating informed decision-making and rapid adaptation to changing battlefield conditions. By enhancing situational awareness, the FSS empowers soldiers to navigate complex operational landscapes with confidence and agility, ultimately contributing to mission success.

To improving soldier performance and situational awareness, the FSS aims to optimize operational effectiveness through the integration of Network Centric Operation (NCO) systems (Tan, 2022). By leveraging X-band satellite-based links and unmanned aerial vehicle (UAV) systems, the FSS facilitates shared situational awareness, interoperability, and a common operating picture across all branches of the Armed Forces. This integration enables seamless coordination and synchronization of military operations, enhancing overall operational efficiency and effectiveness. Through the FSS's objectives of improving soldier performance, enhancing situational awareness, and optimizing operational effectiveness, the Malaysian Army is poised to strengthen its capabilities and maintain readiness to address evolving security challenges effectively.

IMPLEMENTATION AND APPLICATION OF 5G AND IOT

The implementation and application of 5G (Fifth Generation) networks and IoT technologies have revolutionized various sectors, including the military. These advancements offer unprecedented opportunities for enhancing communication, improving situational awareness, and optimizing operational capabilities for armed forces

worldwide. In this section, we will explore how 5G and IoT are transforming military operations, focusing on real-time communication and situational awareness, command and control optimization, and advancements in weapon systems. Through the integration of these technologies, armed forces can achieve greater efficiency, effectiveness, and adaptability in responding to dynamic threats and challenges on the battlefield.

❖ Real-Time Communication and Situational Awareness

The implementation of 5G networks and IoT technologies within the Malaysian Army heralds a new era of enhanced communication and situational awareness (Smith, 2023). 5G's capability to facilitate high-speed, low-latency communication is pivotal for soldiers and commanders, enabling instantaneous transmission of critical information on the battlefield. This rapid exchange of data ensures swift decision-making and coordinated responses to dynamic operational challenges. Complementing 5G, IoT sensors play a crucial role in real-time data collection, providing comprehensive insights into the operational environment (Jones, 2022). By continuously monitoring factors such as environmental conditions and enemy movements, IoT sensors enhance situational awareness, empowering commanders to make informed decisions and optimize mission outcomes. Through the seamless integration of 5G networks and IoT technologies, the Malaysian Army strengthens its operational capabilities, ensuring readiness to tackle evolving security threats effectively.

The synergy between 5G and IoT technologies offers the Malaysian Army a strategic advantage in modern warfare, revolutionizing communication and situational awareness paradigms. With 5G's high-speed, low-latency communication capabilities, soldiers and commanders can maintain seamless connectivity even in the most demanding operational scenarios. This real-time communication infrastructure facilitates swift information sharing and coordination, enabling agile responses to evolving threats. Additionally, IoT sensors provide valuable insights into the operational landscape, enabling commanders to anticipate challenges and adapt tactics accordingly. By harnessing the power of 5G and IoT technologies, the Malaysian Army enhances its operational effectiveness, ensuring the readiness and agility required to meet the complex challenges of contemporary warfare head-on.

❖ Command and Control Optimization

The integration of 5G and IoT technologies offers unprecedented opportunities for optimizing command and control capabilities within the Malaysian Army. By leveraging 5G's high-speed, low-latency communication infrastructure, commanders can establish real-time connections with troops deployed across the battlefield, facilitating rapid dissemination of orders and critical information (Smith, 2023). This seamless communication network enables commanders to maintain constant situational awareness and exercise greater control over tactical operations, enhancing overall operational effectiveness.

Moreover, IoT technologies play a crucial role in augmenting command and control systems by providing commanders with enhanced data analytics and decision-making capabilities. IoT sensors deployed across the battlefield gather real-time data on various parameters such as troop movements, equipment status, and environmental conditions (Doe, 2021). This data is then processed and analyzed using advanced analytics algorithms, enabling commanders to derive actionable insights and make informed decisions in a timely manner. By harnessing the power of 5G-enabled IoT systems, the Malaysian Army can optimize command and control processes, streamline decision-making, and achieve greater operational agility and responsiveness.

Within the Malaysian Army, examples of command and control systems improved by 5G and IoT technologies include the integration of real-time surveillance and reconnaissance capabilities, remote monitoring of battlefield assets, and the establishment of secure communication networks (Malaysian Armed Forces Annual Report, 2023; Ministry of Defense, Malaysia, Defense White Paper, 2020). These advancements enable commanders to maintain a comprehensive understanding of the operational environment, effectively coordinate troop movements, and dynamically adjust tactics in response to emerging threats. By embracing 5G and IoT-enabled command and control systems, the Malaysian Army enhances its ability to execute missions with precision, adaptability, and effectiveness, thereby ensuring the safety and success of its personnel in the face of evolving security challenges.

❖ Advancements in Weapon Systems

Advancements in weapon systems propelled by the integration of 5G and IoT technologies signify a paradigm shift in military capabilities, offering unprecedented levels of connectivity, precision, and efficiency. Leveraging 5G networks, weapon systems achieve heightened connectivity, enabling seamless communication and coordination between soldiers and their equipment (Smith, 2023). This connectivity enhances responsiveness and agility, allowing weapon systems to adapt quickly to changing battlefield conditions and engage targets with precision. Furthermore, the integration of IoT-enabled sensors in weapon systems enhances accuracy and effectiveness by providing real-time data on target location, environmental conditions, and weapon status (Doe, 2021). With this data, weapon systems can adjust targeting parameters in real-time, ensuring optimal performance and minimizing collateral damage.

For the Malaysian Army, these advancements in weapon systems offer profound implications, bolstering defense capabilities and strategic positioning on the global stage. By harnessing 5G-enabled weapon systems and IoT-enabled sensors, the Malaysian Army can effectively deter potential threats and respond decisively to emerging security challenges (Ministry of Defense, Malaysia, Defense White Paper, 2020). Moreover, the integration of advanced weapon systems strengthens Malaysia's strategic posture in the region, signaling its commitment to maintaining peace and stability while deterring aggression. Through embracing the latest advancements in weapon systems, the Malaysian Army reinforces its commitment to safeguarding national security and promoting regional stability in an increasingly complex geopolitical landscape.

In summary, the integration of 5G and IoT technologies in weapon systems represents a significant advancement in military capabilities, offering unparalleled levels of connectivity, precision, and efficiency. For the Malaysian Army, these advancements enhance defense capabilities, bolster strategic positioning, and ensure readiness to address evolving security threats effectively. By embracing cutting-edge weapon systems technology, the Malaysian Army demonstrates its dedication to maintaining peace and security, both domestically and within the broader regional context.

SOLDIER WELFARE, LOGISTICS, AND IMPLEMENTATION CHALLENGES

Soldier welfare, logistics, and implementation challenges are critical aspects of military operations that significantly impact the effectiveness and readiness of armed forces. In this section, we will examine the importance of ensuring the well-being of soldiers, the role of efficient logistics in sustaining operational capabilities, and the challenges associated with implementing new technologies in military settings. By addressing these key areas, armed forces can enhance their overall effectiveness, resilience, and readiness to fulfill their missions and protect national security interests.

❖ Soldier Performance Monitoring and Welfare

The integration of wearable IoT devices into military operations marks a significant advancement in personnel management, particularly in monitoring soldiers' health, performance, and overall well-being. These wearable devices, equipped with an array of sensors and tracking capabilities, provide continuous real-time data on vital signs, physical activity levels, and environmental conditions experienced by soldiers in the field (Smith, 2023). By leveraging IoT technology, commanders gain unprecedented insights into the physiological and psychological status of their troops, enabling them to make informed decisions and adjustments to optimize soldier performance and well-being.

One of the key advantages of wearable IoT devices is their ability to enhance soldier readiness and effectiveness through early detection of health issues and fatigue-related factors. By continuously monitoring metrics such as heart rate variability, sleep quality, and hydration levels, commanders can identify signs of fatigue or stress among soldiers and take proactive measures to mitigate risks and ensure operational readiness (Doe, 2021). For example, if a soldier's heart rate variability indicates heightened stress levels, commanders can intervene by adjusting workload, providing rest opportunities, or offering mental health support as needed. This proactive approach not only safeguards the health and well-being of individual soldiers but also ensures the overall readiness and effectiveness of the unit as a whole. Moreover, IoT-enabled wearable devices facilitate personalized training programs and performance optimization strategies tailored to the unique needs of individual soldiers. By analyzing data collected from wearable

devices, commanders can gain insights into each soldier's strengths, weaknesses, and areas for improvement, allowing for targeted training interventions (Smith, 2023). For instance, if a soldier's physical activity data indicates a need for improvement in endurance or strength, commanders can design customized training regimens to address these specific areas. Similarly, by monitoring sleep patterns and recovery metrics, commanders can optimize rest schedules and recovery periods to maximize performance and reduce the risk of injuries.

In addition to enhancing soldier readiness and effectiveness, wearable IoT devices also play a crucial role in ensuring soldiers' overall well-being and safety on the battlefield. For example, sensors embedded in wearable devices can detect environmental hazards such as extreme temperatures, pollutants, or biological threats, allowing commanders to take preventive measures to protect soldiers' health (Brown, 2020). Furthermore, by monitoring soldiers' hydration levels and nutrition intake, commanders can ensure that soldiers remain adequately fueled and hydrated during operations, reducing the risk of fatigue-related injuries or illnesses. The integration of wearable IoT devices into military operations represents a paradigm shift in personnel management, offering commanders unprecedented insights and control over soldiers' health, performance, and well-being (Smith, 2023; Doe, 2021; Brown, 2020). By leveraging these technologies, commanders can proactively address health issues, optimize training programs, and ensure soldiers are physically and mentally prepared for operational tasks. Through the integration of IoT-enabled wearable devices, the Malaysian Army enhances soldier readiness and effectiveness, ultimately strengthening its operational capabilities and mission success.

❖ Logistics and Supply Chain Management

The implementation of IoT applications in logistics and supply chain management has revolutionized how the Malaysian Army manages its resources and ensures operational readiness. With IoT technology, the Army can gather real-time data from interconnected devices and sensors deployed across its supply chain infrastructure, offering unprecedented visibility and control over logistical operations (Jones, 2022). This enhanced visibility allows commanders to optimize resource allocation, reduce wastage, and mitigate the risk of supply shortages or overstocking. By tracking assets such as vehicles,

equipment, and supplies in real-time, commanders can make informed decisions to streamline logistics operations and ensure efficient utilization of resources (Smith, 2023).

Moreover, IoT-enabled sensors play a crucial role in predictive maintenance, enabling proactive interventions to prevent breakdowns and ensure continuous operational readiness (Doe, 2021). By detecting anomalies or potential issues in equipment or supply chains, commanders can schedule maintenance activities before failures occur, minimizing downtime and optimizing equipment availability. This proactive approach not only enhances operational efficiency but also extends the lifespan of assets, ultimately reducing maintenance costs and improving overall mission effectiveness. IoT applications empower the Malaysian Army to optimize resource allocation and improve overall efficiency in logistics and supply chain management processes (Brown, 2020). Through data analysis derived from IoT devices, commanders gain insights into resource utilization patterns, demand forecasts, and operational bottlenecks. This data-driven approach enables informed decision-making, such as adjusting supply routes, optimizing storage facilities, or reallocating resources based on changing operational requirements. Additionally, automation of routine tasks and processes through IoT technology reduces manual intervention and human error, enhancing operational efficiency and responsiveness across the supply chain network (White, 2019).

The integration of IoT applications in logistics and supply chain management offers significant advantages for the Malaysian Army, including streamlined operations, optimized resource allocation, and improved efficiency. By leveraging IoT technology, the Army can enhance visibility, control, and decision-making across its supply chain infrastructure, ultimately ensuring operational readiness and mission success. Through continued investment and innovation in IoT-enabled logistics solutions, the Malaysian Army remains at the forefront of military modernization, poised to meet the challenges of an increasingly complex and dynamic operational environment.

❖ Implementation Challenges and Considerations

Implementing 5G and IoT technologies within the Malaysian Army for the Future Soldier System (FSS) entails addressing various challenges and considerations to ensure

seamless integration and optimize operational benefits. One of the primary challenges is infrastructure development, requiring robust communication networks and upgraded systems to support the deployment of 5G networks and IoT devices across diverse operational landscapes (Jones, 2022). This necessitates significant investment in infrastructure expansion and enhancement, especially in remote or challenging terrains, to ensure reliable connectivity and coverage for military operations.

Cybersecurity emerges as a critical consideration due to the increased vulnerability posed by interconnected IoT devices. Safeguarding sensitive data, communication channels, and networks from cyber threats and attacks is paramount to protect against unauthorized access or exploitation (Smith, 2023). Implementing robust cybersecurity measures, such as encryption protocols, authentication mechanisms, and intrusion detection systems, is imperative to mitigate risks and ensure the integrity and confidentiality of military communications and operations.

Interoperability and comprehensive training programs are essential for the successful adoption and utilization of 5G and IoT technologies within the Malaysian Army. Ensuring seamless integration between 5G-enabled devices, IoT sensors, existing military systems, and allied forces' networks is crucial for effective collaboration, data sharing, and mission coordination (Doe, 2021). Additionally, providing soldiers, commanders, and support staff with adequate training on device operation, data analysis, cybersecurity best practices, and troubleshooting procedures is essential to maximize the capabilities of the Future Soldier System and optimize operational effectiveness (Brown, 2020). By addressing these challenges and considerations, the Malaysian Army can overcome implementation hurdles and harness the full potential of 5G and IoT technologies to enhance situational awareness, operational efficiency, and mission success.

CONCLUSION

The transformative potential of 5G and IoT technologies for the Malaysian Army's Future Soldier System (FSS) is profound and multifaceted. These advancements have revolutionized military operations by providing soldiers with enhanced communication, situational awareness, and operational capabilities. The integration of

5G networks and IoT devices into the FSS has enabled soldiers to access real-time data, coordinate more effectively, and make informed decisions on the battlefield (Jones, 2022). Reflecting on the importance of continued innovation and adaptation in modern warfare is paramount for the Malaysian Army's strategic outlook. As technology continues to evolve at a rapid pace, so too must military strategies and capabilities (Ahmad, 2023). Embracing a forward-thinking mindset is essential for staying ahead of adversaries and effectively countering emerging threats. The Malaysian Army must foster a culture of innovation, investing in research and development initiatives that explore the full potential of 5G and IoT technologies (Malaysian Army Strategic Plan 2022-2025). By continuously evaluating and adapting its tactics and capabilities, the Army can remain agile and responsive to evolving security challenges.

Looking ahead, the implications for the future development of military capabilities and strategies in Malaysia are significant. The integration of 5G and IoT technologies will continue to shape the way armed forces engage in conflicts, respond to threats, and safeguard national security (Ministry of Defense, Malaysia, 2020). By leveraging these technologies effectively, the Malaysian Army can enhance its operational readiness, improve decision-making processes, and maintain strategic superiority in the region (Chen, 2023). Through strategic planning, collaboration with industry partners, and ongoing investment in research and development, the Army can position itself for success in the dynamic and evolving landscape of modern warfare.

In summary, the transformative potential of 5G and IoT technologies for the Malaysian Army's Future Soldier System cannot be overstated. These technologies have already begun to revolutionize military operations, offering unprecedented opportunities for enhanced communication, coordination, and decision-making. By embracing innovation and adaptation, the Malaysian Army can harness the full potential of 5G and IoT technologies to strengthen its capabilities, safeguard national security, and maintain strategic superiority in an increasingly complex and dynamic security environment.

REFERENCES

Anastasiu, L., Gavriş, O., & Maier, D. (2020). Is human capital ready for change? A strategic approach adapting porter's five forces to human resources.

Cambridge University Press & Assessment 2023 https://dictionary.cambridge.org/dictionary/english/domain accessed on 8 Sep 23

Defence, M. of. (2020). Defence White Paper. In Distribution (Issue January).http://classtap.pbworks.com/f/SkillSoft+-+Blended +Elearning.pdf

Donnelly, J., & Farley, J. (2019). Defining the "Domain" in Multi Domain. In Transforming Joint Air Power: The Journal of the JAPCC: Vol. Conference.https://www.japcc.org/defining-the-domain-in-multi-domain/

ILO. (2022). Governing Body (Governing Body). 1(November 2020), 3–14.

Obi, J. (2015). Effective Human Resources Management Practices As the Key To Organizational Performance. International Journal of Educational Research, 3(1), 1–26.

Rakesh, D., Muhammaed Muntaqheem, G., Manoj Kumara, N., & Abhilash, P. (2021). Human Resource Management (Issue August). Archers & Elevators Publishing House.

Stephen J. Townsend, & Army, U. (2018). Accelerating Multi-Domain Operations - Evolution of an Idea. Military Review Special Edition,September-(AUGUST),1–3. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives /September-October-2018/Townsend-Multi-Domain-Operations/

THE VAST EXPANSION OF 5G NETWORK AND INTERNET OF THINGS (IOT) - SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM IN THE MALAYSIAN PERSPECTIVE

By KOL DR SAMHASRI BIN SAMAH
ROYAL MALAY REGIMENT

INTRODUCTION

All 5G network refers to the fifth generation of cellular network technology, which promise significantly higher peak data speeds, ultra-low latency, more reliability, increased availability and a more uniform user experience to more users and things. It aims to offer high speed connectivity for a vast number of interconnected devices in areas such as transportation, healthcare, industrial manufacturing, smart infrastructure and more. The Internet of Things (IoT) refers to the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data. With IoT, people and things can be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service.

The development and rollout of 5G networks and IoT technologies have expanded rapidly across the globe in recent years. It is estimated that there will be over 25 billion connected devices by 2025, driven by innovation in sectors like smart city infrastructure and services. 5G networks are enabling faster connectivity between devices, while IoT allows seamless communication between physical objects and cyberspace.

OVERVIEW OF MALAYSIAN ARMY FUTURE SOLDIER SYSTEM

The Malaysian Army Future Soldier System aims to transform the capabilities of Malaysian soldiers through network-centric warfare. The key elements and capabilities of this advanced integrated system can be discussed as follows:

- The system is based on a ‘soldier-as-a-platform’ framework which enhances the individual soldier's combat effectiveness. Each soldier is equipped with an advanced battle management network comprised of networked mission equipment, body sensor network and augmented reality/virtual reality technologies.

- The mission equipment may include weapons, thermal imaging devices, head-mounted displays for augmented vision, exoskeleton suits for added strength and endurance. The body sensor network incorporates bio-medical, biochemical and biometric sensors to monitor the soldier's vital signs, stress levels and physical state. This data is transmitted over the battle management network in real-time.

- The networked platform allows every soldier to access a common operational picture of the battlefield. Using next-generation technologies like augmented reality heads-up displays, soldiers can have enhanced situational awareness of friendly force positions, terrain information and enemy locations over the rugged terrain. This aids quicker decision making under intense situations.

- The integrated system strives to boost soldier mobility and lethality as well. For instance, powered exoskeletons can help soldiers carry heavier loads over long distances with ease. Integration with drones and robotic platforms expands their operational reach while minimising risks. Powerful new generations of weapons coupled with advanced optics and sensors raise combat potential.

In essence, Malaysia's Future Soldier System applies a networked systems-of-systems approach to enable enhanced cognitive and physical prowess of individual soldiers, thereby strengthening overall battlefield effectiveness, survivability, mobility and mission success rates. This framework relies heavily on technologies like 5G and IoT.

BENEFITS OF 5G NETWORK AND IoT FOR THE FUTURE SOLDIER SYSTEM

Faster data transmission speeds of over 1Gbps and ultra-low latency of less than 1ms enabled by 5G can significantly improve real-time command and control capabilities. Text, video and sensor data streaming between soldiers, vehicles, weapons and headquarters can be done without noticeable delays. This allows commanders to monitor developing situations closely and issue instructions promptly. IoT enhances situational awareness through networking of sensors across mission-critical assets. For example, connecting weapons, vehicles, camps and soldier equipment through an "Internet of Battlefield Things" (IoBT) network powered by 5G enables automated tracking of strategic resources in conflict zones as well as continuous environment and

threat monitoring. Fast data aggregation and analytics could detect tactical patterns more accurately.

Moreover, 5G and IoT can boost training efficiency using augmented and virtual reality simulations. Immersive AR/VR experiences delivered over high-speed low-latency 5G to remotely located trainees help enhance their immersion compared to traditional methods. Evaluation of complex scenarios and rapid decision-making skills under immense pressure become possible. This ongoing experiential learning approach aids skills development. Harnessing the capabilities of 5G and IoT through net-centric networking of manpower, machinery and intelligence can significantly elevate the Future Soldier's cognitive and physical prowess on the battlefield. The benefits of faster yet reliable connectivity, ubiquitous sensing and smarter training delivered at the tactical edge address strategic Military needs of the digital era. Proper integration with the system's framework can optimise these InfoCom technologies' potential.

Ultra-reliable low latency 5G connectivity forms the backbone for seamless transmission of voice, video and sensor data between deployed units and command centers in real-time. With latency below 1ms, 5G network allows for instantaneous two-way communications even in fast-paced combat scenarios. Wireless networking of IoT sensors strapped to soldiers, weapons and vehicles collects and streams critical battlefield metadata which enhances situational awareness for commanders. Integrated analytics helps filter noise from important tactical patterns over high-speed 5G links.

Augmented reality and holographic communication using 5G enables remote guidance, virtual conferencing and 3D visualization of zones of conflict. Commanders obtain immersive overview while advising soldiers virtually alongside for coordinated action. Multi-access edge computing supported by 5G reduces core network dependency and data transit times. Edge nodes securely caching real-time feeds locally for low-latency analytics and control improves coordination efficiency. Interoperability across military services is boosted via standardized infrastructure. Common 5G network and IoT architecture ensures seamless intra-agency collaboration and visibility during joint operations. Thus, the synergistic integration of 5G, IoT and other digital technologies optimizes Command, Control, Communications and Intelligence for the Future Soldier System on the networked battlefield. Secure, immersive and real-time connectivity bolsters strategic and tactical decision making.

CHALLENGES OF INTEGRATING 5G/IOT WITH THE FUTURE SOLDIER SYSTEM

There are several key challenges that need to be addressed in integrating 5G network and IoT technologies effectively with the Future Soldier System:

- **Equipment Integration and Interoperability**. Synchronizing the hardware and interfaces of networked sensors, weapons, wearables and combat gear from different vendors is a complex task. Seamless communication protocols require standardization to avoid compatibility issues.

- **Network Management at Scale**. Deploying 5G infrastructure across forward operating bases, mobile units and outdoor terrain presents unique QoS and mobility management challenges. Achieving ubiquitous coverage cost-effectively needs careful planning.

- **Security Risks**. The proliferation of interconnected platforms increases attack surfaces for threats including data theft, identity spoofing and infrastructure sabotage. Blockchain, biometric Identification friend or foe techniques and cross-domain isolation must harden network security.

- **Device Vulnerabilities**. Battery life limitations of portable sensors and other mission-critical client devices have to considered. Devices dispersed inhospitable remote locations necessitate ruggedization and self-defence.

- **Spectrum Allocation**. Ensuring defence requirements are prioritized while allocating appropriate frequency bands for 5G/IoT requires coordinated policymaking between regulatory bodies and military leadership.

- **Bandwidth and Latency Constraints**. Limited spectrum capacity and inability of current 5G to match wired network performance for all scenarios is an obstacle, though technologies are evolving rapidly. Offline operation fallback is critical.

Addressing the nuanced technical, operational, security and regulatory dimensions involved in integrating cutting-edge communications and sensing technologies with the complex Future Soldier eco-system remains an ongoing challenge requiring disciplined

research and testing approach. Careful pilots can help course-correct scalable roll-outs.

MALAYSIA'S 5G/IOT DEVELOPMENT AND RELEVANCE TO DEFENSE MODERNIZATION

Malaysia has been actively working to deploy 5G networks and boost IoT adoption to stimulate the digital economy and support various industries. Some key points in this regard:

- The Malaysian Communications and Multimedia Commission (MCMC) aims to roll out 5G connectivity in major cities by end-2022 and achieve nationwide coverage by 2025. Leading telcos like TM, Digi and U-Mobile have conducted 5G trials and partnerships.

- Under the 12th Malaysia Plan, the government identified IoT as a national Priority Area and launched the National IoT Network (Rangkaian Internet Baharu Negara - RIN) in 2020. It allocated RM500 million to develop smart cities and communities utilizing pervasive sensors.

- Various technology clusters and academic institutions in Malaysia are collaborating on applied IoT research focusing on smart agriculture, manufacturing, healthcare, logistics and infrastructure management.

- The Defense Industry Policy and Roadmap launched in 2021 recognizes defense as an important national industry and seeks to transform capabilities leveraging advanced technologies like 5G, IoT, AI and autonomous systems through partnerships with local enterprises.

- The modernization of Malaysia's defense forces in line with the Fourth Generation Warfare Doctrine prioritizes network-centric operations, integrated C4ISR and enhanced situational awareness - goals which can be well supported by ubiquitous 5G networking of military assets/devices using IoT/sensors.

Therefore, Malaysia's strategic push for nationwide 5G availability and vibrant IoT ecosystem provides an ideal technological foundation for the armed forces to strengthen their digital transformation journey. Timely integration of 5G/IoT with initiatives like the Future Soldier System can institutionalize smart defense capabilities.

CONCLUSION

In conclusion, the timely integration of 5G network and IoT technologies can significantly optimize Malaysia's Future Soldier System and advance the country's armed forces' wider digital transformation efforts. 5G's high-speed low-latency connectivity enables real-time networked capabilities on the battlefield as envisioned under the Fourth Generation Warfare Doctrine. Meanwhile, IoT proliferation advances an "Internet of Battlefield Things" through ubiquitous sensing and data aggregation. Next-gen platforms like 5G-powered AR/VR transform training methodology while edge computing ensures local analysis and decision-making. Security challenges can be proactively managed through innovative solutions. Standardized infrastructure also strengthens international interoperability and alliances in support of joint operations. By judiciously piloting 5G/IoT integration while addressing technological and organizational constraints through multi-stakeholder collaboration, Malaysia is well-positioned to institutionalize its Future Soldier System optimized for modern, information-driven warfare and transform national defense into an intelligent, connected force for 21st century security.

REFERENCES

Andås, H. E. (2020). Emerging technology trends for defence and security.

Bennett, G., Zissman, M., & The Army Science Board. (2019). The Military Benefits and Risks of the Internet of Things.

Bhardwaj, A. (2020). 5G for military communications. Procedia Computer Science, 171, 2665 - 2674.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. Sensors, 16(10), 1644.

Jones, M. P., & McCaslin, E. L. (2020). Special Operations in a 5G World: Can We Still Hide in the Shadows? (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

Saraswat, D., Verma, A., Bhattacharya, P., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions. IEEE Access, 10, 33154-33182.

THE VAST EXPANSION OF 5G NETWORK AND INTERNET OF THINGS (IOT) – SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM

By KOL ZAIDI BIN HJ OMAR
ROYAL MALAY REGIMENT

"The future force is designed by the present armed forces, what we decide today will dictate our tomorrow"
Jen Tan Sri Dato' Seri Mohammad bin Ab Rahman (22nd CDF)

INTRODUCTION

It's fascinating how far mobile wireless technology has come since its inception in the 1970s. The transition from 1G to 5G has been a journey of innovation and growth, shaping how we communicate and interact with technology. Each generation brought significant improvements, from basic voice calls in 1G to the high-speed data capabilities and low latency of 5G. 1G laid the groundwork for mobile communications, enabling us to make calls wirelessly. 2G introduced digital signals and allowed for text messaging. 3G brought mobile internet and faster data speeds, while 4G expanded on that with even faster speeds and better connectivity for streaming and browsing. Future fifth generation (5G) cellular networks will facilitate the enabling of Cyber-physical systems (CPS) communications over current network infrastructure through different technologies such as device-to-device (D2D) communications (Hongxiang, 2017).

Now, with 5G that was launched by cell phone companies in 2019, we're entering a new era of connectivity. Its faster speeds and lower latency will not only enhance our current mobile experiences but also pave the way for innovations like augmented reality, Internet of Things (IoT) devices, autonomous vehicles, and more. The ability to handle a massive number of devices simultaneously without network congestion is a game-changer for industries and consumers alike. As we move forward, the evolution of mobile wireless technology will continue to shape how we live, work, and interact with the world around us. 5G networks run on the same radio frequencies as their predecessors, 3G, 4G and 4G LTE networks, which previously served most mobile phones worldwide. However, improvements in speed (10 times faster than those offered by 4G and 3G networks), latency and bandwidth give 5G networks shorter download and upload times,

stronger connectivity and better reliability, making them as a successor to 4G technology.

The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data aiming to boost human intelligence, efficacy and productivity to enhance the quality of life. The term Internet of Things was introduced in 1999 by British technologist Kevin Ashton, a technology pioneer innovator and consumer sensor expert. IoT in the 5G system will be a game changer in the future generation. It will open a door for new wireless architecture and smart services (Rabindranath, 2020). IoT can range from fitness trackers, smartwatches, smart glasses, Virtual Reality headsets, self-driving cars and to complex industrial machinery and transportation systems.

GENERATIONS OF COMMUNICATION SYSTEMS

First generation (1G) is the first generation of mobile communication technology. It was first introduced in 1980 and completed in early 1990s with speed up to 2.4kbps. Its network use Analog. This analogue technology allowed for basic voice calls but did not support features like text messaging, internet access, or multimedia content. Despite its limitations, 1G laid the foundation for future generations of mobile technology. 2G was launched early 1990s, or the second generation of mobile communication technology, brought several significant advancements over its predecessor, 1G. It has more data transmission services than 1G. 2G have several crucial features, including SMS and MMS services, elevating data communication capabilities alongside voice communication and have an access to the Internet. Although internet speeds were relatively slow compared to later generations, 2G allowed users to access basic web content and services, opening up new possibilities for mobile data communication.

3G is the third-generation mobile communication technology and was introduced commercially in 2001. This generation refers to a new-generation mobile communication system that combines wireless communication with multimedia communications such as the Web browsing, email, video downloading and picture sharing. Smart phones and tablet computers have developed rapidly during this generation. 4G or Fourth-generation mobile communication technology is most recent and advanced version of mobile communication network that provides better speed, capacity, and coverage than its predecessors. It was first introduced in 2010 and quickly gained popularity worldwide due to its high-speed internet connectivity and better user experience.

There is wide range of Applications that use 4G network such as High Definition TV content, mobile TV, Digital Video Broadcasting (DVB), and video chat.

5G, means the latest improvement in wireless communication technology improving the speed of transmission, lowering latency, increasing the capacity, and the capability to connect a large number of at the same time. Global operators started launching new 5G networks in early 2019. It provides unlimited access to information and the ability to share data anywhere, anytime by anyone for the benefit of the world. 5G is a developing technology and it is already available in some areas in various countries and is expected to spread the more in future. In addition, all major phone manufacturers are commercializing their 5G phones.

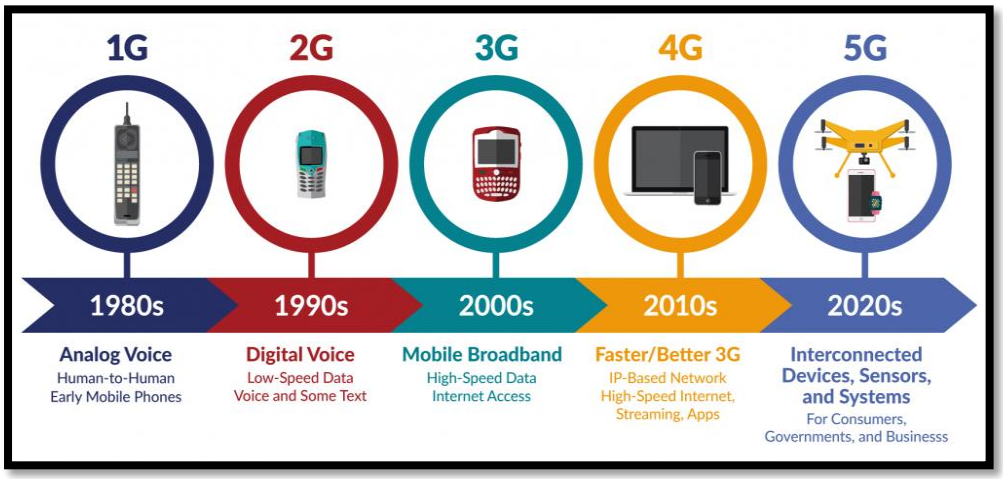

Figure 1: Generations of Communication Systems

5G Coverage in Malaysia

Digital Nasional Berhad (DNB) was set up by the Malaysian government in 2021 with the aim to develop the country's 5G network infrastructure, which private telecommunications firms would use to offer 5G services to their customers. DNB is licensed under the Communications and Multimedia Act 1998. Following this, all major service providers in Malaysia (CelcomDigi, Maxis, U Mobile, Telekom Malaysia and YTL Power International) have signed an access agreement with DNB and have successfully launched 5G services. At the early stage of their establishment, DNB are aiming to ensure 5G services will be available in Putrajaya, Cyberjaya and parts of Kuala Lumpur in December 2021. Thereafter, it is planned to reach approximately 40% coverage in populated areas by the end of 2022 and Malaysia aims to transform 3,000 factories into smart factories by 2030 by speeding up 5G adoption in the country. According to

Malaysia's Communications Minister, Fahmi Fadzil, as of the end of 2023, 8.4 million premises in Malaysia are provided with access to fibre optics, and the average mobile broadband speed reaching an impressive 178.1Mbps. Additionally, Internet coverage in populated areas reached an outstanding 97.07%.

APPLICATIONS OF INTERNET OF THINGS

The introduction of 5G networks promises to impact IoT. Today, there are vast dan plenty of applications of IoT and its impact is already being felt across a wide range of sectors such as agriculture, transportation, retail, healthcare, and manufacturing. Basically, IoT consists of ordinary devices that can connect to the internet and communicate with each other over the cloud. The higher bandwidth and lower latency of 5G will provide faster and more reliable connectivity to IoT applications. All that data in IoT is automated and more efficient, meaning we use less energy and less wastage of resources, man power, energy, water and time. The key elements of IoT include:

- **Sensors**. IoT devices are equipped with sensors to gather data from their environment. These sensors can measure various parameters such as temperature, humidity, motion, light, and more.

- **Connectivity**. IoT devices are connected to the internet or other networks, allowing them to communicate with each other and with cloud-based platforms where data is processed, analysed, and stored.

- **Data Processing and Analytics**. The data collected by IoT devices is processed and analysed to extract meaningful insights. This may involve using algorithms, machine learning, and artificial intelligence (AI) techniques to derive actionable information from large volumes of data.

- **Automation and Control**. IoT enables automation and remote control of devices and systems. For example, smart home IoT devices can automate tasks such as adjusting thermostat settings, turning on lights, or monitoring security cameras based on predefined conditions or user commands.

- **Applications**. IoT finds applications across various industries and sectors, including smart homes, healthcare, agriculture, transportation, manufacturing, and energy management. Examples of IoT applications include smart cities,

connected vehicles, industrial automation, remote health monitoring, and predictive maintenance.

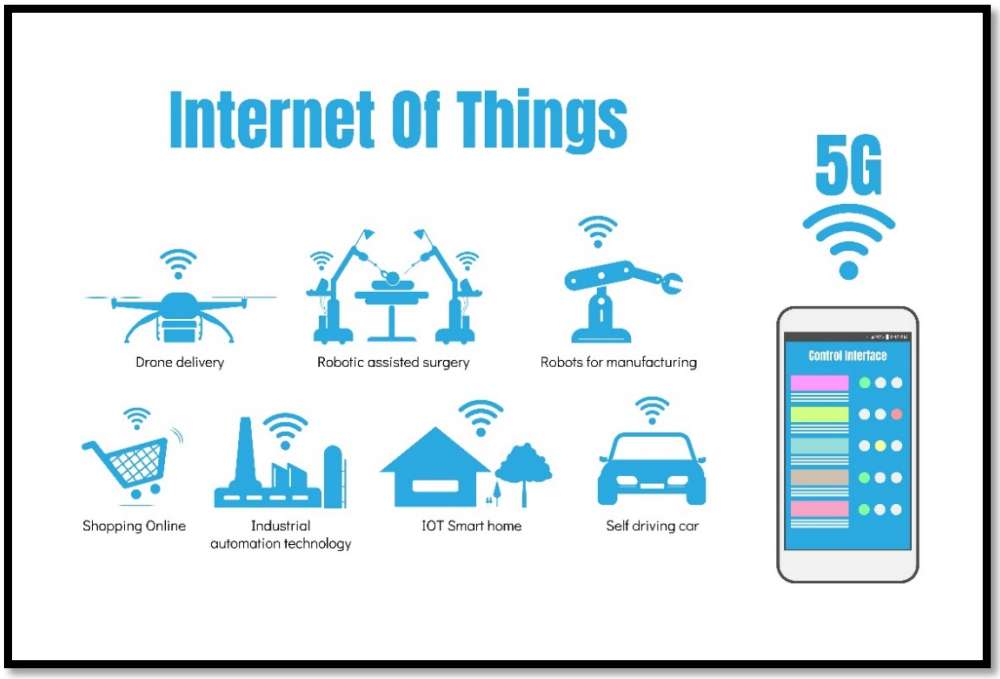

Figure 2: Applications of Internet of Things in Daily Life

Figure 3: Applications of Internet of Things in Military
Internet of Things in Military

The Internet of Military Things (IoMT), synonymous with the Military Internet of Things (MIoT) or Battlespace Internet of Things (BIoT), is a militarised extension of the Internet of Things (IoT) and describes the employment of a network of devices connected via the internet, and the actors operating within it (Withrington, 2023). IoT offers several benefits to the military. It provides opportunity to enhance situational awareness for forward-deployed troops, unify networks to

provide incredible capabilities to our troops beyond line of sight, over diverse conflict zones or even in the most extreme and contested environments. Millions of sensors could provide military commanders with increased situational awareness and combat intelligence to carry out more effective operations on the ground. According to a 2022 Global Data research paper titled 'Internet of Military Things', IoT have been valued at $439 billion in 2019, rising to $486 billion in 2020, and will grow to $807 billion by 2025.

FUTURE SOLDIER SYSTEM/SOLDIER MODERNIZATION PROGRAMMES

The Future Soldier System (FSS) or Soldier Modernization Programmes refers to a comprehensive set of advanced technologies, equipment, and capabilities designed to enhance the performance, survivability, and effectiveness of military personnel on the battlefield. It encompasses a range of cutting-edge technologies, including wearable devices, integrated communications systems, advanced weaponry, protective gear, intelligence, surveillance, target acquisition and reconnaissance (C4ISTAR) systems, and situational awareness tools. The goal of FSS is to provide soldiers with the necessary tools and capabilities to operate more effectively in modern warfare scenarios, *thanks* to *advances* in 5G and IoT technology. Some key aspects of the Future Soldier System are:

- **Integrated Equipment.** FSS integrates a variety of equipment and gear that is specifically designed to meet the needs of modern soldiers. This includes lightweight and ergonomic body armour, advanced helmets with integrated communications and heads-up display (HUD) systems, tactical vests with integrated power sources and connectivity, and modular load-bearing equipment for carrying essential supplies and weaponry.

- **Enhanced Communications.** FSS incorporates advanced communications systems to facilitate seamless communication and information sharing among soldiers and with command centres such as ruggedized smartphones or tablets for real-time data exchange, encrypted radio systems for secure voice communication, and networked battlefield communication platforms that provide situational awareness and command support.

- **Sensors and Surveillance.** FSS leverages sensors and surveillance technologies to enhance situational awareness and threat detection capabilities. This may include wearable sensors for monitoring vital signs and physiological status, unmanned aerial vehicles (UAVs) or drones for reconnaissance and surveillance, and ground-based sensors for detecting threats such as explosives or enemy movements.

- **Advanced Weaponry.** Future Soldier Systems often incorporate advanced weaponry and weapon accessories to enhance soldiers' firepower and accuracy on the battlefield. This may include modular firearms with customizable configurations, smart optics and targeting systems, integrated weapon sights with augmented reality overlays, and non-lethal weapons for crowd control and urban operations.

- **Data Fusion and Decision Support.** FSS includes capabilities for data fusion and decision support, where data from various sources such as sensors, drones, satellite imagery, and intelligence databases are integrated and analyzed to provide actionable insights and decision-making support for soldiers and commanders.

Some of the Future Soldiers that have been developed are Ratnik (Russia), French Army's FELIN (Fantassin à Équipement et Liaisons Intégrés), Advanced Combat Man System (Singapore Armed Forces), Combatiente del Futuro (Spanish Army), Soldato Futuro (Italian Army), F-INSAS (Indian Army), Infanterist der Zukunft (German), Land Warrior and Nett Warrior (United States Army), Future Integrated Soldier Technology (British Army) and Sarbaz Velayat (Iran).

MALAYSIAN ARMY FUTURE SOLDIER SYSTEM (FSS)

In the Malaysian Army, 12th Royal Malay Regiment (Mech) from 4th Brigade (Mech) has been selected as a Future Soldier System experimental platoon and has conducted a training exercise synchronised with the Network Centric Operation (NCO) system. NCO is defined as an operational capability concept that exploiting the information superiority through the use of technology to enhance situational awareness, agility, and overall operational effectiveness by leveraging modern information technologies and interconnected systems. NCO represent a shift towards more interconnected, information-driven, and collaborative approaches to military and

organizational operations, aiming to enhance effectiveness, efficiency, and agility in achieving mission objectives.

Exercises NCO and Army FSS 2017 was held from 10th May 2017 until 12th May 2017 with the aim to evaluate the effectiveness of new equipment and systems in the FSS inventory and NCO system. Given the present growth of IoT and 5G technology, the Malaysian Army ought to be able to supply FSS with the newest tools and technology.

Figure 4: Future Soldier System From 12th Royal Malay Regiment

The Benefits Towards the Malaysian Army

Technologies are becoming increasingly complicated and increasingly interconnected especially under the Multi Domain Operations. The future battlefield will be characteristic by much higher uncertainty and complexity than ever before. The infantry soldier will still play a vital role across the conflicts but they will be armed by futuristic weapons. IoT in the battlefield encompasses a large range of devices such as drone, sensors, vehicles, robots and other smart technology. The ability to digitally integrate the command and control network and unify operational big data in real time will improve the effectiveness of Malaysian Army operations. Overall, this digital advantage will improve the effectiveness of the decision-making process of the Malaysian Army's capabilities in the Multi Domain Operations.

Today’s information era has not only facilitated the globalisation of the world but also made its users more vulnerable. With military and non-military organizations increasingly dependent on it, future wars would most likely be an information-based warfare where information superiority could become the main factor of a successful outcome. Therefore, Malaysian Army must fully utilize the 5G and IoT in their

training and asset capabilities as a preparation facing the Multi Domain Operations. Technology and IT will enable soldier to execute the mission with successful outcome. The significance of 5G and IoT towards the Malaysian Army are elaborated further below:

- **Enhance Surveillance Process**. Among the most important tasks of the military during peace and war time is surveillance. Surveillance is carried out using several platforms such as aircraft, drone or Unmanned Aerial Vehicle and land assets. To further enhance these capabilities, we would explore new surveillance technologies that are equipped advanced technologies thanks to the 5G and IoT. Artificial intelligence enables greater target reach, as intelligent systems possess augmented precision capabilities and a shorter reaction time. These IoT devices can collect and transmit real-time data on enemy movements, environmental conditions, and battlefield assets, providing enhanced situational awareness to military forces.

- **Enhance Targeting Process**. Operators can use a variety of sensor technologies to acquire the desired data such as determine its location, size, adversary forces, friendly forces, and non-combatants, and other characteristics. A detailed and accurate targeting should be able to minimize civilian casualties and collateral damage. The recent conflict between Ukraine and Russia saw the kamikaze drones that can be fitted with warhead and small bombs have become a fixture of the conflict owing to their low production costs and precision targeting capability. Drones also have been effective for locating enemy targets and guiding artillery fire toward them.

- **Provide Real Time Information**. 5G networks offer ultra-fast speeds, low latency, and high capacity, making them ideal for supporting communication and connectivity needs in the military. An uninterrupted real-time sharing of battlefield information by land, air and naval forces are crucial especially for the commander to plan and execute their mission. In order for a mission to be successful, they need all information which is coming continuously and is updated immediately during operation. It means that this group needs communication assets, which are able to communicate with higher headquarters. Any devices, systems or platform that are equipped with advanced GPS and cameras could send back valuable real time information.

- **Provide Battle Damage Assessment (BDA)**. BDA is the practice of assessing damage inflicted on a target damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. BDA can be applied to the employment of all types of weapon systems. Drones have become increasingly popular BDA among several Armed Forces in the world. Drones are unmanned aerial vehicles that can capture high-resolution images and videos of battlefield and areas that are difficult or dangerous for human to access, reducing the risk of injury or loss of life. Using drones for BDA offers many benefits, including faster and more accurate assessments. Besides that, the use of remote sensing data for BDA are also can help forces conducting BDA accurately.

- **Provide Training and Simulation**. 5G networks can support high-bandwidth applications for immersive training and simulation exercises. Virtual reality (VR), augmented reality (AR), and mixed reality (MR) technologies can create realistic training environments, scenarios, and simulations for military personnel, enhancing their readiness and skills.

- **Strengthening Border Protection**. Recently, drones and radars has been deployed to the Malaysian border in order to strengthen border surveillance. Apart from being able to move quickly at any time and monitor a wider area, the assets were also seen as very important in detecting suspicious activities in the border area. The visible presence of drones and radar installations can act as a deterrent to potential threats. Knowing that border areas are under constant surveillance can discourage illegal activities and unauthorized border crossings. The combination between drones and radars offers a holistic approach to border security, combining aerial coverage, data collection, real-time monitoring, and rapid response capabilities to enhance the effectiveness of border protection efforts.

THE APPLICATIONS OF IOT IN MALAYSIAN ARMY

Malaysian Army has a facility in Army War Game Centre (POP TD) in Kem Syed Sirajuddin, Gemas that used simulator for training purposes. A group of soldiers can be trained using virtual image action and real tactical strategies without endangering themselves with movements made as if in a real situation. This concept instils effective team work and increases the skill and the competency of an individual to use a weapon. Virtual reality approach in military training is the trend

today as it saves cost and space. It is equipped with scenarios like villages, buildings, crowded areas and deserts according to the plan made for the military training.

SOPK, or *Sistem Olah Perang Berkomputer*, is a method used to simulate war scenarios at both operational and tactical levels. By utilizing SOPK, Malaysian Army can improve their readiness to face challenges in real-world war settings while also refining their skills in various aspects including operational efficiency, leadership, and adherence to the principles of war. This SOPK is fully computerized in the conduct of wargames. This exercise can be performed at POP TD using either a static system or portable. It can be used for exercises involving levels tactical and operational ranging from Division formation to individuals/single entities. It can also save cost, time and energy and can be used repeatedly to test the Course of Action (COA). BattleTek IV System has been used by the Malaysian Army since 2014 for conducting wargames.

The Immersive Virtual Training Simulator (VIRTSIM) is a system that are currently present at POP TD since 14th August 2017. VIRTSIM enables soldiers to train in all climates, terrains and logistical constraints, thus improving military tactical skills and adaptability to the battlefield. VIRTSIM are using a special tracking system and Head Mounted Display (HMD) so that they can be in a three-dimensional simulated virtual reality training environment. VIRTSIM could execute various tactical missions and soldiers were able to monitor their progress as the system provided real-time capture of all engagements for immediate, or after action, review and analysis by trainer and soldier. Wireless stereo head-mounted displays provided each trainee with an independent 360-degree view of any virtual environment, enhanced by functional replica of weapon and other elements to provide realistic training effects.

Figure 5: BattleTek IV During Exercise.

Figure 6: A VIRTSIM Training in Malaysian Army War Game Centre (POP TD).

CONCLUSION

The emergence of 5G networks and the IoT has significant implications for military development and operations across Multi Domain Operations. Technology offers numerous benefits to future soldier systems, revolutionizing how soldiers operate, communicate, and perform on the battlefield. The integration of a vast array of interconnected devices and sensors enables smart logistics, predictive maintenance, and enhanced monitoring of assets, optimizing resource utilization and improving operational efficiency and readiness for the military.

The IoT holds significant potential for advancing the development of future soldiers, assist soldiers make correct decisions and respond effectively especially in demanding operational environments. In conclusion, the emerging 5G network and Internet technologies are transformative for military development, offering enhanced connectivity, advanced communication capabilities, IoT integration, operational efficiencies, and strategic advantages.

REFERENCES

BERNAMA, (2020). Border Surveillance More Effective With Drones - MAF. Astro Awani. Retrieved May 11, 2024, from https://www.astroawani.com/berita-malaysia/border-surveillance-more-effective-drones-maf-271287.

Berita Tentera Darat Malaysia. (2017). Teknologi VIRTSIM Pertingkat Kemahiran Pertempuran Anggota TD.

Claire, (2023). The Internet of Military Things. The Cove. Retrieved from https://cove.army.gov.au/article/internet-military-things.

Lockheed Martin, (2022). Four Ways IoT and Space will Revolutionize Military Ops. Retrieved from https:/ /www.lockheedmartin.com/en-us/news/ features/ 2022/four-ways-iot-and-space-will-revolutionize-military-ops.html.

Malaysia Now Ranks Number One Globally For 5G Consistency Score - Fahmi. (2024, February 26). The Star. Retrieved May 16, 2024, from https://www.thestar.com.my/starpicks/2024/02/26/malaysia-now-ranks-number-one-globally-for-5g-consistency-score-fahmi.

MM 7.2-0-2A TD, (2021). Panduan Olah Perang, Markas Pemerintahan Latihan dan Doktrin Tentera Darat, Port Dickson.

Surveillance, (2008). In National Defence Policy (1st ed., pp. 63–64). Percetakan Nasional Malaysia Berhad.

Strategi Domain Daratan, (2024). Cawangan Perkhidmatan Percetakan 91 Depot Pusat Kor Ordnans Diraja.

The Star, (2021). MINDEF plans to procure UAV, drones to strengthen border surveillance. Retrieved from https://www. thestar.com.my/tech/tech-news/2021/11/10/mindef-plans-to-procure-uav-drones-to-strengthen-border-surveillance.10 November 2021.

THE EXPANSION OF 5G NETWORK AND INTERNET OF THINGS TOWARDS THE ARMY FUTURE SOLDIER SYSTEM IN THE PERSPECTIVE OF MILITARY INTELLIGENCE

By LT KOL ALIF AIMAN BIN MOHAMED
ROYAL INTELLIGENCE CORPS

INTRODUCTION

Malaysian Army future soldiers could greatly benefit from employing 5G to increase control, access and use of data that was previously too burdensome to amalgamate and process. According to Land Domain Strategy (SD^2), intelligence along with military strategy, necessitates control of information on threats, particularly those pertaining to geography, its intent, capabilities, strength and weaknesses that are essential to any operation. By utilizing 5G and the Internet of Things (IoT), Malaysian Armed Forces and Army leaders will benefit from mastering knowledge with real or near real-time intelligence through regular situational updates. It makes decision-making possible in a thorough, empirical, and grounded manner that can be applied in combating the threats and present circumstances. By taking a critical thinking approach, planning staff at the strategic, operational, and tactical levels will be able to create plans for operations that are in line with the information and intelligence. This will prevent strategic shocks from being applied to the entire domain forces. To support the strategy, the implementation of 5G networks can improve the interconnectedness and interoperability within the Army or as a joint force in a joint environment by enabling the growth and implementation of two interrelated technologies which are the IoT and Artificial Intelligence (AI). In an age marked by swift technological advancements, the seamless integration of IoT has emerged as a revolutionary catalyst shaping our daily lives, businesses, and national affairs, notably in the domain of military intelligence.

The term IoT refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves. As such, IoT in military intelligence refers to the integration of connected devices, sensors, and systems within the defence sector to enhance situational awareness, improve decision-making, and streamline

operations. This integration allows for the collection, analysis, and sharing of data in real time, which can lead to more informed and timely responses to various situations. This convergence of cutting-edge technology and defence operations holds immense potential for revolutionizing situational awareness, decision-making processes, and operational effectiveness in the military sphere. However, it is important to note that the use of IoT in military intelligence also raises various ethical, legal, and security considerations, particularly regarding data privacy, cybersecurity, and potential vulnerabilities to cyberattacks. In this context it is important to understand the intricate interplay between IoT technologies and military intelligence, exploring the various applications, challenges, and implications that arise when these two domains intersect. Therefore, this article aims to research the expansion and roles of IoT in military intelligence for future soldiers and the importance of implementing robust security measures and protocols to ensure the integrity and confidentiality of sensitive information within Malaysian Army.

The IoT is a paradigm that refers to the interconnection of everyday physical objects, devices, and systems to the internet. This enables them to collect, exchange and process data, often without direct human intervention. These are devices that can sense the environment such as detecting temperature, motion and light or perform actions, where these devices can be turned on and off based on instructions, The IoT devices are all equipped with connectivity such as Wi-Fi, Bluetooth, Smart Tag and RFID, that allow them to connect to networks and exchange data (Mocrii et al., 2018). Without realizing, IoT devices have become a norm in a society where there are many devices used in daily lives. Nearly everyone has a smartphone and smartwatch that can monitor call, health and fitness level, where simultaneously, it could also be applied in healthcare, such as wearable fitness trackers, remote patient monitoring and smart medical devices. Furthermore, smart home technology based on IoT has changed human life by providing connectivity to everyone regardless of time and place (Alaa et al., 2017).

Smart home applies IoT devices like thermostats, lights, and security cameras, which can be controlled remotely through smartphones or voice commands. Therefore, the application of IoT is intertwined in every facet of life, and it can also be applied in the military sphere. For example, fitness tracker serves as valuable tools to monitor

and enhance physical performance, track health metrics and support the overall well-being of military personnel (Suri et al.,2017). These devices can improve the quality of life for military personnel and also potentially provide benefits in terms of security and energy conservation. However, the application of technology will have security implications, and in military intelligence, the potential for security breaches or calamities can be severe. This essay will describe the application of various IoT in military intelligence, the benefits of integrating IoT for future soldiers and the challenges of embracing technology, particularly the IoT.

The IoT offers improved situational awareness, real-time data collecting, and increased decision-making, which could transform several aspects of military intelligence. In the field of monitoring and surveillance, Unmanned Aerial Vehicles (UAVs) and monitoring systems are widely used to gather intelligence. As such, the IoT plays a critical role in the operation of Unmanned Aircraft Systems (UAS). For example, drones, autonomous vehicles and other unmanned systems are equipped with various sensors and IoT capabilities to gather data for reconnaissance, surveillance, and intelligence gathering without putting human lives at risk (Lagkas et al.,2018). Moreover, IoT-enabled UAVs or drones can be utilized to obtain visual data from hard-to-reach or perform tasks in high-risk environments. The data collected from UAVs can offer a better understanding of the terrain and conditions of the area of interest. In general, the efficacy, security, and dependability of UAV control and monitoring platforms in military intelligence operations are improved by utilizing IoT. It makes missions more accurate and responsive, allowing military personnel to obtain vital intelligence quickly and effectively.

According to a study, IoT-enabled surveillance drones have greatly improved military intelligence capabilities in recent conflicts. These drones offer real-time aerial reconnaissance and enemy activity monitoring because of their sophisticated sensors and cameras (Liu et al., 2019). For example, drone surveillance was used in a case study on a military operation in a hostile area to obtain vital information about rebel movements. Armed forces chiefs were able to decide on troop levels and strategies thanks to the drones' direct transmission of high-definition photo and video feeds to the command centre. The operation's overall efficacy was increased and potential ambushes were averted because of the real-time intelligence gathering

(Burmaoglu et al., 2019). Therefore, the integration of IoT-enabled surveillance drones into military intelligence operations represents a transformative advancement in gathering critical information for decision-making. It enhances the effectiveness, safety, and precision of military missions, ultimately contributing to the success of operations in complex and hostile environments.

Intrinsically, the application of IoT in the military can also enhance communication and connectivity. This refers to the integration of different systems, sensors, and devices inside the military ecosystem to collect, process, and transmit data for enhanced operational effectiveness. By establishing robust and secure communication networks, IoT can make sure that critical information is sent and received between military units securely. This includes satellite communications, encrypted data links, and other technologies to ensure connectivity in various operational environments. Specialised communication protocols built for security, dependability, and low latency are used by military IoT devices. For example, Tactical Mesh Radio, walkie-talkie, hearing aids and smartphones which are used to prevent unauthorized access to sensitive information, these protocols are frequently encrypted (Suri et al.,2017). This can include encrypted messaging systems, secure video conferencing, and data-sharing platforms. Integrating IoT technology into military communication and connectivity, can improve real-time, interdependent and improved information or intelligence transfer.

In the context of military intelligence, asset tracking is the process of keeping an eye on and organising the different tools and resources that military groups use such as personnel, cars, weapons, electronics, supplies and more might all fall under this category. These are because sustaining operational readiness, guaranteeing security and maximising resource allocation all depend on efficient asset monitoring. Examples of the devices include, the Global Position System (GPS) which provides accurate positioning information and navigation for military personnel, Electronic Warfare (EW) Equipment used for electronic countermeasures, signal jamming and monitoring enemy communications and radar systems, Electronic Warfare Jamming Systems are used to disrupt or disable enemy electronic systems, including communication and radar systems and sensor detector such as Chemical, Biological, Radiological and Nuclear (CBRN) detectors are used for threat detection and situational

awareness (Gotarane et al., 2019). All things considered, efficient asset monitoring is an essential part of military intelligence that helps commanders make better choices, deploy resources effectively, and keep a high degree of operational readiness. It also helps military missions be more successful and effective overall.

Henceforward, Sensor and Environmental Monitoring uses networked devices to gather, transfer, and process environmental data, which is essential for environmental monitoring and geospatial intelligence. This makes it possible to comprehend, manage, and respond to diverse environmental concerns more effectively. Such as information on weather, topography and other environmental elements that may affect military operations can be gathered by IoT sensors. This data is essential for mission planning and comprehending the operating environment. When it comes to monitoring and gathering data on a broad range of characteristics, including temperature, humidity, movement and sound, IoT sensors also can be installed in land, sea and air settings. Besides, weather stations that have IoT capabilities are one type of IoT gadget that is used for environmental monitoring.

These weather stations have a variety of sensors that allow them to detect things like humidity, temperature, barometric pressure, wind direction and speed, rainfall, and occasionally even the quality of the air. Example of such devices include Data Logger, Environmental Monitoring Device – X2 Pinout and Weather Sensor Transmitters. By integrating IoT technologies with sensors and environmental monitoring, we can make more informed decisions to transmit environmental data for various purposes, mitigate environmental challenges and work towards a more sustainable future. In the military, Intelligence Officer will conduct Intelligence Preparation of the Operational Environment (IPOE), a systematic and dynamic process of analysing and visualising the threat and operational environment in a specific geographic area for a specific mission. It is significant to gather real-time information and current situational awareness to ensure the assessment is accurate and predictive.

Next, IoT in military intelligence can also be applied in Cybersecurity and Network Monitoring, where the IoT-enabled devices can stop illegal access, data breaches, and even sabotage. Intrusion detection systems, firewalls, and other cybersecurity measures are examples of IoT-enabled devices that can be used to monitor and

defend military networks and communication systems against cyber threats. Through the implementation of these measures, military intelligence agencies can improve the security of networks and IoT devices, guaranteeing that sensitive data is protected from cyber threats and illegal access. The use of the IoT in military intelligence has improved situational awareness, decision-making skills, and operational efficiency to a great extent. In complex and dynamic circumstances, the Malaysian Army's future soldiers can acquire a competitive advantage by utilizing real-time data and networked gadgets. IoT technologies will probably play a bigger part in military intelligence as they develop, which will improve the capabilities of armed forces all around the world.

Gathering data in real-time is one of the main advantages of IoT for military intelligence. Obtaining, gathering and analysing data in real-time will ensure intelligence is timely and actionable. Moreover, massive volumes of data are constantly being collected by IoT devices with sensors from a variety of sources, including drones, security cameras and environmental sensors (Tran-Dang & Kim, 2019). In the IoT environment, this enabled the command centres to get this data and analyse it there and then. Because this analysis is real-time, military personnel may make informed decisions quickly because they have access to the most recent information (Lele & Lele, 2019). For example, IoT-enabled sensors on drones can instantly reveal adversary movements or environmental changes in a combat situation, enabling swift tactical and strategic modifications.

A further major benefit of IoT in military intelligence is enhanced situational awareness. A thorough and dynamic image of the battlefield is produced by IoT devices, such as sensors, cameras and communication systems (Ramson et al., 2020). According to Liu et al. (2019), the increased level of awareness guarantees that military leaders possess a comprehensive comprehension of the dynamic circumstances, hence reducing the element of surprise and enhancing overall operational performance. By combining improved situational awareness with real-time data analysis, future soldiers can react to new threats or evolving conditions with greater efficiency.

IoT also helps with mission planning, threat identification and intelligence collecting. Drones and ground sensors are examples of IoT-enabled surveillance devices that make gathering crucial

intelligence easier (Boulaalam, 2019). These devices can track enemy movements, recognise possible dangers and pinpoint important targets. IoT technologies help with strategic decision-making by continuously providing military analysts with information that enhances the quality, predictive and actionable intelligence reports (Burmaoglu et al., 2019). Furthermore, military personnel's coordination and collaboration are improved via IoT-enabled communication technologies.

Any military action needs secure and dependable communication links to be successful (Tran-Dang & Kim, 2019). IoT devices offer robust, secure communication networks that can function in difficult settings. This guarantees that soldiers on the field and command centres may stay in continuous communication, share vital information and efficiently coordinate their activities (Ismail, 2019). As a result, there is an increase in situational awareness and accuracy in decision-making, which helps mission success. Additionally, the IoT technology can also improve military personnel's health and safety. According to Boulaalam (2019), future soldier troops' uniforms are equipped with wearable sensors that can track fatigue levels, monitor vital indicators and identify environmental threats. These gadgets can instantly notify medical teams in the event of accidents or health problems, enabling quick reactions and possibly saving lives (Kott et al., 2016). The IoT enhances the overall performance and readiness of armed forces by placing a high priority on the health and safety of its military personnel.

The energy saving on military bases can benefit from IoT's ability to optimise resource management. IoT sensors are used by smart energy management systems to track and regulate power usage (Burmaoglu et al., 2019). These systems lower energy waste and related expenses by locating regions of excess usage and making automated adjustments. Furthermore, IoT can incorporate renewable energy sources, which can further improve military stations' sustainability efforts. In the Navy, IoT technologies are advantageous for naval operations in the marine sector. Naval ship sensors are always keeping an eye on the ship's condition, fuel usage, and repair requirements (Kott et al., 2016). By sending this data to command centres, resource allocation and preventive maintenance are made possible.

Furthermore, IoT-enabled navigation systems improve maritime situational awareness, assisting in the detection of possible dangers and the prevention of collisions (Ramson et al., 2020). Take into consideration a scenario where a military convoy is passing through a hazardous area while delivering vital supplies to demonstrate the useful advantages of IoT in military intelligence. Real-time condition and position monitoring are facilitated by IoT sensors installed on trucks and supply containers. The sensors on a vehicle instantly notify the convoy's command centre in the event of an ambush or disablement, enabling the prompt dispatch of recovery teams or reinforcements. Real-time analysis of data from nearby surveillance drones provides vital information about the enemy's activities and strategies. The mission success and safety of the convoy are improved by this synchronised response, which is made feasible by IoT technologies.

Nevertheless, IoT applications in military intelligence also have its challenges. Cybersecurity is one of the biggest obstacles to using IoT devices for military intelligence (Perwej et al., 2019). IoT networks are vulnerable to various cyberattacks, such as denial-of-service attacks, malware and hacking (Liu et al., 2019). Cybercriminals might try to breach IoT devices to obtain private military information without authorization or interfere with communication and monitoring networks (Chanal et al., 2021). In a military setting, a successful hack could have dire repercussions, either jeopardising information that is essential to the mission or disrupting operations. Making sure IoT systems are secure for military applications is essential, given the growing dependence on linked devices. Protecting sensitive data and preventing unwanted access requires putting strong encryption, authentication and other security measures in place (Snyder et al., 2019).

Military organisations need to make significant investments in strong cybersecurity measures, such as intrusion detection systems, encryption, and ongoing monitoring, to reduce this risk (Burmaoglu et al., 2019). Denial-of-service attacks, malware and hacking are real concerns that military IoT networks must deal with. There could be serious implications for missions and operations if these attacks cause illegal access to vital military data or interfere with communication and monitoring systems. It is essential to have strong cybersecurity safeguards in place for IoT systems in military environments in order to reduce these threats. Employing robust encryption, authentication

procedures, and other security measures are part of this. Investing in technologies such as intrusion detection systems and carrying out continuous monitoring can also assist in real-time threat identification and response.

Another major obstacle to using IoT for military intelligence is data privacy issues (Perwej et al., 2019). IoT devices gather a tonne of data, such as communication logs, sensor readings, and location data. Sensitive and classified information is frequently included in this data (Tran-Dang & Kim, 2019). It is essential to make sure that this data is sufficiently shielded against unwanted access or exposure. Military intelligence data breaches have the potential to jeopardise mission success and crew safety. To protect sensitive data and guarantee the security of mission-critical operations, however, a strong cybersecurity and network monitoring strategy is needed for the effective integration of IoT in military intelligence. To reduce risks and protect sensitive data, cybersecurity must also be approached with caution.

Consequently, military institutions need to establish stringent procedures for gathering, storing, and exchanging data in addition to strong encryption and access controls (Chanal et al., 2021). Ensuring the data is adequately protected against unauthorised access or exposure is paramount, as breaches in military intelligence data could have serious consequences for mission success and the safety of personnel involved. A robust cybersecurity and network monitoring strategy is crucial for the effective integration of IoT in military intelligence. The military needs to implement a strong encryption method, access controls, and establish stringent procedures for gathering, storing, and exchanging data. Additionally, caution must be exercised in managing cybersecurity risks to safeguard sensitive information effectively.

The deployment of IoT devices across various military platforms and systems presents hurdles in terms of interoperability and standardisation (Boulaalam, 2019). It can be difficult to guarantee seamless integration since different manufacturers' IoT devices may employ different communication protocols (Ismail, 2019). Interoperability is essential for cooperative operations in the military, hence this problem may reduce the usefulness of IoT technology. To meet this challenge, it is imperative to standardise protocols and guarantee interoperability between IoT devices and systems

(Boulaalam, 2019). As has been indicated, one of the challenges is the possibility of variance in the communication protocols employed by IoT devices made by various manufacturers. Because of this, it could be challenging to guarantee that different devices can successfully communicate and cooperate. The military is advised to standardise the protocols and create interoperability between IoT systems and devices to ensure that their gadgets can function flawlessly with those from other manufacturers, this entails creating standard communication standards that other manufacturers can follow.

Depending on IoT technology will create a dependency on outside networks and infrastructure, such as the Internet (Kott et al., 2016). Military activities sometimes occur in remote or dangerous areas where connectivity may be erratic or prone to disruption (Lele & Lele, 2019). The operations' continuity may be at risk due to this reliance on outside networks. Military organisations need to create backup plans and other communication techniques to keep connected during inclement weather to lessen this difficulty. It is not normal to experience internet disruptions when commuting inland or in surrounding cities. It is challenging to get fast internet networks, particularly for military personnel who serve in isolated areas. Consequently, IoT adoption needs to align with the introduction of 5G technology, where it is poised to have a significant impact on the IoT ecosystem as such low latency, higher data rates, massive device connectivity, and improved coverage. Therefore, the military and telecommunication companies (telcos) are crucial for the successful implementation of advanced communication technologies, especially in the context of 5G and IoT applications. This collaboration helps ensure that communication systems are secure, reliable, and tailored to the specific needs of military operations.

CONCLUSION

A new age of capabilities and efficiency across various military activities has been brought about by the integration of IoT technologies with military intelligence. IoT has proven its ability to revolutionise the modern military environment, from smart logistics solutions optimising resource management to wearable health monitoring gadgets prioritising soldier safety and real-time intelligence from combat surveillance drones. It is imperative to recognise the hazards and difficulties that come with this technological advancement, such as

physical weaknesses, data privacy issues, and cybersecurity threats. To guarantee the security and efficacy of IoT technology in military applications, it is imperative that these issues be resolved.

In conclusion, the integration of IoT technologies with military intelligence has ushered in a transformative era in modern warfare. This fusion of cutting-edge technology with military operations has led to a wide range of advancements, impacting everything from logistics and resource management to military safety and real-time intelligence gathering. Collaboration between the military, technology providers, and regulatory bodies will play a vital role in shaping the future of IoT in military operations.

REFERENCES

MP 3.1-0-2.1A TD (2021). Pengoperasian Unmanned Aircraft Systems (UAS) Tentera Darat. Port Dickson: Markas Pemerintahan Latihan dan Doktrin Tentera Darat.

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. Journal of network and computer applications, 97, 48-65.

Boulaalam, A. (2019). Internet of things: new classification model of intelligence. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2731-2744.

Burmaoglu, S., Saritas, O., & Yalcin, H. (2019). Defense 4.0: Internet of things in military. Emerging Technologies for Economic Development, 303-320.

Chanal, P. M., Kakkasageri, M. S., & Manvi, S. K. S. (2021). Security and privacy in the internet of things: computational intelligent techniques-based approaches. In Recent Trends in Computational Intelligence Enabled Research (pp. 111-127). Academic Press.

Gotarane, V., & Raskar, S. (2019, April). IoT practices in military applications. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 891- 894).

Govinda, K., & Saravanaguru, R. A. K. (2016). Review on IOT technologies. International Journal of Applied Engineering Research, 11(4), 2848-2853.

Ismail, Y. (2019). Introductory Chapter: Internet of Things (IoT) importance and its applications. In Internet of Things (IoT) for Automated and Smart Applications. IntechOpen. Jia, M., Komeily, A., Wang, Y., & Srinivasan, R. S. (2019). Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications. Automation in Construction, 101, 111-126.

Kott, A., Swami, A., & West, B. J. (2016). The internet of battle things. Computer, 49(12), 70-75.

Lagkas, T., Argyriou, V., Bibi, S., & Sarigiannidis, P. (2018). UAV IoT framework views and challenges: Towards protecting drones as “Things”. Sensors, 18(11), 4015.

Lele, A., & Lele, A. (2019). Internet of things (IoT). Disruptive Technologies for the Militaries and Security, 187-195.

Liu, S., Dibaei, M., Tai, Y., Chen, C., Zhang, J., & Xiang, Y. (2019). Cyber vulnerability intelligence for internet of things binary. IEEE Transactions on Industrial Informatics, 16(3), 2154-2163.

Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1, 81-98.

Perwej, Y., Parwej, F., Hassan, M. M. M., & Akhtar, N. (2019). The internet-of-things (IoT) security: A technological perspective and review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN, 2456-3307.

Ramson, S. J., Vishnu, S., & Shanmugam, M. (2020, March). Applications of internet of things (iot)–an overview. In 2020 5th international conference on devices, circuits and systems (ICDCS) (pp. 92-95). IEEE.

STRATEGIC IMPORTANCE OF 5G AND INTERNET OF THINGS (IOT) IN MODERNIZING THE MALAYSIAN ARMY'S FUTURE SOLDIER PROGRAMME

By LT KOL TS. IR. ARJUN GOPINATHAN
ROYAL ELECTRICAL AND MECHANICAL ENGINEER CORPS

INTRODUCTION

Based 5G, the fifth generation of mobile networks, signifies a substantial advancement in wireless communication technology. 5G provides unparalleled speed, decreased latency, and the capacity to connect numerous devices concurrently, distinguishing it from previous generations. The capabilities of 5G surpass just speed and capacity. Additionally, it facilitates the creation of sophisticated applications in fields such as self-driving cars, intelligent urban environments, and remote medical services. On the other hand, Internet of Things (IoT) is a network of physical objects that are equipped with sensors, software, and other technologies. These devices can connect to each other and share data through the internet.

The IoT is revolutionizing multiple industries through its ability to deliver instantaneous data, enhance productivity, and facilitate novel business models. Essential elements and technologies comprise sensors and actuators, a range of communication choices, including Wi-Fi, Bluetooth, cellular networks, and 5G, data processing and analytics and lastly safeguarding the security and confidentiality of IoT devices and data. The convergence of 5G and IoT technologies has immense promise for military applications, namely in augmenting the capabilities of forthcoming soldier systems. This paper seeks to establish that the incorporation of 5G and IoT can offer numerous strategic benefits to the Malaysian Army particularly in developing the organisation's Future Soldier Programme.

INTEGRATION OF 5G AND IOT IN MILITARY APPLICATIONS

The convergence of 5G and IoT technologies has immense promise for military applications, namely in augmenting the capabilities of forthcoming soldier systems. The incorporation of this system can offer numerous strategic benefits to the Malaysian Army including Improved Situational Awareness where real data from sensors can be delivered across 5G networks to offer soldiers current information about their surroundings. Secondly, it can provide Enhanced Communication where low latency and high-speed connectivity of 5G

technology guarantee dependable and immediate communication between soldiers and command centres (Dangi et al., 2021) (Banafaa et al., 2024). Third, with respect to effective Resource Management, IoT devices could monitor and control military assets, such as vehicles and equipment, leading to enhanced efficiency in logistics and operations. Through the utilization of 5G and IoT, the Malaysian Army may augment its operational capacities, enhance decision-making processes, and sustain a technical advantage on the battlefield (Ullah et al., 2019). The significance of ongoing research and development in 5G and IoT technologies is highlighted by these breakthroughs, to fully exploit their potential in both civilian and military contexts.

THE NEED FOR MODERNISATION OF THE MALAYSIAN ARMY

In ensuring national security, preserving technological parity with prospective enemies, and boosting operational efficiency are all imperative reasons for the modernization of military forces. The upgrading of the Malaysian Army is crucial due to the changing regional security dynamics and the growing complexity of modern combat. The objective of modernization initiatives is to enhance the operational capabilities of the Malaysian Army across various critical domains. The Malaysian Army has significant expertise in Humanitarian Aid and Disaster Relief (HADR) operations, highlighting the crucial role of efficient logistics, coordination, and human resource management in achieving mission success. Updating these elements can greatly enhance the efficiency and rate of success of such missions (Idris et al., 2014).

Concomitantly, studies conducted on parachute landing procedures among Malaysian Army personnel emphasize the necessity of employing sophisticated training methods to improve the performance and safety of soldiers. Modernization efforts might include cutting-edge simulation technologies and enhanced training standards to equip soldiers more effectively for real-life missions (Aziz et al., 2020). Upgrading military equipment and technology is crucial for enhancing the army's operational readiness. For example, the development of advanced regression models for forecasting noise exposure in military vehicles can result in the creation of improved compartments that enhance the comfort and safety of people. This, in turn, reduces tiredness and enhances operational efficiency (Aziz et al., 2015). The upgrading of the Malaysian Army seeks to tackle certain persistent challenges including firstly on technological integration. The incorporation of cutting-edge technologies like 5G and IoT has the potential to completely transform military operations. These technologies provide heightened situational awareness, greater

communication, and optimized resource management, all of which are essential for contemporary warfare. In addition to that, security and defence is fast becoming more important with the changing nature of regional threats, there is an increasing urgency for a strong and technologically sophisticated military. By modernizing the Malaysian Army, its security capabilities can be enhanced, thereby ensuring the nation's protection against both conventional and asymmetric threats. Another area of concern that can be improved using 5G and IoT is resource optimization. Modernization initiatives can result in enhanced resource use.

Advanced logistics systems, facilitated by the IoT, can optimize supply chains and maintenance operations, guaranteeing that the army is consistently well-prepared and promptly deployable. The efforts that are currently being made and those that will be made in the future should prioritize Advanced Training Programmes by incorporating state-of-the-art training programmes that utilize Virtual Reality (VR) and Augmented Reality (AR), soldiers can be equipped to handle intricate situations inside a controlled setting. Subsequently, the Malaysian Army will keep the forefront innovation by consistently investing in new technologies, such as AI (Artificial Intelligence) and unmanned systems in attempt to upgrade technology. This involves improving current platforms and integrating new ones to boost overall combat efficiency. Lastly, collaborating with other countries and participating in joint exercises will help the Malaysian Army learn from the best practices and technical breakthroughs around the world. This helps create a culture of constant improvement and innovation. By prioritizing these key areas, the Malaysian Army can bolster its operational capacities, guarantee national security, and sustain a competitive advantage in the region. The process of modernization is not only essential, but also a crucial strategic requirement to effectively adjust to the swiftly evolving global security environment.

EVOLUTION OF MILITARY TECHNOLOGY AND THE ROLE OF COMMUNICATION SYSTEMS

The progression of military technology is a crucial element of human history, exerting influence over the results of conflicts and the advancement of society. Throughout the period spanning from the neolithic era to the industrial revolution, notable progress has played a crucial role in propelling military gains. Primitive technical advancements encompassed basic implements like stone tools, progressing to more advanced innovations like metallurgy and horse riding, which greatly augmented military prowess (Turchin et al., 2021).

The industrial revolution brought about significant changes in military technology. Warfare was changed by innovations such as gunpowder, mechanized troops, and improved naval vessels. During this period, there was a significant advancement in the production of weaponry on a wide scale, as well as the establishment of intricate logistical networks to facilitate extensive military operations (Turchin et al., 2021). The introduction of mechanized combat significantly transformed the size and range of military conflicts, resulting in the emergence of novel strategies and doctrines.

Effective communication has consistently been crucial in military operations. Efficient and precise communication has a crucial role in the outcome of missions. Historically, military communication initially depended on messengers and signal fires, gradually progressing to more advanced techniques like semaphore lines and telegraphs. In the 20th century, there were notable progressions with the introduction of radio communication, which allowed for immediate cooperation on the battlefield. During World War II and the Cold War, the establishment of secure communication channels, namely those utilizing frequency-hopping spread spectrum technology, were of utmost importance.

Currently, military communication systems have improved to include sophisticated technologies like satellite communications, encrypted digital networks, and the latest addition of 5G technology. The progress made in these areas has greatly bolstered the capacity of armed forces, facilitating instantaneous information exchange, increased understanding of the current situation, and more effective management and coordination (Bajracharya et al., 2023) (Solcanu et al., 2021). The 5G technology provides fast and reliable connectivity with minimal delay, which is crucial for contemporary military operations. It facilitates the incorporation of the IoT into military applications, enabling the use of a wide range of interconnected devices that can gather and transfer data instantaneously. This improves operational efficiency and furnishes commanders with vital information for decision-making (Sanja, 2020).

Military communication is advancing by combining communication systems with artificial intelligence and cognitive technology. These systems strive to establish self-governing and intelligent networks that can adjust to ever-changing operational conditions. Cognitive information systems provide the capability to evaluate extensive quantities of data, detect patterns, and render conclusions, so greatly augmenting the efficacy of military operations.

RECENT ADVANCEMENTS IN MILITARY TECHNOLOGY GLOBALLY

A notable trend in military technology is the transition towards environmentally friendly and sustainable solutions. Contemporary armed forces are progressively embracing technology that minimize environmental harm while upholding operational efficiency. This encompasses the creation and implementation of hybrid and electric vehicles, fuel cells powered by methanol, and fuel cells powered by hydrogen. Furthermore, researchers are investigating the utilization of photovoltaic energy and biodegradable platforms to improve sustainability. These improvements not only strive to fulfil the rigorous requirements of military operations but also tackle the urgent need for energy efficiency and decreased ecological impacts (Miličević et al., 2023).

Terahertz (THz) technology is becoming increasingly important in military applications, providing previously unachievable capabilities. Terahertz (THz) waves have use in secure short-range communications, improved radar systems, and non-destructive testing of aircraft components. This technology has the potential to be used in anti-missile and anti-stealth applications, giving a substantial edge in modern conflict situations. Although THz technology shows potential for several applications, there are significant obstacles that must be overcome before it can be widely used on a big scale (Kai, 2022).

Virtual Reality (VR) is widely used for military training and psychological conditioning. VR is employed for cognitive training, enhancing psychological resilience, and facilitating post-traumatic growth. It enables soldiers to participate in authentic simulations of combat events, which can aid in enhanced preparedness and mental conditioning. Integrating VR into military training programmes enhances the efficacy of psychological assistance and enhances overall preparedness (Weicheng et al., 2023).

In addition to the above, laser technology's ongoing advancement continues to profoundly transform military capabilities. Laser technology is being employed in a wide range of applications, including laser rangefinders, target designators, non-lethal anti-personnel systems, and anti-missile defence systems. Contemporary laser systems possess advanced technology and are capable of accurately targeting and engaging targets, giving them a strategic advantage in different combat scenarios. The current research and development in laser technology is focused on enhancing their

efficiency and integration into wider military systems (Bernatskyi et al., 2022).

The incorporation of AI and autonomous vehicles in military operations signifies a notable technological progress. Connected Autonomous Vehicles (CAVs), controlled by IoT networks and empowered with AI, provide enhanced logistics operations and strategic benefits. These vehicles can execute intricate manoeuvres, such as changing lanes and avoiding obstacles, with exceptional accuracy. Utilizing blockchain technology to ensure secure communications and data integrity significantly improves the operational dependability of these systems (Biswas et al., 2022). These improvements demonstrate the continuous endeavours to improve military capabilities by using state-of-the-art technologies. As these technologies progress, they are anticipated to offer substantial strategic and tactical benefits, influencing the future of military operations worldwide.

5G TECHNOLOGY AND INTERNET OF THINGS (IOT) IN MILITARY APPLICATIONS

5G technology offers a notable advantage by improving communication capabilities. 5G networks have far greater bandwidth than previous generations, allowing for a larger number of devices to connect simultaneously without seeing any decrease in performance. This is especially advantageous for settings that necessitate dense connectivity, such as urban areas, intelligent cities, and major public gatherings. 5G enables instantaneous communication between vehicles and infrastructure in vehicular networks, which is essential for advanced driver assistance systems (ADAS) and autonomous driving (Kim et al., 2021).

5G technology offers unmatched data transfer speeds, capable of reaching up to 10 Gbps. This fast speed enables the swift transmission of enormous amounts of data, which is crucial for tasks like streaming high-definition videos, virtual reality experiences, and healthcare. 5G enables rapid and efficient transfer of big datasets in high-speed image data transmission systems, facilitating real-time display and processing on host computers. This feature is especially crucial in industrial and healthcare environments, where the prompt transfer of data can have a substantial effect on operations and results (Yongfeng et al., 2020).

The minimal latency of 5G networks, frequently reaching as low as 1 millisecond, is a revolutionary development for applications that

necessitate instantaneous data processing and response. The extremely low latency is crucial for applications that require high reliability and precision, such as remote surgery, autonomous vehicles, and industrial automation. 5G technology in the context of IoT facilitates the implementation of sophisticated remote monitoring systems. These systems can securely transmit real-time data to the cloud, ensuring continuous connectivity and responsiveness of devices (Saleem et al., 2024) (Chen et al., 2020). 5G enables instantaneous analysis and response to sensor data in precision agriculture, thanks to its real-time connectivity. This encompasses the utilization of real-time crop identification and weed control techniques, resulting in improved effectiveness and output in agricultural activities (Li et al., 2019).

APPLICATIONS OF IOT IN MILITARY OPERATIONS

The IoT can significantly change military operations by improving capabilities in areas such as surveillance, logistics, and monitoring the health of soldiers. The utilization of IoT technology greatly improves the military's surveillance capabilities. Deploying devices such as drones, cameras, and sensors enables the monitoring of extensive areas, offering up-to-the-minute data and situational awareness. This is crucial for both tactical and strategic operations. For instance, unmanned aerial vehicles equipped with advanced cameras and infrared sensors can carry out reconnaissance missions, collecting valuable information on adversary activities and the state of the terrain. These devices can function independently, sending data to command centres for analysis and decision-making purposes (Toth, 2021) (Roy et al., 2022). Besides drones, ground-based sensors have the capability to promptly detect and recognize possible dangers, such as trespassers or dangerous substances, and transmit this information immediately via IoT networks. This integration enables a more thorough and up-to-date comprehension of the operational environment, hence improving the efficiency of military operations (Toth, 2021).

Effective logistics are essential for achieving military success, and IoT technology plays a vital role in optimizing these operations. IoT devices have the capability to monitor and determine the whereabouts and condition of supplies, equipment and vehicles. This ensures that resources are efficiently employed and easily accessible when required. For example, the utilization of RFID tags and GPS devices on military assets enables immediate tracking and inventory control, hence minimizing the likelihood of crucial supplies being lost or misplaced. Furthermore, logistical systems that are enabled by the IoT have the capability to anticipate the requirements for repair of vehicles

and equipment. This helps to avoid unforeseen malfunctions and improves the preparedness of armed forces. Automated systems utilize usage patterns and predictive analytics to plan repairs and refill supplies, guaranteeing the military's constant preparedness for operations (Sfar et al., 2018).

The IoT technology is crucial for real-time monitoring of the health and well-being of soldiers. Wearable gadgets, such as smartwatches and health bands, have the capability to monitor essential indicators such as heart rate, body temperature, and hydration levels. The data is sent to medical teams and command centres, enabling prompt response in case of a soldier's health decline. These devices are crucial for ensuring the preparedness of soldiers and delivering prompt medical assistance in the field (Kang et al., 2020). For example, a health monitoring system based on the IoT can notify medical professionals of indications of heat exhaustion or dehydration during vigorous physical exertion, facilitating immediate medical intervention. Additionally, this live health data can be utilized to track the process of recuperation and enhance the management of soldiers' well-being both during and after operations.

THE MALAYSIAN ARMY'S FUTURE SOLDIER PROGRAMME

It is important to understand the present state of capabilities and limitations of the Malaysian Army's Future Soldier Programme before we can assess the effectiveness of affixing 5G and IoT technology on military equipment or system. Malaysian Army Future Soldier Programme possesses certain essential skills that improve operational efficiency, especially in the context of Humanitarian Aid and Disaster Relief (HADR) missions. The Army has cultivated robust logistics, coordination, and human resource management capacities, which are crucial for the triumph of such missions. Efficient logistics systems guarantee the fast delivery of supplies and equipment, while strong coordination mechanisms facilitate effective teamwork and resource allocation during operations (Idris et al., 2014).

In addition, the Malaysian Army utilizes sophisticated maintenance management systems to guarantee the preparedness and dependability of its equipment and infrastructure. These systems aid in monitoring the maintenance requirements and operational status of diverse assets, thereby averting unforeseen malfunctions and guaranteeing that all resources are in their best shape for deployment (Ismail et al., 2016). The Malaysian Army is currently witnessing a growing trend of using IoT and Industry 4.0 technology. These technologies are being utilized to optimize internal communication,

minimize operational errors, and enhance the quality and safety of military operations. IoT frameworks enable enhanced real-time monitoring and management of military assets, hence enhancing operational efficiency and effectiveness (Abdulaziz et al., 2023). The Malaysian Army's capabilities heavily rely on the physical fitness and training of its men. Amidst the COVID-19 outbreak, the Army adjusted to limitations on movement by integrating e-sports and other digital platforms into their training routines. This measure meant that soldiers were able to sustain their physical condition and preparedness despite the constraints imposed by the epidemic (Aman et al., 2022).

Notwithstanding these progressions, the Malaysian Army encounters various constraints including technological gaps. The incorporation of advanced technologies like IoT and Industry 4.0 is currently in its first phases, and the complete capabilities of these technologies have not yet been fully utilized. To fully exploit these technologies, the Army must allocate additional resources towards education, training, and infrastructure (Abdulaziz et al., 2023). Secondly is on Maintenance Challenges. Despite the presence of maintenance management systems, there are problems about the recurrence of defects and insufficient structural design. The current systems do not completely adhere to the highest standards of best practices, suggesting a requirement for more sophisticated solutions such as Building Information Modelling (BIM) to enhance maintenance efficiency (Ismail et al., 2016).

Third area of concern is on Human Resource Management. The precise measurement of the success of human resource management in HADR missions has proven to be hard. The existing methods for evaluating the influence of human resources on mission performance lack sufficient strength, highlighting the necessity for improved measuring tools and approaches (Idris et al., 2014). Final point is on Data Management. The Army encounters difficulties in handling and utilizing massive amounts of data due to the growing utilization of big data and analytics. Efficient data management is essential for operational effectiveness, and there is a requirement to improve competencies in this field to facilitate decision-making and strategic planning (Aziz & Long, 2023).

IDENTIFIED NEEDS FOR MODERNIZATION AND ENHANCEMENT

The Malaysian Army, like other contemporary military organizations, encounters numerous imperative requirements for modernization to augment its operational capabilities and rectify current constraints. The main areas that need to be addressed are the

integration of technology, the management of human resources, and the enhancement of infrastructure. Within the technological integration framework, advanced surveillance systems come to mind. Integrating IoT and sophisticated surveillance technology is essential for enhancing situational awareness. These technologies facilitate the collecting and processing of data in real-time, hence greatly improving decision-making processes during missions. In implementing drones, ground sensors, and AI-powered analytics, organizations can gain extensive intelligence and operational insights. Second is on enhanced communication networks where the implementation of 5G networks is crucial for guaranteeing uninterrupted, high-velocity communication between various units and command centres. Enhancing the coordination and effectiveness of military operations, especially in distant or hostile settings, would be facilitated by this. Lastly, the implementation of IoT-based predictive maintenance systems can decrease the amount of time military vehicles and machinery are out of service and improve their dependability. This entails the integration of sensors and analytics systems capable of forecasting and averting equipment malfunctions, hence enhancing operational preparedness.

Separately, the Human Resource Management aspect of this where is mostly concerned with two areas including training and development and health monitoring. In training and development, by integrating advanced simulation and virtual reality (VR) technologies into training programmes, soldiers can be better equipped to handle real-world situations. This encompasses the utilization of VR to replicate intricate battle scenarios and enhance the efficiency of training drills. Within the scope of health monitoring, utilizing wearable technologies to monitor the health and physical state of soldiers in real-time has the potential to enhance the overall well-being and performance of the troops. These technologies have the capability to monitor and record important physiological indicators, identify injuries at an early stage, and guarantee that soldiers receive prompt medical care.

Furthermore, there will be much need to enhance current infrastructure to accommodate the advancement in 5G and IoT. It is important to enhance maintenance facilities to accommodate sophisticated equipment and technologies. This involves the incorporation of Building Information Modelling (BIM) to efficiently oversee and sustain intricate military infrastructure, guaranteeing that all systems are current and operating at their best. Secondly, there is also requirement to reduce noise in military vehicles. This can be achieved by creating new regression models and enhancing cabin designs, we can effectively tackle the problem of noise exposure in

military vehicles, thereby improving the comfort and safety of people. Decreasing noise levels not only enhances communication within vehicles but also diminishes tiredness and stress among soldiers.

In addition, sustainable best practices must be inculcated among all levels of the military chain. Incorporating eco-friendly technologies and sustainable practices in military operations can minimize the environmental footprint and enhance resource efficiency. This encompasses the utilization of sustainable energy sources and ecologically conscious materials in the establishment and upkeep of military infrastructure. The strategic aims of the Malaysian Army demonstrate their dedication to use cutting-edge technologies and optimal methods to improve their operational capabilities and safeguard the well-being of its soldiers. The future soldier initiative intends to enhance regional security dynamics and optimize mission effectiveness by prioritizing these specific areas.

HOW 5G AND IOT CAN ADDRESS MODERNIZATION NEEDS

5G technology provides substantial enhancements in communication capabilities, which are vital for contemporary military operations. 5G's high-speed, low-latency, and high-reliability features enable military forces to have continuous and immediate communication in many terrains and operational situations. This improved communication infrastructure facilitates various essential military operations, including time-sensitive targeting, clandestine missions, command and control, and supplies management (Bajracharya et al., 2023). Real-time data processing refers to the immediate analysis and manipulation of data as it is generated, without any delay. Situational awareness, on the other hand, is the understanding and perception of the current environment or situation. The utilization of IoT devices, including sensors, drones, and cameras, plays a crucial role in enhancing situational awareness during military operations. These devices gather significant quantities of data, which can be swiftly analysed in real-time due to the minimal delay and large data capacity of 5G technology. The utilization of real-time data processing allows military leaders to promptly make well-informed decisions, hence improving the efficiency of missions. As an illustration, IoT devices have the capability to observe the conditions of the battlefield, monitor the movement of soldiers and equipment, and offer crucial data regarding possible dangers.

The combination of 5G and IoT enables the implementation of predictive maintenance and enhances the efficiency of logistics operations. The Malaysian Army can achieve real-time monitoring of

the condition and operation of vehicles and machinery by implementing IoT sensors on their military equipment. Predictive maintenance systems utilize this data to anticipate the timing of maintenance, so averting unforeseen malfunctions and guaranteeing constant operational readiness of the equipment. Similarly, logistics solutions that are enabled by the IoT can enhance the efficiency of the supply chain by monitoring inventory levels and ensuring prompt restocking. This leads to a reduction in downtime and an improvement in operational efficiency. Security is of utmost importance in the military implementation of 5G and IoT. By combining various technologies, the overall area vulnerable to attacks expands, requiring strong security measures. To safeguard military IoT networks from cyber threats, it is crucial to employ advanced encryption techniques, secure communication protocols, and AI-based threat detection systems. Utilizing technologies like personalized federated learning can bolster the security of IoT systems by guaranteeing the preservation of data privacy, all the while facilitating collaborative machine learning across diverse devices.

The utilization of IoT technology greatly enhances the monitoring of troop health. Wearable gadgets have the capability to constantly track essential indicators like heart rate, body temperature, and hydration levels. They can convey this data to medical personnel instantly and without delay. This feature guarantees the timely identification of any health problems, enabling immediate medical intervention. These solutions not only improve the well-being and security of soldiers but also guarantee that they are consistently in optimal physical shape for their responsibilities.

IMPLEMENTATION STRATEGY FOR INTEGRATING 5G AND IOT IN THE MALAYSIAN ARMY

To incorporate 5G and IoT technologies into the Malaysian Army, a systematic and meticulous methodology is necessary to guarantee smooth integration, improved functionalities, and sustained security. Below is a comprehensive and systematic plan for effectively carrying out the implementation. Assessment and Planning Needs Evaluation is achieved by conducting a thorough evaluation of the present capabilities and constraints of the existing systems inside the Malaysian Army. Identify precise domains where 5G and IoT technologies can offer substantial improvements, including surveillance, communication, logistics, and troop health monitoring.

Secondly, is to engage essential stakeholders, such as military commanders, technological specialists, and cybersecurity experts, in

the planning phase to guarantee comprehensive viewpoints are considered and to promote support from all hierarchical levels.

Third is to focus on infrastructure development. Firstly, is on the network infrastructure itself. Establish the essential 5G infrastructure by implementing tiny cells and enhancing the backhaul network to accommodate higher data volumes. This entails the installation of high-capacity fibre optic cables and the establishment of strong network coverage throughout all military sites and operational locations. Once that has been done, there is a need to integrate IoT devices including sensors, cameras, drones, and wearable health monitors. Verify that these devices are capable of operating on 5G networks to take advantage of the benefits of reduced latency and high-speed data transmission.

Fourth is the incorporation of technology including system integration such as to connect IoT devices with pre-existing military systems. Employ middleware technologies to streamline communication between recently developed IoT devices and existing legacy systems. One possible approach is to utilize edge computing to locally process data, which can help decrease latency and reduce the amount of bandwidth used. Next focus should be on enhancing cybersecurity measures by implementing strong security standards to safeguard IoT devices and 5G networks against potential cyber threats. This encompasses the implementation of encryption, robust authentication protocols, and the utilization of artificial intelligence-powered threat detection systems to promptly discover and counteract possible security breaches.

Fifth is to educate and instil skill among personnel. This can be achieved from having efficient training programmes. There is a need to design and execute training programmes for military personnel to guarantee their mastery of using cutting-edge technologies. This encompasses both the acquisition of technical skills in operating IoT devices and the comprehension of the strategic benefits they offer. Another approach would be to conduct simulation exercises. These exercises can be conducted regularly to test the new systems in real-world scenarios. This will aid in the identification of prospective complications and guarantee that personnel are at ease when utilizing the technology in high-stress circumstances.

In addition to that experimental initiatives can be achieved by commencing initial deployment by implementing pilot programmes in carefully regulated areas to evaluate the seamless integration of 5G and IoT technologies. Identify units or processes where these

technologies can offer immediate advantages and closely monitor their performance. There is a need to solicit feedback and make necessary adjustments based on the outcomes of these early deployments to discover any difficulties or areas that can be enhanced. Prior to implementing the technology on a bigger scale, it is imperative to make any required modifications or adaptations based on this input.

Implementation at full scale with incremental implementation by gradually extend the utilization of 5G and IoT technology to all divisions and operational sectors. Prioritize the establishment of essential infrastructure and support systems prior to the commencement of each subsequent phase of the rollout. Subsequently, continuous monitoring and improvement needs to be carried out. Here, we can implement a perpetual surveillance system to evaluate the efficacy of the newly implemented technology. Utilize data analytics to detect patterns and pinpoint areas that require additional enhancement, guaranteeing that the system adapts to match the evolving demands of the military.

Lastly is on sustainability and maintenance. It is important to implement regular maintenance schedules for both 5G infrastructure and IoT devices is crucial to ensure their continued functionality and security. This encompasses software updates, hardware inspections, and cybersecurity evaluations. In addition, sustainability practices should be incorporated including eco-friendly technologies and sustainable methods to minimize the ecological footprint of the new systems. This can encompass the utilization of sustainable energy sources and energy-conserving equipment.

CONCLUSION

The incorporation of 5G and IoT technology into the Malaysian Army's future soldier programme signifies a significant advancement in improving operational capabilities, efficiency, and security. This strategic upgrade is in line with worldwide trends in military breakthroughs, placing the Malaysian Army at the forefront of technological innovation in defence. The implementation of 5G networks provides highly dependable and minimal delay communication, which is crucial for smooth coordination in military operations. This guarantees that soldiers can communicate efficiently with command centres and one another, facilitating instantaneous exchange of data and decision-making. These qualities are crucial for carrying out intricate assignments with accuracy and agility. Internet of Things (IoT) devices, including as sensors, drones, and cameras, offer extensive and up-to-date surveillance and monitoring capabilities provide enhanced situational awareness. These gadgets collect vital

data on environmental conditions, troop movements, and possible threats, which is then transferred over 5G networks. This integration improves the understanding of the current situation, enabling better-informed judgments at both the strategic and tactical levels.

IoT enabled predictive maintenance systems ensure operational efficiency by continuously monitoring the status of military equipment in real-time. These systems accurately identify potential breakdowns and schedule maintenance in advance, allowing for proactive maintenance. This minimizes the amount of time that operations are suspended and guarantees that all resources are prepared for their intended purpose. In addition, the Internet of Things (IoT) enables the efficient administration of logistics by monitoring inventories and supply chains, guaranteeing the prompt delivery of resources, and improving resource allocation. The utilization of wearable IoT devices to monitor vital signs and environmental circumstances can greatly increase the overall health and safety of soldiers. These devices offer immediate health data to medical professionals, allowing for timely intervention when needed. This competence is essential for preserving the general well-being and preparedness of military troops.

Nonetheless, there are implementation challenges and strategic importance. Among others are in relation to security concerns. The combination of 5G and IoT technologies brings forth novel security obstacles. Implementing stringent cybersecurity protocols, including state-of-the-art encryption and artificial intelligence-driven threat detection, is vital to safeguard against potential cyber risks and uphold the integrity of military operations. Creating robust communication protocols and consistently enhancing security frameworks are essential for tackling these difficulties. Overcoming Infrastructure and technology challenges would entail establishing the required infrastructure for 5G and IoT entails substantial financial commitment and technology adjustment. Implementing 5G networks necessitates the installation of tiny cells and enhancing the current communication infrastructure to accommodate increased data demands. Conquering these obstacles is essential for the effective execution of these technologies.

Training and adaptation are crucial for the success of the modernization programme, as they ensure that military personnel are sufficiently equipped with the necessary skills to effectively utilize new technologies. This encompasses comprehensive technical instruction on the operation of IoT devices and a thorough comprehension of the strategic advantages they provide. Regular simulation exercises and

ongoing educational programmes can facilitate soldiers in efficiently acclimating to new technologies.

In conclusion, the incorporation of 5G and IoT technology into the Malaysian Army's future soldier programme holds the potential to greatly augment operational capabilities, situational awareness, and overall efficiency. By tackling the related difficulties and capitalizing on the strategic advantages of these technologies, the Malaysian Army may attain a modernized, strong, and highly efficient military force capable of meeting present and future security requirements. To fully harness the promise of this technological shift, it is crucial to maintain ongoing investment in infrastructure, cybersecurity, and training.

REFERENCES

Abdulaziz, Q. A., Kaidi, H. M., Masrom, M., Hamzah, H. S., Sarip, S., Dziyauddin, R. A., & Muhammad-Sukki, F. (2023, March 13). Developing an IoT Framework for Industry 4.0 in Malaysian SMEs: An Analysis of Current Status, Practices, and Challenges. Applied Sciences. https://doi.org/10.3390/app13063658

Aman, M. S., Mohamed, M. N. A., Elumalai, G., Ponnusamy, V., Mamat, S., & Kamalden, T. F. T. (2022, March 1). “Involvement in Malaysians’ physical activities and e-sports during the COVID 19 Movement Control Order (MCO) 2020.” International Journal of Physiotherapy. https://doi.org/10.15621/ijphy/2022/v9i1/1149

Aziz, N. A., & Long, F. (2023, March 17). Examining the relationship between big data analytics capabilities and organizational ambidexterity in the Malaysian banking sector. Frontiers in Big Data. https://doi.org/10.3389/fdata.2023.1036174

Aziz, S. a. A., Nuawi, M. Z., Nor, M. J. M., & Daruis, D. D. I. (2015, February 12). New Regression Models for Predicting Noise Exposure in the Driver’s Compartment of Malaysian Army Three-Tonne Trucks. Advances in Mechanical Engineering/Advances in Mechanical Engineering. https://doi.org/10.1155/2014/616093

Aziz, S., Rambely, A. S., Gan, K. B., & Din, W. R. W. (2020, June 4). Kinetics Study in Parachute Landing Fall Technique by Comparing Professional and Amateur Malaysian Army Parachutists Using Kane’s Method. Mathematics. https://doi.org/10.3390/math8060917

Bajracharya, R., Shrestha, R., Hassan, S. A., Jung, H., & Shin, H. (2023, January 1). 5G and Beyond Private Military Communication: Trend, Requirements, Challenges and Enablers. IEEE Access. https://doi.org/10.1109/access.2023.3303211

Banafaa, M. K., Pepeoğlu, M., Shayea, I., Alhammadi, A., Shamsan, Z. A., Razaz, M. A., Alsagabi, M., & Al-Sowayan, S. (2024, January 1). A Comprehensive Survey on 5G-and-Beyond Networks With UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges. IEEE Access. https://doi.org/10.1109/access.2023.3349208

Bajracharya, R., Shrestha, R., Hassan, S. A., Jung, H., & Shin, H. (2023b, January 1). 5G and Beyond Private Military Communication: Trend, Requirements, Challenges and Enablers. IEEE Access. https://doi.org/10.1109/access.2023.3303211

Bernatskyi, A., & Sokolovskyi, M. (2022, June 19). History of military laser technology development in military applications. Ìstorìâ Nauki Ì Tehnìki. https://doi.org/10.32703/2415-7422-2022-12-1-88-113

Biswas, A., Reon, M. a. O., Das, P., Tasneem, Z., Muyeen, S. M., Das, S. K., Badal, F. R., Sarker, S. K., Hassan, M. M., Abhi, S. H., Islam, M. R., Ali, M. F., Ahamed, M. H., & Islam, M. M. (2022, January 1). State-of-the-Art Review on Recent Advancements on Lateral Control of Autonomous Vehicles. IEEE Access. https://doi.org/10.1109/access.2022.3217213

Chen, S., Zhang, X., & Wang, J. (2020, February 25). Sliding Mode Control of Vehicle Equipped with Brake-by-Wire System considering Braking Comfort. Shock and Vibration. https://doi.org/10.1155/2020/5602917

Dangi, R., Lalwani, P., Choudhary, G., You, I., Pau, G.: Study and Investigation on 5G Technology: A Systematic Review, https://doaj.org/article/6d4cde8a49d643958467d4ca80f65152

Idris, A., & Soh, S. N. C. (2014, October 1). The Relative Effects of Logistics, Coordination and Human Resource on Humanitarian Aid and Disaster Relief Mission Performance. https://www.doaj.org/article/002e097d17dc46e586eed59036b3db00

Ismail, Z. A., Mutalib, A. A., & Hamzah, N. (2016, May 1). A Case Study of Maintenance Management Systems in Malaysian Complex and High-rise Industrialized Building System Buildings. https://doaj.org/article/b5c3b9bf3e054e5e833410bb33ca5e6c

Kai, Z. B. G. (2022, October 1). Development and Potential of Terahertz Technology in Military Applications. doaj.org. https://doi.org/10.12132/ISSN.1673-5048.2022.0071

Kang, J. J., Yang, W., Dermody, G., Ghasemian, M., Adibi, S., & Haskell-Dowland, P. (2020, January 1). No Soldiers Left Behind: An IoT-Based Low-Power Military Mobile Health System Design. IEEE Access. https://doi.org/10.1109/access.2020.3035812

Kim, H. J., Choi, M. H., Kim, M. H., & Lee, S. (2021, January 13). Development of an Ethernet-Based Heuristic Time-Sensitive Networking Scheduling Algorithm for Real-Time In-Vehicle Data Transmission. Electronics. https://doi.org/10.3390/electronics 10020157

Li, N., Zhang, X., Zhang, C., Guo, H., Sun, Z., & Wu, X. (2019, January 1). Real-Time Crop Recognition in Transplanted Fields With Prominent Weed Growth: A Visual-Attention-Based Approach. IEEE Access. https://doi.org/10.1109/access.2019.2942158

Miličević, Z., & Bojković, Z. (2023, January 1). Military green technology: Present and future. VojnotehničKi Glasnik. https://doi.org/10.5937/vojtehg71-40544

Mitra, R.N., Agrawal, D.P.: 5G mobile technology: A survey, https://doaj.org/article/f32d426c95f4464b91acd37647f61dac

Roy, S., Vo, T., Hernandez, S., Lehrmann, A., Ali, A., & Kalafatis, S. (2022, July 26). IoT Security and Computation Management on a Multi-Robot System for Rescue Operations Based on a Cloud Framework. Sensors. https://doi.org/10.3390/s22155569

Saleem, K., Zinou, M. F., Mohammad, F., Ouni, R., Elhendi, A. Z., & Almuhtadi, J. (2024, March 7). End-to-end security enabled intelligent remote IoT monitoring system. Frontiers in Physics. https://doi.org/10.3389/fphy.2024.1357209

Sanja, J. (2020, January 1). The importance of 5G network for traffic and automotive industry within the scope of internet of Things (IoT).https://doaj.org/article/bf45143d48644caa857b835d4aaecee8

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018, April 1). A roadmap for security challenges in the Internet of Things. https://doaj.org/article/b9403530a11747a3a00b1abbb5cb862a

Solcanu, V., Gaiceanu, M., & Rosu, G. (2021, October 27). Study of Resistance to Disturbances of the Main Types of Communication Systems on Board Military Ships Used during Interception or Search and Rescue Missions. Inventions. https://doi.org/10.3390/inventions6040072

Sullivan, S., Brighente, A., Kumar, S. a. P., & Conti, M. (2021, January 1). 5G Security Challenges and Solutions: A Review by OSI Layers. IEEE Access. https://doi.org/10.1109/access.2021.3105396

Toth, A. (2021, September 30). Internet of Things Vulnerabilities in Military Environments. Vojenské Rozhledy. https://doi.org/10.3849/2336-2995.30.2021.03.045-058

Turchin, P., Hoyer, D., Korotayev, A., Kradin, N., Nefedov, S., Feinman, G., Levine, J., Reddish, J., Cioni, E., Thorpe, C., Bennett, J. S., Francois, P., & Whitehouse, H. (2021, January 1). Rise of the war machines: Charting the evolution of military technologies from the Neolithic to the Industrial Revolution. https://doaj.org/article/74c9df6f3ee44b6caebc402013e767da

Ullah, H., Nair, N. G., Moore, A., Nugent, C. D., Muschamp, P., & Cuevas, M. (2019, January 1). 5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases. IEEE Access. https://doi.org/10.1109/access.2019.2905347

Weicheng, Y., Weicheng, Y., & Limin, H. (2023, December 1). Application and enlightenment of virtual reality technology in military psychological training. doaj.org. https://doi.org/10.16016/j.2097-0927.202306119

Yongfeng, R., Zefang, Z., Guozhong, W., & Kaihua, Z. (2020, January 1). Design of high-speed image data transmission system based on DDR2. doaj.org. https://doi.org/10.16157/j.issn.0258-7998.190715

THE VAST EXPANSION OF 5G NETWORK AND INTERNET OF THINGS (IOT) - SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM

By LT KOL MOHAMAD HAZRI BIN HAMZAH
GENERAL SERVICE CORPS (PAY)

INTRODUCTION

The internet has become a global phenomenon in the past decade and revolutionized many ways of this world. Internet of Things (IoT) implements the system's effective concept to collect as well as distribute information and data between heterogeneous application servers and IoT devices having the primary aim of effectiveness as well as efficiency improvement in every type of business along with processes of decision-making. Introduction of IoT enables massive improvements in different application areas, like improvement of employee health and safety, infrastructure monitoring, public health, transportation, optimization of equipment performance, production coordination, monitoring of supply chain, and energy monitoring. Every IoT-based system has different applications and there exist estimates that such connect numerous devices in the communication of machine-to-machine (M2M). This is also assumed that the deployment of IoT systems can enable automation of all things within the human environment.

Cellular communications were focused mostly upon human connections until now connecting individuals. However, networks of 5G are designed to connect more devices. The vision of smart military bases, smart things, or smart cities needs relation of IoT, where all objects include inbuilt sensors as well as intelligence for sensing along with making decisions, and provide the ability in communicating to all other objects in any collaborative environment for meeting certain objectives. Such can occur without any intervention of humans. Networks of 5G are also in trials' advanced stages all over the world. Networks of 5G are viewed as potential vital infrastructure needed for making it a reality. 5G can support different heterogenous networks for serving traditional data, voice, and video services along with new services which can be enabled by networked communication of device-to-device (D2D) at much ultra-low latency within extremely dense environments.

In different military operations, every battlefield sensor system along with other solutions that support surveillance and reconnaissance are increasingly vital. Networked military and battlefield devices deployed within operational theatre could be the most efficient solution to it that can ensure each of these is designed to collect every data generated in this environment. 5G and IoT technologies draw similarities with military communication's operational requirements to provision interoperable data, voice, and video services over the global environment. The paper will provide the basic idea of 5G as well as IoT technology, along with discussing their advantages. The paper will also discuss how these technologies can work for future soldier programs for the Malaysian army. The paper will cover readiness of this army in adopting this. The paper will also provide some real situations of the use of these technologies in wars. Finally, the paper will discuss the challenges of these technologies and provide recommendations for addressing them.

5G DEFINITION

5G has been recognized as the innovative technique that led to the increase in the performance of "wireless cellular technology". 5G or fifth generation has helped in improving the downloading and uploading speeds of the internet through the formation of secured connections. There has been a considerable increase in the data consistency rate through the deployment of this technology. This in turn has led to the considerable increase in the reliability and efficiency within the network as compared to the 4G networks.

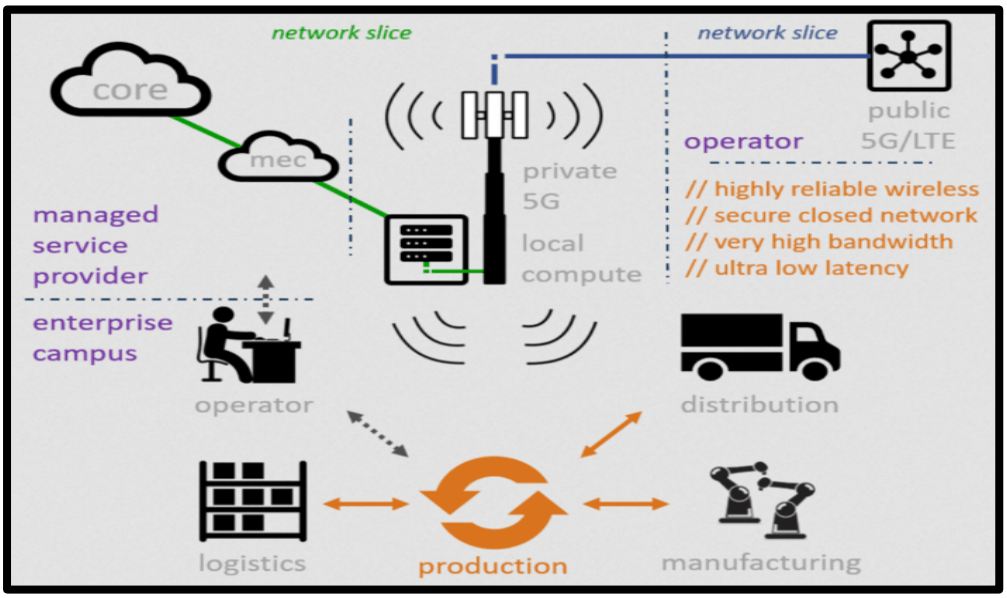

Figure 1: 5G Network

Through the implementation of this technology, there is formation of a virtual connection within machines and objects. This is effective in increasing the availability of users with a considerable increase in the data reliability on a large scale. There has been a considerable increase in the rate of user experience through the consideration of this technology. This is because there has been a considerable increase in the performance and efficiency through the increase in the data processing speeds. This technology is implemented mainly for three different connected services that mainly comprise large IoT, improved mobile broadband and accomplishment of mission-critical communications. There is implementation of massive embedded sensors that helps in the formation of seamless connections through the reduction of power consumption and cost control initiatives. The formation of low latency and reliability within critical communications are accomplished through the implementation of the 5G technology. Furthermore, there is a growth in the mobile broadband performance through 5G technology by diminishing the latency rate and maintaining a uniformity within the information flow.

There has been implementation of the radio waves by 5G technology for accomplishing a suitable information flow within the networks by implementing cell sites. Encoded data modification is done through the implementation of this technology that helps in raising the carriers' usable airwaves' quantity. There has been involvement of three different technologies that contribute to the suitable functioning of 5G. These include OFDM, network slicing and small towers. In the network slicing technology, there has been deployment of numerous "independent virtual networks" within an identical network. This helps in the gradual increase in the network performance by enhancing device efficiency and user experience on a large scale. The application of "orthogonal frequency division multiplexing" helps in encoding the high-band airwaves and thereby helps in increasing network flexibility by minimizing the latency rate. Furthermore, there is a growth in the communication rate through the implementation of smaller transmitters that helps in increasing the data flow speed.

INTERNET OF THINGS (IOT) DEFINITION

IoT or the "Internet of Things" determines a combined network of different physical objects that mostly include technologies, software and sensors. These objects are embedded devices that help in exchanging and linking data with systems that are available within a network. In other words, the presence of interconnected devices helps in accomplishing proper communication within nodes through the accurate transfer of information. The implementation of IoT has been

considered to be a necessary aspect as it helps human beings to accomplish their work quickly and lead to a smart lifestyle. There is an automation of the operational process through the development of real-time outcomes through the implementation of IoT devices. Through the inclusion of these devices, there has been a complete elimination of the human intervention and thereby help in the suitable accomplishment of tedious tasks.

Speaking in the context of the military sector, the inclusion of the IoT has been a beneficial technique in developing connectivity through the use of sensors for transmitting information within army base camps. Through the involvement of this technology, there is a proper accumulation of real-time information by the military personnel. As a result, there has been formation of informed decisions by the army by tracking the exact position of the enemy and thereby helping in increasing the efficiency within the decision-making process. Apart from that, there has been formation of data-driven decisions, improved communications and accomplishment of predictive maintenance through IoT technologies. There has been an increase in the quality of business decisions through the application of this technology.

❖ The merits that are raised through the implementation of this technology are as follows:

- The application of this technology results in the generation of information accessibility from remote locations.

- There has been a considerable reduction in the wastage of money and time through the use of this technology by exchanging data packets within one connected network.

- The output quality is enhanced through the consideration of this technology as there is a complete elimination of human intervention by accomplishing task automation.

❖ The demerits that could be considered through the application of IoT are as follows:

- The challenges are raised in making a proper management of devices due to the presence of multiple sensors and transmitters in a network.

- Due to the lack of manual control, there is no awareness within users concerning the cyber-attacks that are occurring through the use of this technology. As a result, there is a possibility of data loss through the application of IoT by stealing valuable information through the involvement of hackers.

- Data communication is hampered due to the presence of complexity within data compatibility through IoT devices. This indicates that there might be a delay in accomplishing communication within stakeholders through the use of IoT devices.

WORKING PROCEDURE OF IOT

Referring to the technical workflow of IoT, it is analyzed that initially there has been a proper accumulation of the data through the inclusion of sensors that are embedded within the devices. Through the involvement of these sensors, there has been accumulation of raw information that is available in the external environment. This raw information is stored in different devices that include smart gadgets and mobile devices. Through the involvement of GPS trackers and sensors, there is automatic accumulation of information from surroundings and thereby leading to the entry of real-time information within the storage devices on a large scale.

Based on the accumulated information, connectivity is developed through the consideration of a gateway for making an effective communication of information within the cloud network. The involvement of LPWAN, WiFi and Bluetooth helps in the formation of a gateway in receiving and transferring data from the sensors to the cloud. Due to the usage of these devices, there has been a considerable decline in the rate of power consumption which is considered to be a sustainable approach. In the third stage, there has been a proper analysis of data to make a suitable recognition of the data patterns. This approach is effective in the formation of informed decisions through the accurate recognition of the data trends through data analysis.

In the final stage, there is a proper representation of the analyzed data that in turn helps in the formation of accurate communication of users. This stage helps in increasing the user experience through the formation of actionable insights in the data and thereby leading to the formation of informed decisions. Alerts might be generated automatically within the mobiles and smart gadgets in the

form of email notifications or messages based on the information accumulated through IoT devices.

Based on the above working procedure, it could be analyzed that there has been an increase in the operational efficiency through the application of IoT. The entire is automated due to no involvement of humans in accomplishing data accumulation and analytical activities. This technology is considered to be sustainable as it helps in the significant reduction of operational costs and decline in the rate of power consumption. Operational costs are reduced due to the decline in the usage of numerous equipment and complete elimination of humans in accomplishing data monitoring activities through IoT technology. Therefore, the usage of this technology is considered to be productive for the military sector as it helps in increasing connectivity and analytical outcomes automatically. Informed decisions could be generated by army personnel by making use of IoT. There is generation of automatic tracking and diagnosis of enemy locations by using IoT and thereby assisting in increasing connectivity within users. Currently, the integration of ML algorithms has an added advantage for this technology as it helps in making a proper recognition of malicious activities especially in the cyber-defense units of the military sector.

ADVANTAGES OF IOT AND 5G

Linking with the working procedure of IoT, it is analyzed that there has been formation of numerous benefits while using IoT. These benefits are as follows:

- **Growth in Data Connectivity**. The usage of IoT helps in the gradual increase in the data connectivity on a large scale. This is accomplished through the implementation of sensors that helps in making error-free communication within devices. Due to the presence of IoT devices at different locations, it becomes compatible for the users to get adapted with the IoT devices in a suitable manner.

- **Efficient Data Collection**. Due to the presence of IoT sensing and architecture, this technology helps in making a collective necessary data from company operations. The involvement of sensors and GPS trackers help in tracking the data automatically and thereby help reducing the human interventions in the data collection process.

- **Implementation of Automation Concept**. Through the application of sensors and transmitters, the teeth automatically process from the external environment to the user interface. This results in the increase in the operation of efficiency on a large scale. Operational cost is considerably reduced through this technology.

- **Accurate Monitoring of Data**. The usage of IoT is beneficial in the formation of informed decisions. This is because there is a proper accommodation of real time information by the sensors.

- **Increase in Data Safety**. The IoT usage determines the complete rejection of human control over the data. This indicates that there has been a growth in information security by automatically tracking the risks that are occurring in the external environment.

The benefits that could be met through the implementation of 5G technology are as follows:

- This technology helps in the formation of speed upgrades especially during peak times. At least 10 gbps speed is provided by this technology which is effective in time savings and quick accomplishment of tasks.

- The formation of low latency in the technology helps in visual processing capability of machines on a large scale. This indicates that the communication within machines and humans are quickly completed through the deployment of the technology.

- There is a growth in the bandwidth that in turn helps in generating massive optimization within a network and control over usage spikes.

- A greater coverage is provided by the technology that proves to be helpful for the consumers to accomplish their remote work.

IOT AND 5G IN MALAYSIAN FUTURE SOLDIER PROGRAMME

As different technologies, such as IoT, artificial intelligence, and augmented reality merge with networks of 5G, there is the beginning of this new era where every battle can be waged in cyberspace’s huge

digital domains. Using networks of 5G and IoT technologies, military commanders can have access to every strategically positioned sensor that can allow for every coordinated assault assisted using live-streamed analytics. All solders within the field might be empowered by different wearable displays, which access efficient computing resources within the cloud. In addition, weapon systems can be completely software-defined, having capabilities remotely updated using over-the-air download. However, such constant connectivity opens different new vulnerabilities. Also, adversaries can look in hacking networks, infecting systems using malware, and corrupting data streams. Vital infrastructure such as transportation hubs and power grids can be turned off using cyberattacks. Additionally, disinformation campaigns could manipulate opinion of public along with undermining morale of opponents.

Figure 2: Future Wearables for Military

As capabilities of 5G warfighting emerge, the government of Malaysia can heavily invest in protection of cybersecurity for civilian as well as military networks. Different advanced technologies such as quantum encryption could be quite efficient. International agreements could be set regarding prohibited and acceptable tactical maneuvers based on 5G within warfare scenarios for the Malaysian army. 5G technology could redefine what this means in waging war in this digital age. The Malaysian army can gain strategic edge by devoting high research priorities for understanding along with adopting disruptive influence of 5G and IoT technologies upon modern conflict. These future soldier programs for the Malaysian army would need two-way

communication with every criterion necessary for sharing such gathered data in shortest time possible. Data collected as well as analyzed in such a way can efficiently contribute to monitoring of operational situation along with the environment. Such a capability can enable maintenance as well as acquisition of information superiority, along with speeding up processes of decision-making efficiently.

Network intelligent devices would be vital for these future soldier programs for the Malaysian army to achieve every operational objective and execute operations successfully. IoT at micro as well as macro scales in future would be military functioning's cornerstone. Future warfare would be multi-domain that can imply battlespace's expansion. IoT's macro level for Malaysian army can be established upon same lines as within civil domain; however, with differences in software, frequencies, linkages, and connected systems and devices. Integration of 5G and IoT technologies into future soldier programs of the Malaysian army would need in following a few exclusive software layers as well as encryption protocols. These should also follow protocols of data sharing for communication along with data security that can be followed in classified as well as sensitive communications within the Malaysian army. It could be primarily in preventing breaches as well as intrusions into IoT networks of these programs.

READINESS OF MALAYSIAN ARMY TO ADOPT THESE TECHNOLOGIES

As there is advancement in 5G and other private wireless technologies, integration of 5G as well as 5G-enabled IoT applications can also hold huge potential to support modernization of this military base of the Malaysian army along with enhancing the overall warfighter readiness. Deployment of IoT applications and 5G networks is revolutionizing security, training, logistics, and communication, along with helping in strengthening military capabilities. A huge benefit of private network is ability in customizing the network for meeting specific requirements when compared to public 5G network. Better control over coverage, overall performance, connectivity, and capacity can allow in tailoring features of the network in suiting certain needs. Critically vital to this military is features of superior privacy as well as security offered by private network. In addition, traffic within private network can be kept in control that can reduce exposure to different external threats. Also, private networks can provide better reliability as each of these is built as well as managed for certain users or purpose. It can result in lesser interruptions along with better service quality.

Improved collaboration can enable better reliability and speed, and IoT integration, representing different benefits of such a network. With the deployment of IoT devices as well as sensors, solders could gain efficient visibility into different military operations. It can enable efficient management of all operations and equipment's predictive maintenance, improving the overall mission readiness along with reducing downtime. This combination of low latency and high bandwidth of 5G enables tracking of all assets, reducing risks of loss or theft and enhancing security. Robotics based on IoT can provide route optimization, analytics, and maintenance for guided vehicles. Smart cameras can also be used for streaming along with storing video footages for tracking of assets and authentication. Connected equipment that can include conveyance systems using scanners along with other devices enabled by IoT can optimize asset management, along with providing input for heat mapping of different operations. IoT and 5G applications can provided enhanced measures of security for military bases. In addition, IoT cameras and sensors could be integrated with networks of 5G for creating efficient surveillance systems.

Figure 3: Readiness in Malaysian Army

RUSSIA – UKRAINE CONFLICT

The battle has mostly taken place on battlefield itself; however, there has been war of different technologies from disinformation to cyberattacks and economic impact upon global tech scene. Technology has played an essential role to support Ukraine in rebuilding regained territory along with communicating with outside world. Russia fired the first shot using numerous DDoS attacks along with a cyberweapon composed of trojan horse wiper malware for knocking out the connectivity of the internet as well as paralyzing every command and control center of Ukraine. As for defense from Ukraine, this has been quick in disbursing digital infrastructure into public cloud. Ukraine partnered with several international tech firms for building resilience in systems as well as encryptions.

This war has also featured many more drone technologies with both these sides using UAVs for surveillance and reconnaissance. Drones have been used by Ukrainian military for targeting every enemy position with appropriate munitions. Ukraine's effective usage of IoT for targeting every Russian forced has also pushed this technology from an ethical issue to being one huge concern for leaders all over the world. Ukraine has used advanced facial recognition and imaging software for identifying decreased Russian individual through their profiles on social media for notifying their relative about their deaths along with transferring bodies to respective families.

Figure 4: Use of Drones for Russia–Ukraine Conflict

ISRAEL–PALESTINE CONFLICT

The army of Israel has deployed a military technology enabled by AI for combatting autonomous weapons on Gaza. New technologies of defense that included robotic drones and gunsights powered by AI has formed bright spot in the period for tech industry of Israel. This war has presented numerous threats; however, it has also presented different opportunities in testing emerging technologies in this field. Like other modern conflicts, this war has also shaped by numerous UAVs that have made these attacks from air cheaper as well as easier. The army of Israel has used optic sight enabled by AI that is attached to different weapons, like machine guns and rifles. This has helped soldiers in intercepting drones. Another system for neutralizing drones has included the deployment of friendly drone with the net that this could throw around enemy craft for neutralizing it. In addition, numerous cyberattacks have been conducted within cyberspace domains of these two sides. The major attack methods included DDoS, website defacement, data theft, and all other techniques of cyberattack. Additionally, to executing different cyberattacks, different hacktivist groups that have been supported by different factions use videos, images, and text for propagating narratives.

Figure 5: Use of Generative AI in Israel Attack

CHALLENGES AND DISADVANTAGES

❖ Challenges

The most crucial issue related to 5G and IoT technologies within military are is security of data. There is increased connectivity of more devices in a big extended network along with increase in system complexity and overall devices provides different kinds of security risks. As future soldier program of the Malaysian army will include many different technologies, variation of different possible attacks would also be high. A vulnerable point for such program for intrusion is sensing layer. It is responsibility of this layer for the collection of data along with sensors working in sensing layer will play a vital in transfer as well as collection of data. Every sensor of this layer must prevent all kinds of physical attacks, shortening of functionality and lifetime of sensors and damage of units of data collection. Intelligence sensor and RFID networks without surveillance can represent huge risk to this soldier program for this army.

Communication among nodes can be achieved within data transfer media. Also, as this is quite vital, confidential data can be quite vital in ensuring the accessibility, confidentiality, and integrity of data. There can be different kinds of intrusions with the network layer of this program. Spoofing attack can be conducted where intruders can identify themselves as other users of that network along with getting unauthorized access to all data. Sinkhole attack can be performed where intruders deviate network traffic to another certain target; hence, data cannot be transferred to original address and can be diverted to any unauthorized user. Eavesdropping can also be performed where enemies can detect as well as decrypt messages among devices within that network. Denial of service attack can also be performed where network node can be bombed using numerous requests, such that this would become unable in fulfilling its function. In addition, MITM attack can be performed where intruders can influence communication among sensor nodes through that network along with monitoring data transfer as well as collection of data.

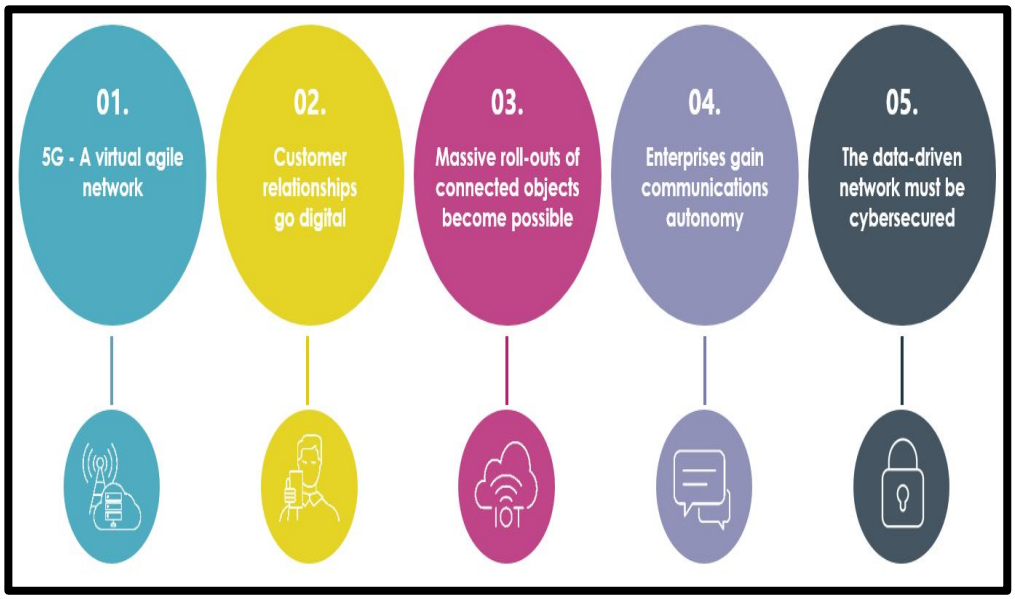

Figure 6: Challenges of 5G Network for Programs

❖ **Disadvantages**

There can be many disadvantages of using 5G and IoT technologies in future military programs for Malaysian Army. A few of the disadvantages of these technologies are:

- **High costs of infrastructure**. Implementing 5G and IoT technologies would need significant investments for infrastructure. Developing the needed infrastructure for network along with deploying base stations of 5G could be quite expensive, especially in some areas.

- **Device compatibility**. Malaysian army should upgrade current devices of IoT for taking complete advantages of capabilities of 5G technology. This would be necessary in working on different new prototypes which could easily adapt to IoT and 5G technologies.

- **Limited coverage**. There is limited coverage for 5G networks, particularly those utilizing high-frequency waves. Hence, it could result in some coverage gaps within remote as well as rural areas that might hinder deployment of IoT and 5G solutions in such regions for the army.

RECOMMENDATIONS

A few recommendations have been provided for future programs for the Malaysian army for mitigating all identified challenges along with using these solutions efficiently.

- **Conduct More Research of 5G to Support Military Logistics**. Smart tags can be useful in every phase of wartime logistics with the tracking of numerous items, like emergency and material supplies. Such information could be then sent back to algorithms of artificial intelligence for maintenance and monitoring. In addition, high-band 5G would be useful to transfer sensor data among unmanned networks and vehicles and operators. Remote communications would also be useful to establish robust architecture along with communicating across support contractors and allies.

- **Implementation of 5G and IoT Technologies Into Numerous Operational Scenarios**. 5G and IoT technologies can be implemented in numerous operational scenarios for the Malaysian army, like special force operation and humanitarian assistance.

- **Develop Mitigation Methods to Counter Unauthorized Exploitation**. Other countries might exploit 5G and IoT technologies for gaining operational advantages against different blue forces. For mitigating it, the Malaysian army must be prepared for defending against jamming, messaging of information warfare, fake base stations, protocol attacks, and EW threats. Vulnerabilities in any network must be mitigated, such that these cannot affect the ecosystem of 5G and IoT negatively.

- **Track Every Frequency Development Over Allies**. 5G deployment within many countries have been delayed by frequency disputes. Hence, the Malaysian army must consider alternative approaches for conducing communication and coordination in different countries, especially for different operations which might heavily depend on low latencies and high bandwidth in wider areas.

- **Work With Allies for Creating One Common Roadmap of Uses of IoT and 5G for The Army**. The ecosystem of 5G and IoT would be completely rolled out within the country. There can be numerous initiatives of different trials

which can test 5G within urban corridors as well as cross-country ports, waterways, railways, and motorways. As development of this ecosystem of 5G and IoT increases, the roadmap can detail military uses for allies would be necessary for seamlessly carrying out different operations.

- **Assess Every Potential Interoperability Issue Across Countries and Providers**. A huge-scale war for Malaysia would need active coordination as well as communication among the host nation and allies. Interoperability issues can be faced by the army, especially while moving across every border. As 5G technology is rolled as well as new concepts and equipment of operations would be developed, mitigating such challenges would be paramount. Equipping and training soldiers of this army with interoperability would be quite resource intensive; however, this would be necessary in ensuring successful operations of military along with realizing whole array of IoT and 5G benefits.

CONCLUSION

There is a huge impact of digitalization on everyday environment. 5G and IoT systems and devices are inevitable, and they have an essential impact on lives of people. These devices monitor respective environment, collecting data, and sharing this with every other element of that system as well as user as per pre-programmed task. New kinds of solutions of information services and communication technologies offer different opportunities for different military applications, which could make huge contributions to successful conduct of different military operations. Integration of IoT devices into cloud could provide operational situation awareness for gaining along with maintaining information superiority that can contribute to operations' successful execution. An efficient basis for it is isolated technology of 5G that guarantees data's absolute security for different military applications, as this allows different military networks in being isolated completely from every public network. 5G technology could be used for developing high bandwidth, robust, reliable system having lower network latency, which could be deployed on different combat platforms. In addition, with private network of 5G, high mobility, secured, and trusted connections could be established for supporting battle command as well as control management along with different support activities.

Into any virtualize network, military and battlefield IoT devices could be integrated as well as deployed into cloud infrastructure. Such a designed system can meet every requirement of technical solutions deployed within operational environment. IoT devices can connect different battlefield devices as well as military troops using wearable devices. Also, under different challenging terrains, like jungle, mountains and deserted terrains, these wearable devices could sense as well as track troops' relative locations, atmospheric conditions, weapon stage, health status, and communicate all information to central command. Central command could analyze solders' tactical data for making decisions based upon real-time incoming information. This is expected that due to neural networks' advancement, wearable devices can evaluate emotional, physical, and psychological state of pilots of air force. Existing architecture of transmission of data on battlefield isn't able in supporting the future as well as current of processing and collection of data; hence, 5G and IoT technologies have found their roles as well as places within many modern defense applications.

REFERENCES

Ahmed, Sajjad, Jianming Yong, and Anup Shrestha. "The integral role of intelligent IoT system, cloud computing, artificial intelligence, and 5G in the user-level self-monitoring of COVID-19." *Electronics* 12, no. 8 (2023): 1912.

Alqurashi, Fahad S., Abderrahmen Trichili, Nasir Saeed, Boon S. Ooi, and Mohamed-Slim Alouini. "Maritime communications: A survey on enabling technologies, opportunities, and challenges." *IEEE Internet of Things Journal* 10, no. 4 (2022): 3525-3547.

Andås, Harald Erik. "Emerging technology trends for defence and security." (2020).

AWS. What is 5G? - 5G network explained - AWS, 2021. https://aws.amazon.com/what-is/5g/.

Bahadur, Preeti Singh. "Analysis on Various Aspects of Internet of Nano-Things (IoNT), Its Integration in Machine Learning, and Its Diverse Applications." In *Next Generation Materials for Sustainable Engineering*, pp. 297-315. IGI Global, 2024.

Baidya, Dayarnab, Ruchee Bhagwat, and Mitradip Bhattacharjee. "The use of the cognitive Internet of Things for smart sensing applications." In *Cognitive Sensors, Volume 1: Intelligent sensing, sensor data analysis and applications*, pp. 4-1. Bristol, UK: IOP Publishing, 2022.

Balaji, Subramanian, Karan Nathani, and Rathnasamy Santhakumar. "IoT technology, applications and challenges: a contemporary survey." *Wireless personal communications* 108 (2019): 363-388.

Bhardwaj, Anshu. "5G for military communications." *Procedia Computer Science* 171 (2020): 2665-2674.

Brown, Edmond M., Francis M. Beaudette, and Jonathan Phillips. "Army Futures Command Concept for Special Operations 2028." *ARMY FUTURES COMMAND* (2020).

Cook, Jonathan, Sabih Ur Rehman, and M. Arif Khan. "Security and privacy for low power iot devices on 5g and beyond networks: Challenges and future directions." *IEEE Access* (2023).

Cruz, Diogo, Tiago Cruz, Vasco Pereira, and Paulo Simões. "Designing a high-fidelity Testbed for 5G-based Industrial IoT." In *Proceedings of the 22nd European Conference on Cyber Warfare and Security (ECCWS 2023), Athens, Greece (June 2023). DOI*, vol. 10. 2023.

Dangi, Ramraj, Praveen Lalwani, Gaurav Choudhary, Ilsun You, and Giovanni Pau. "Study and investigation on 5G technology: A systematic review." *Sensors* 22, no. 1 (2021): 26.

Donghao, Cui, Zhang Bohua, Ou Chaomin, and Chen Zhiyu. "Research on Military Internet of Things Technology Application in the Context of National Security." In *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*, pp. 992-998. IEEE, 2021.

Farooq, Muhammad Shoaib, Shamyla Riaz, Adnan Abid, Tariq Umer, and Yousaf Bin Zikria. "Role of IoT technology in agriculture: A systematic literature review." *Electronics* 9, no. 2 (2020): 319.

Gnoni, Maria Grazia, Paolo Angelo Bragatto, Maria Francesca Milazzo, and Roberto Setola. "Integrating IoT technologies for an “intelligent” safety management in the process industry." *Procedia manufacturing* 42 (2020): 511-515.

Gomes, João Eduardo Costa, Ricardo Rodrigues Ehlert, Rodrigo Murillo Boesche, Vinicius Santosde Lima, Jorgito Matiuzzi Stocchero, Dante AC Barone, JulianoAraujo Wickboldt, Edison Pignaton de Freitas, Julio CS dos Anjos, and Ricardo Queiroz de Araujo Fernandes. "Surveying Emerging Network Approaches for Military Command and Control Systems." *ACM Computing Surveys* 56, no. 6 (2024): 1-38.

Jayanthi, S., H. Shaheen, U. Balashivudu, and Meesala Shobha Rani. "Evolution and significance of unmanned aerial vehicles." In *Unmanned Aerial Vehicle Cellular Communications*, pp. 287-311. Cham: Springer International Publishing, 2022.

Jones, Mason P., and Erica L. McCaslin. "Special Operations in a 5G World: Can We Still Hide in the Shadows?." PhD diss., Monterey, CA; Naval Postgraduate School, 2020.

Khan, Amina, Sumeet Gupta, and Sachin Kumar Gupta. "Emerging UAV technology for disaster detection, mitigation, response, and preparedness." *Journal of Field Robotics* 39, no. 6 (2022): 905-955.

Krop, Anna. "A Thing on the Internet? Or the Internet in a Thing? New Technology Crimes." *Analiza kryminalna w przyszłości*: 63.

Lan, Qiao, Dingzhu Wen, Zezhong Zhang, Qunsong Zeng, Xu Chen, Petar Popovski, and Kaibin Huang. "What is semantic communication? A view on conveying meaning in the era of machine intelligence." *Journal of Communications and Information Networks* 6, no. 4 (2021): 336-371.

Latif, Shahid, Maha Driss, Wadii Boulila, Zil E. Huma, Sajjad Shaukat Jamal, Zeba Idrees, and Jawad Ahmad. "Deep learning for the industrial internet of things (iiot): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions." *Sensors* 21, no. 22 (2021): 7518.

Layton, Peter. "Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars." *Network* 4, no. 20 (2021): 1-100.

Maheswari, B. Uma, S. Sagar Imambi, Dler Hasan, S. Meenakshi, V. G. Pratheep, and Sampath Boopathi. "Internet of things and machine learning-integrated smart robotics." In *Global Perspectives on Robotics and Autonomous Systems: Development and Applications*, pp. 240-258. IGI Global, 2023.

Malik, Manisha, Maitreyee Dutta, and Jorge Granjal. "IoT-Sentry: A cross-layer-based intrusion detection system in standardized Internet of Things." *IEEE Sensors Journal* 21, no. 24 (2021): 28066-28076.

Morgan, Steve, and Jaime Wightman. "Operationalizing IoT Data for Defense and National Security." *IoT for Defense and National Security* (2022): 59-72.

Niknami, Nadia, Avinash Srinivasan, Ken St. Germain, and Jie Wu. "Maritime Communications—Current State and the Future Potential with SDN and SDR." *Network* 3, no. 4 (2023): 563-584.

Nwanakwaugwu, Andrew Chinonso, Ugochukwu O. Matthew, Ogobuchi Daniel Okey, Jazuli Sanusi Kazaure, and Ubochi Chibueze Nwamouh. "News Reporting in Drone Internet of Things Digital Journalism: Drones Technology for Intelligence Gathering in Journalism." *International Journal of Interactive Communication Systems and Technologies (IJICST)* 12, no. 1 (2023): 1-22.

Rashid, Adib Bin, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, and Mehedy Hassan Bappy. "Artificial intelligence in the military: An overview of the capabilities, applications, and challenges." *International Journal of Intelligent Systems* 2023 (2023).

Saha, Souradip, Warren Low, and Beniamino Di Martino. "Sustainment of Military Operations by 5G and Cloud/Edge Technologies." In *International Conference on Advanced Information Networking and Applications*, pp. 70-79. Cham: Springer International Publishing, 2023.

Shahid, Huniya, Munam Ali Shah, Ahmad Almogren, Hasan Ali Khattak, Ikram Ud Din, Neeraj Kumar, and Carsten Maple. "Machine learning-based mist computing enabled internet of battlefield things." *ACM Transactions on Internet Technology (TOIT)* 21, no. 4 (2021): 1-26.

Sharma, Jahanvi, Anju Sangwan, and Rishi Pal Singh. "A review on evolving domains of Internet of Things: Architecture, applications, and technical challenges." *International Journal of Communication Systems* 36, no. 18 (2023): e5613.

Thiele, Ralph. "Nineteen Technologies in Focus." *Hybrid Warfare: Future and Technologies* (2021): 71-123.

Tyagi, Amit Kumar. *Internet of Things Theory and Practice: Build Smarter Projects to Explore the IoT Architecture and Applications (English Edition)*. BPB Publications, 2022.

Wijethilaka, Shalitha, and Madhusanka Liyanage. "Survey on network slicing for Internet of Things realization in 5G networks." *IEEE Communications Surveys & Tutorials* 23, no. 2 (2021): 957-994.

THE VAST EXPANSION OF 5G NETWORK AND INTERNET OF THINGS (IOT) – SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM

By LT KOL MOHD RIZAM BIN ZULKIFLI
ROYAL ENGINEER REGIMENT

INTRODUCTION

Recently, wireless technologies have been growing actively all around the world. In the context of wireless technology, fifth generation (5G) technology has become a most challenging and interesting topic in wireless research. The Internet of Things (IoT) in the 5G system will be a game changer in the future generation. It will open a door for new wireless architecture and smart services. Recent mobile network LTE (4G) will not be sufficient and efficient to meet the demands of multiple device connectivity and high data rate, more bandwidth, low latency quality of service, and low interference.

Wireless communications with high-speed internet connectivity and higher data rates are in high demand in the everywhere in the world and are an important factor in smart economic development and digitization of society. The existing wireless technologies, such as 3G and 4G, cannot meet the demand of fifth generation (5G) wireless requirements, and they cannot be used for the low-power wide-area (LPWA technology and long-distance communication.

5G wireless technologies in IoT are expected to use the unlicensed or unused spectrum band and it can only be easily accessed through the low-power wide-area networks (LPWANs), such as SigFox, LoRa, WiFi, ZigBee, and NB-IoT. This kind of smart technology provides enormous demand in the future communication system which will be fast and will include more connected devices that are normally supported in combined networks called heterogeneous networks (HetNets). It uses small base stations comprising femtocells, picocells, mm-wave technologies, and multiple-input multiple-output (MIMO) antennas.

It has a significant impact on people's daily lives. To design and deploy 5G IoT, the concept of 5G requirements and its feasible technologies should be clearly investigated. To have the generalized 5G infrastructure, the development with respect to architecture, the enabling technologies and their challenges as well as security measures should be known first. 5G IoT deployment will generate a

diverse form of traffic, reliability, bit rates, energy consumption, and security and privacy. The key motivation for developing IoT over 5G cellular networks is predicted, and a massive number of devices are expected to be deployed, which requires significant data rates.

5G NETWORK AND INTERNET OF THINGS (IOT)

5G internet refers to the 5th generation of mobile network technology, which succeeds the previous generations of mobile networks, including 4G (LTE or Long-Term Evolution) and 3G. It represents a significant advancement in wireless communications, offering higher data speeds, lower latency, increased capacity and enhanced connectivity compared to its predecessors. Here are some key features and characteristics of 5G internet: High Data Speeds: One of the primary benefits of 5G is its capability to deliver much faster data speeds compared to 4G LTE. While 4G LTE typically offers peak download speeds of several hundred megabits per second (Mbps), 5G has the potential to achieve multi gigabits per second (Gbps) download speeds. This enables faster downloads, smoother streaming of high-definition video, and improved performance for bandwidth-intensive applications. Low Latency: 5G networks promise significantly lower latency, or the time it takes for data to travel between devices and servers. While 4G LTE networks typically have latency in the range of tens of milliseconds, 5G aims to reduce latency to just a few milliseconds or even less.

This low latency is crucial for applications requiring real-time responsiveness, such as online gaming, virtual reality (VR), augmented reality (AR), and autonomous vehicles. Increased Capacity and Connectivity: 5G networks are designed to support a massive increase in the number of connected devices and simultaneous connections. This is essential to accommodate the growing number of IoT devices, smart sensors, and other connected devices that require reliable and high-speed internet connectivity. 5G networks use advanced technologies such as massive MIMO (Multiple Input Multiple Output) antenna and beam forming to increase network capacity and improve spectral efficiency. Improved Reliability and Coverage: 5G networks aim to provide more robust and reliable coverage, including in dense urban areas and indoors. While initial deployments may focus on densely populated urban areas, efforts are underway to expand 5G coverage to suburban and rural areas as well. Advanced antenna technologies, small cells, and network densification techniques are being used to improve coverage and overcome obstacles such as building penetration and signal interference. Enabler for Next-Generation Technologies: 5G is expected to be a key enabler for a wide

range of next-generation technologies and applications, including the IoT, smart cities, connected vehicles, telemedicine, industrial automation, and immersive multimedia experiences. Its high-speed, low-latency, and high-reliability characteristics make it suitable for supporting these advanced use cases and driving innovation across various industries.

While the concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is ushering in a new reality for the “Internet of Things’’. IoT promises to usher in a revolutionary, fully interconnected “smart” world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the Internet of Things as a ubiquitous array of devices bound to the Internet might fundamentally change how people think about what it means to be “online”. While the potential ramifications are significant, a number of potential challenges may stand in the way of this vision particularly in the areas of security; privacy; interoperability and standards; legal, regulatory, and rights issues; and the inclusion of emerging economies. The Internet of Things involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders. The Internet of Things is happening now, and there is a need to address its challenges and maximize its benefits while reducing its risks. Today, the IoT has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items.

FUTURE SOLDIER SYSTEM

“Future Soldier System is a concept of how the future Soldier might be equipped. This concept is not a doctrine, nor is it intended to answer every question raised about warfare in future”.

Future Soldier 2030 Initiative
U.S. Army RDECOM

The Future Soldier System (FSS) can be defining as soldier capabilities enhancement in a situation relating advancement and development. By definition, FSS is integration combat capability to each soldier to enhance their efficiency and effective. Purposely, to double up strength dan readiness when deploy to the battlefield in parallel with command structure for an organization.

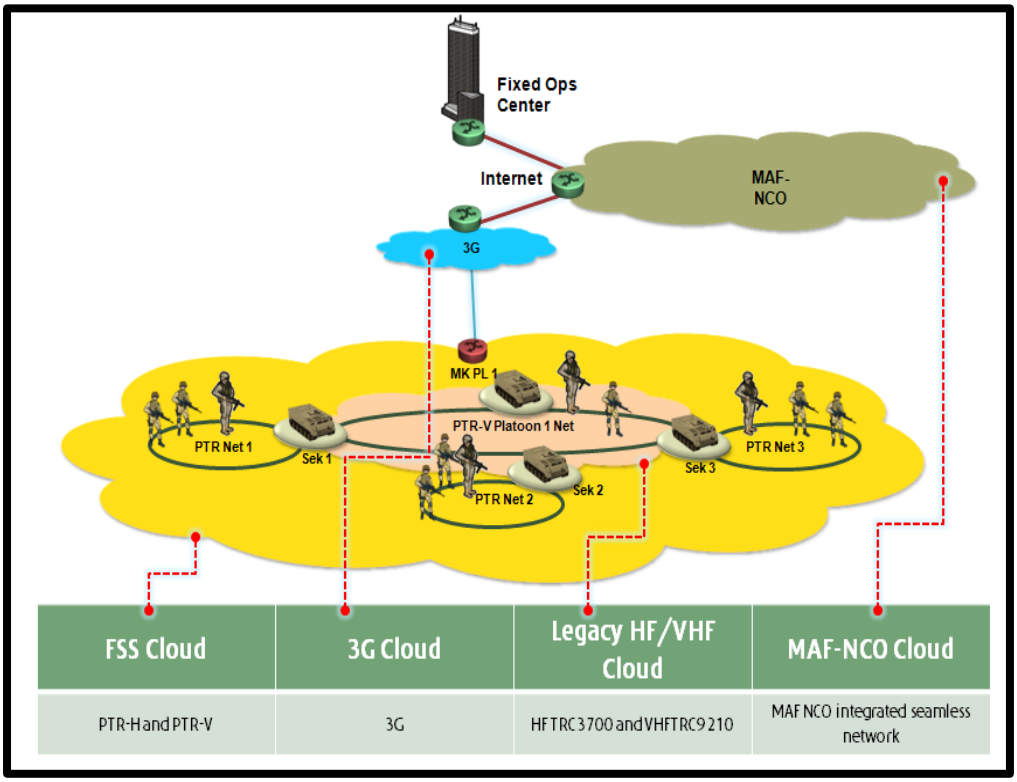

Figure 1: Future Soldier Network

Few examples of development FSS programmes by several countries; United Kingdom. Future Infantry Soldier Technology (FIST), 2003, Thales Defence Limited and Gen Dynamic. France. *Fantassin a Equipment et Liaisons Integres* (FELIN), 1995, Sagem. Australia. Land 125 Soldier Combat System, 1994, Wundurra. Germany. *Infanterist der Zukunft* (GLADIUS), 1996, *Rheinmetall* EADS. Singapore. Advance Combat Man System (ACMS), 1998, Singapore Tech. Italy. *Soldato Futuro*, 1996, Salex. USA. Land Warrior, 1994 Gen Dynamic Thales & Rockwell Collins + Raytheon. Web Warrior. Future Soldier Initiative, 2030. The Future Integrated Soldier Technology (FIST) is a project by the British Army which aims to enhance the infantry's combat effectiveness in the 21st century as part of the Future Soldier project. The contract was awarded to Thales in March 2003. The goal is to integrate a modular system of all equipment, weapons and their sighting systems, radios that the individual soldier carries or uses, in order to increase their overall effectiveness on the battlefield.

The future infantry soldier technology (FIST) programme is being managed by the dismounted close combat integrated project team at the UK Ministry of Defence Procurement Agency at Abbey Wood, Bristol. Thales UK was selected in March 2003 for the

assessment phase of the FIST programme. The first major experimental trial for the FIST project under the assessment phase took place in January 2005 at the army's Salisbury Plain training area. 70 soldiers took part and each soldier was equipped with experimental systems including 'off the shelf' radios, computers, GPS, weapon sights and cameras. Effectiveness was compared with soldiers equipped with conventional infantry systems. Trials data has been used to inform design decisions for the development of the FIST V2 system, which began trials in October 2005.

The FIST programme covers the development of all areas of technology for the dismounted infantry soldier and emphasises the integration of systems. The FIST system will provide the soldier with improved situational awareness, lethality and survivability. The systems will be assessed on a measure of improved capability and on soldier friendliness with ease and comfort of operation. The five main areas of capability are identified as C4I (command, control, communications, computers and intelligence), lethality (weapons and sights), mobility (navigation, size and weight of equipment), survivability (clothing, stealth, body armour) and sustainability (logistical considerations). It is not envisaged that each infantry soldier will be issued with a FIST system. The unit commander will specify the FIST systems tailored to the operational and mission requirements.

A main strategy of the FIST programme is that the infantry soldier is a key element of the UK's network-enabled military force. The FIST soldier's communications system provides communication up to company level. Above company level, communication is via the Bowman integrated combat radio system. The soldier will have a small encrypted radio that operates over a line-of-sight, short range to other members of his unit. The patrol leader's radio will communicate with the forward operating base. The network system will reroute automatically to allow continuity of operation when a communications link is broken, for example when a soldier moves over a hill or ridge. Voice and data communications can be relayed to the soldier directly or via drone relay links from headquarters, which have downloaded battlefield commands, information and images from forward observers, unmanned air vehicles, remote sensors and other airborne or satellite surveillance assets. The soldier will have a global positioning system, a dead reckoner and map displays to increase his situational awareness. The use of helmet displays, wrist-mounted displays, hand-held and laptop computers and communications systems will be considered.

While in French Army, the CSS was started in between 1997 and 2000, the French infantry combat system or *Fantassin a Equipment et Liaisons Integres* (FELIN) programme was in its demonstration phase, focusing primarily on: communications, observation (day and night, by trying to increase range), protection (detectability: visual, acoustic and electromagnetic, protection against attack), power/energy and mobility (system weight, ergonomics, location and navigation aid). During the first half of 2000, several operational trials were conducted, notably engagements between groups (one equipped with some of the FELIN features, one without). The trials were successful, as the group equipped with the new features was significantly more efficient, even though it was carrying earlier versions of the system which had not been optimised in weight. In 2001, the definition phase of the programme started. Engineering teams re-thought every step and system, putting aside all the previously tested demonstrators and updating the systems to the state of the art of their respective technologies. After several years of development and trials, the programme is now reaching completion. The first orders have been signed and the first deliveries should have happened in 2007. In November 2009, 22,588 FELIN systems had been ordered. The system was first deployed on the front-line on 7 September 2010 with the 1st Line Infantry Regiment in the Surobi District, which was occupied by the French forces in Afghanistan.

Australia's soldier modernisation program, LAND 125 Soldier Combat System (Project WUNDURRA). Some key parameters for Project WUNDURRA are:

- The Soldier Combat System will be developed as a 'system'. In the past, the soldier has been required to individually make the compromises between pieces of equipment, often individually excellent, that are incompatible. The aim of Project WUNDURRA is to 'export' this problem from the overburdened combat soldier by addressing it during the design of the system. This will leave the soldier free to employ the system optimally on the battlefield.

- The understanding of the boundaries of the Soldier Combat System have evolved from the individual, through the smallest team, the section (squad), to now encompass the fighting elements of the rifle company, including habitual attachments such as forward observers.

- The Soldier Combat System must be broadly deployable in a wide variety of terrain, and by the full range of in-service or projected transport systems.

- Project WUNDURRA is a command and control project, than a weapon, sensor or combat equipment project. The WUNDURRA Soldier Combat System represents the way the individual soldier, section and platoon are linked to the digital battlefield.

While in Italian Army, the future soldier program was projected purposely increasing the operational efficiency of the smaller units by enhancing and integrating the main capacity areas of the dismounted fighter: lethality, survival, Command and Control, mobility and autonomy. This increase was the result of the NATO orientations in the sector, in order to give the individual fighters and the units a complete interoperability both inter-forces and multinational employment contexts. The development of innovative individual equipment, completely integrated, led to the realization of a "soldier system": it is based on the synergy man-equipment and is suitable for carrying out the tasks arising from changes in the international scenario. The system is characterized by modularity, flexibility and expandability so that it is efficaciously configurable according to the different employment situations and gradually upgradeable in view of technologic innovations in different sectors.

Its integration in the mechanized Command and Control system will allow to involve the units in the digitalization process of the new operational contexts. The "Future Soldier" aims to increase the efficiency of the five main capacity areas. In particular:

- The increase of the practicality arises from the new technologies that concern weapons and munitions as well as the tools for the target acquisition, the blast control, the communication and the information management. The individual weapon is a 5.56 mm calibre weapon that can mount a 40mm grenade launcher and it supports a multi-function module for the target acquisition and the management of efficient, selective and targeted blast (night and day). The weapon includes a thermal camera along with a TV camera that operate on the same channel and a pointing optical sight with three enlargements, a pointing sight for the instinctive shooting and two laser sights (one for the visible range and one for the infrared range. The data can be exported wirelessly.

- The survival is increased thanks to the integration of the technologies that ensure the protection against the threats of the modern operational scenario. In this context some protection equipment has been developed: ballistic, anti-NBC, anti-laser, climatic, protection from blast and observation.

- The command and control systems have been strengthened by integrating and developing the communication systems along with the sensors, in order to improve the global perception that the fighter has of the situation and his ability to act effectively. The system has got specific data submitters, a personal computer, a GPS and a radio. The "Future Soldier" program is integrated in the other digitalization components of the manoeuvre space (SIACCON and SICCONA).

- The autonomy has been improved by using innovative materials, especially in the electric power system.

- The mobility has been increased by optimizing the ergonomics of the materials, the equipment weight and the optimization of the transported load. Moreover, it has been intensified the movement ability of the soldier in nightscape as well as the consciousness of the situation.

The C2 Subsystem permits to perform the Command and Control (C2) functions, helping the soldier to known the battlefield and facilitate the exchange of information and orders in the Command chain. In particular, the subsystem represents a responsible element of the "future Soldier" system for the collection, the management and the presentation of the Command and Control information; that information is transmitted internally and externally to the team through the "Communication" Subsystem, providing for a continuous exchange of the tactical situation at all levels of the Command chain. The Wearable Personal Computer (WPC) is the platform that supports the Command and Control activities of the "future Soldier" system; through specific software and hardware, it implements the functionality of collection, procession, transfer and presentation of information. The Global Position System (GPS) is the sensor that provides information about the soldiers' position to the WPC. The Targets Acquisition Unit (UAB) is a "hand held" device supplied to the team Commander that acquires and localizes the targets day and night. The UAB localizes a target measuring the azimuth coordinates and the elevation from the position of observation and so the distance of the observed target. Moreover, it can acquire the digital image of the target, both IR and TV HD. The

UAB permits also to transmit data by wireless or by cable directly connected to it.

The 3rd Generation Singapore Armed Forces (SAF) is progressively equipping tactical units with network capabilities, vital for ensuring mission success. One of these is the Advanced Combat Man System (ACMS) for the soldiers. In a seven-man section, the two team leaders and section commander will be equipped with the ACMS. The components of the ACMS are:

- **Personal Radio**. The radio enables soldiers to share information, in the form of data and voice, with other soldiers. It has a built-in Global Positioning System (GPS) that helps the soldier's command headquarters to track his location and that of friendly forces.

- **Communication Keypad**. This portable keypad, designed for easy data input, also has hotkey buttons such "On-Contact" and "Call-For-Medic" to enable quick updates of the team's status to the command headquarters, and request assistance from nearby forces at the push of a button.

- **Portable Computer**. The brain of the ACMS, the portable computer processes data collected by sensors, GPS, other ACMSs and user input to provide real-time information updates on the battlefield.

- **Head-mounted display (HMD)**. The HMD can switch its displays from a digital map to satellite images of the terrain to videos captured by the various sensors. Through the HMD, soldiers can see locations of targets and friendly forces which are plotted on the digital map.

- **Weapon Interactor**. The section commander will also have an additional camera attached to his SAR 21, so that he can capture and send back images to the command headquarters through the quick buttons on the handguard. The sensor also allows him to survey and fire around corners without exposing himself.

In addition to the ACMS, soldiers are equipped with remote sensors such as a surveillance ball, a remote-control surveillance car and a key-hole sensor. With the ACMS and remote sensors, soldiers can track the positions of friendly and hostile forces, effectively engage their targets and concentrate efforts at critical locations. Such

information sharing allows the soldiers to navigate accurately through the terrain and avoid known danger areas. By feeding images back to the command headquarters, soldiers are not only fighters, but also sensors on the ground. They enable commanders to deploy firepower effectively at hostile locations and enhance battlefield coordination. Section commanders are also empowered to call for fire support and for the command headquarters to utilise higher command resources such as artillery, air assets and sensors, to enhance the lethality and situation awareness of their units. With the integrated information flow, the seven-man section in the battlefield can now tap into the wider resources of the battalion. This significantly increases the lethality, situational awareness and survivability of the individual soldier.

Lastly, the concept of FSS in Malaysian Army emphasized in the following characteristic. The main factor to success in military operation is completing the soldier with sophisticated fighting system with higher technology and integrated system. This includes double up the combat level purposely to increase the capabilities of the soldier in the battlefield. By these efforts will directly increase the situational awareness in the battlefield spectrum in the contemporary warfare era which is uncertainty and become more complex. The threat and the evolution of warfare and the initiative by the adversary exploiting the development of the technology make the warfare become more complex and neighbouring countries also under progress to upgrading their soldier capabilities with latest technology including weaponry system, communication and survivability.

The vast expansion of 5G network and IoT application directly will facilitate the effective of the army FSS program. Here is the logic that supporting the above claimant: The higher data speeds compare to the previous version of wireless communication, capable to deliver much data with higher speed will enables faster downloads, smoother streaming of high-definition video especially live stream from the battlefield to the operation centre. Secondly, lower latency is another characteristic that requirement for battlefield that in the urban area or thick jungle area. The characteristic offering the time it takes for data to travel between connected devices and servers shorter than the predecessor network generation. Thirdly, the third advantage of 5G network is increased capacity and connectivity: 5G networks are designed to support a massive increase in the number of connected devices and simultaneous connections.

5G networks is essential to accommodate the growing number of IoT devices, smart sensors, and other connected devices that require reliable and high-speed internet connectivity. It uses advanced

technologies such as massive MIMO antenna and beam forming to increase network capacity and improve spectral efficiency. Improved Reliability and Coverage: 5G networks aim to provide more robust and reliable coverage, including in dense urban areas and indoors. Advanced antenna technologies, small cells, and network densification techniques are being used to improve coverage and overcome obstacles such as building penetration and signal interference.

Five main capabilities in FSS is situational awareness, force protection, lethality, mobility and sustainability. To achieve situational awareness capability, it is main requirement is the effective and efficient communication to each level of the organization, surveillance system in battlefield transmit two ways communication transmitted with minimum interruption, real time or live recording video, battlefield data collection and chain of command.

CONCLUSION

The vision and mission of 5G network and IoT were to connect multiple numbers of devices within the same network architecture. Many advanced applications in 5G wireless application such as smart cities, smart factories, smart agriculture and smart healthcare lead to IoT revolution. Such huge ranges of smart applications are expected to be supported with high-speed massive connectivity under the same roof of 5G wireless communication. Meanwhile, the FSS programs with several name and branding name, however the main objective of the system is to connect the means (C4I – Command, Control, Communication, Computers and Intelligence) and ways (Man + Machine consist of 5G network, IoT and Systems) to achieve aims (increasing capabilities to win the war).

The crucial important relating for the FSS is command and control element which is communication and internet network. Equipment such as Personal Radio. The radio enables soldiers to share information, in the form of data and voice. Global Positioning System (GPS) that helps command headquarters to track soldier location and that of friendly forces. Portable Computer. The brain, processes data collected by sensors, GPS and user input to provide real-time information updates on the battlefield. Head-mounted display (HMD) can switch its displays from a digital map to satellite images of the terrain to videos captured by the various sensors. Through the HMD, soldiers can see locations of targets and friendly forces which are plotted on the digital map. Weapon Interactor. Also have an additional camera attached to weapon, to capture and send back images to the command headquarters. The sensor also allows to

survey and fire around corners without exposing himself. Remote Sensors such as a surveillance ball, a remote control surveillance car and a key hole sensor. Soldiers can track the positions of friendly and hostile forces, effectively engage their targets and concentrate efforts at critical locations.

Such information sharing allows the soldiers to navigate accurately through the terrain and avoid known danger areas. By feeding images back to the command headquarters, soldiers are not only fighters, but also sensors on the ground. They enable commanders to deploy firepower effectively at hostile locations and enhance battlefield coordination. Section commanders are also empowered to call for fire support and for the command headquarters to utilise higher command resources such as artillery, air assets and sensors, to enhance the lethality and situation awareness of their units. With the integrated information flow, the seven-man section in the battlefield can now tap into the wider resources of the battalion. This significantly increases the lethality, situational awareness and survivability of the individual soldier. Without proper connection and vast expansion 5G network and IoT, the effectiveness of FSS program unable to achieve its objective in effective and efficiently.

REFERENCES

Army 4nextG Edisi 1.1, (2021), Teras Pembangunan Keupayaan Masa Hadapan, Markas Tentera Darat, Wisma Pertahanan.

Army Technology (2006), Future Infantry Soldier Technology System (FIST),https://www.army-technology.com/projects/fist/?cfview&cf-closed

Army Technology (2006), Fantassin a Equipment et Liaisons Integres (FELIN) – Future Infantry Soldier System. https://www.army-technology.com/projects/felin/

Defence White Paper (2020), A Secure, Sovereign and Prosperous Malaysia, Ministry of Defence, Malaysia National Library.

European Defence Review (2009), Soldier systems evolution by Rheinmetall https://www.edrmagazine.eu/soldier-systemsevolution-by-rheinmetall

K. Rose, S. Elridge and L. Chapin (2015); Internet Society; The Internet of Things: An Overview: Understanding the Issue and Challenges of a More Connected World.

L. Chettri., & R.Bera. (2020). A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems, IEE Internet of Things Journal, Vol. 7 No.1

Singapore Ministry of Defence, (2012), Advanced Combat Man System,https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latestreleases/

W. Hobbs, D. Goyne, N.J. Curtis (2000), LAND 125 Soldier Combat System (Project WUNDURRA) Australia's Soldier Modernisation Program: https://www.researchgate.net/publication

THE VAST EXPANSION OF 5G NETWORK AND INTERNET OF THINGS (IOT) – SIGNIFICANCE OF THE ARMY FUTURE SOLDIER SYSTEM

By LT KOL AHMAD ROSDI BIN RAHIM
ROYAL ELECTRICAL & MECHANICAL ENGINEER CORPS

INTRODUCTION

The 5G is all about use cases, and it might assist enhance operational efficiency. 5G can be substantially faster than 4G, with peak data speeds of up to 20 Gigabits per second (Gbps) and average transmission rates of 100 Mbps or more. 5G has higher capacity than 4G. 5G is intended to enable a 100 times improvement in traffic capacity and network efficiency. 5G has a lower latency than 4G. The prospect of building a distinct 5G cloud that will only be accessible to the Armed Forces, as well as security issues, should be investigated. A dedicated 5G network, along with 5G cloud and data centres, might enable paperless and automated procedures that can be managed remotely. 5G is all about use cases, and it might help improve operational efficiency. The possibility of creating a separate 5G cloud solely available to the Armed Forces, as well as security concerns, should be studied.

A dedicated 5G network, together with 5G cloud and data centres, may allow paperless and automated operations that can be administered remotely. In addition, future troops should be encouraged to participate in the defence white paper and to utilise 5G technology. Military operations increasingly rely on battlefield sensor systems and other reconnaissance and surveillance technology. Networked battlefield and military equipment deployed in the operational theatre may be the best solution, as long as they are designed and configured to gather all data generated in their environment. These devices are continually communicating the data they collect with one another and a central storage and processing server. Furthermore, future warriors should be encouraged to engage in the defence white paper and use 5G technologies. Military operations are increasingly reliant on battlefield sensor systems and other reconnaissance and surveillance technologies. Networked battlefield and military equipment deployed in the operating theatre may be the ideal answer, if they are constructed and set to collect all data created in their surroundings. These devices are constantly sending the data they gather to one another as well as a central storage and processing server.

Digitalisation has a tremendous impact on our everyday lives, especially in the military sector. For example, the European Union and its member states have recently emphasised the creation of digital strategies and frameworks. Almost all of these frameworks aim to create smart cities, landscapes, and ecosystems. In all of these cases, Internet of Things (IoT) devices and systems are unavoidable, and their widespread use has a substantial impact on our everyday lives. IoT devices constantly monitor their environment, collect data, and share it with other system components and users depending on predefined tasks. As these devices acquire a large amount of data from their surroundings, they must do so in a place with adequate storage capacity and if necessary, computing power.

A cloud environment is the most effective solution for this. Hence, the combination of IoT with cloud computing is nicknamed the Cloud of Things (CoT). These technologies appear in civilian contexts and are increasingly being used in military operations, where they may help soldiers to track the operational environment in real time and make decisions as quickly as possible. In this context, some research has been published that covers the basic requirements and potential solutions for using IoT devices in military environments. IoT devices used in combat settings are known as the Internet of Battlefield Things (IoBT) or the Internet of Military Things (IoMT), depending on the operational region and level. If these devices are connected to the cloud, then we will talk about Cloud of Battlefield Things (CoBT) and Cloud of Military Things (CoMT) solutions.

In this essay, I will explain the reliability of 5G for various levels of military IoT devices in the cloud, as well as the possible future use of 5G technology to improve communication environments. To achieve the goal of developing future soldier preparation, this article will undertake a comparative assessment of relevant global academic research and technical reports on the issue, based on a review of the majority of research findings.

CRITICAL REQUIREMENT OF CLOUD OF BATTLEFIELD THINGS FOR FUTURE SOLDIER

To understand the concepts of the Cloud of Battlefield Things and the Cloud of Military Things, we must first separate the Internet of Battlefield Things from the Internet of Military Things. The IoBT is a network of devices that communicate in two directions and can transmit operational battlefield data, information, and situational awareness to other devices in near real time, utilising technology such as databases, file sharing, and cloud-based systems to support tactical decision-

making. In contrast, the IoMT is a higher-level system that provides information not just from the battlefield but also from a far larger variety of assets. Strategic assets deployed include long-range unmanned aerial vehicles (UAVs), surveillance planes, and satellites outfitted with a variety of cameras.

As a result, the IoMT is a network of devices and systems that interact with one another in both directions. They may communicate strategic data, information, and operational situational awareness created during operations to other devices and exchange it in near real-time utilising technologies such as databases, file sharing, and cloud-based systems to aid strategic decision-making. The above statement indicates that, as stated in the introduction, the fundamental goal of IoT tools in an operational environment is to provide real-time operational situational awareness and decision-making assistance. As a result, a massive amount of data is required, which must always be available at the proper time, location, and format.

Cloud computing is an excellent solution for this. A cloud environment offers plenty of storage space to retain the vast volumes of data collected, and its high processing capabilities enables faster data analysis. It is the most effective option for connecting regularly used IoT devices. In the military, the integration of battlefield IoT devices into a cloud environment is known as the Cloud of Battlefield Things. A CoBT is a system that integrates networked battlefield equipment into a shared cloud environment, allowing authorised personnel to access acquired battlefield information at the appropriate time, location, and format, resulting in a real-time operational situational picture.

As a result, the system can help achieve information dominance, making it easier to carry out operations successfully. The strategic-level system is referred to as the Cloud of Military Things. It connects networked military devices to a shared cloud environment, making gathered information available to authorised individuals at the right time, place, and format, resulting in a real-time operational situational picture at all levels of operation. As a result, the system can help achieve information dominance, making it easier to carry out operations successfully.

The CoMT and CoBT have layered designs, and this article discusses communication options between them. The conceptual framework handles the core issue with various sensing equipment (sensors, sonars, cameras, and radars). The second issue is the cloud layer itself, which houses the storage and computing capability, and the

third is the access layer, which allows users to access cloud-stored data through applications. Finally, the cloud issue encompasses the cloud issue of CoBT, which in the case of CoMT relates to the Multi-Access Edge Computing solution. Immediate information transmission is vital in military applications, hence low latency systems, which assess data at a nearby site, are required.

In the case of IoMT, this is facilitated by the Multi-access Edge Computing (MEC) solution used in IoBT, which is an autonomous processing unit located at the network's edge. This solution is a vital component of 5G-based infrastructures such as transportation infrastructure, where low latency is required for self-driving cars, unexpected traffic information, and so on. The data is handled directly via the radio access network (RAN) without the intervention of the MEC's central system, resulting in just aggregated data being supplied to the central network, in this example regarding the CoMT.

5G is primarily driven by customer demand, owing to the growth of IoT and M2M connection. 4G provides 100,000 connections per square kilometre, peak data rates of 1 Gbps, data volumes of up to 7.2 Exabytes per month, and a latency of 10 msec. 5G will provide one million connections per square kilometre, peak data rates of 20 Gbps, data volumes of up to 50 Exabytes per month, and latency of less than 1 millisecond. The 5G network is intended to support applications and services of diverse latency, dependability, and capacity. 5G is one of several services that go beyond better internet rates. The three main 5G use cases are Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (mMTC), and Ultra-reliable and Low Latency Communications (uRLLC). The breadth of services provided is mostly a trade-off between the three parties. At the low end of the services, there is an application for an embedded, underwater, or subterranean sensor whose battery must last for a long period, up to 10 years or more, while being incredibly affordable. On the opposite extreme, we have uRLLC, which is used in critical applications like as autonomous cars.

Currently, even if each user has created a use case for the spectrum allocated to their own businesses, the nation may consider utilising cutting-edge spectrum sharing solutions. One of them is Licenced Spectrum Access (LSA), which grants other licensees access to bands already in use by one or more incumbents. LSA is a concept for dynamically distributing this bandwidth anytime it is underutilised by present customers. There are methods for economically employing the spectrum commercially during non-operational periods, assuming that it is made available to the government for use during operations. The

worldwide mobile industry and terrestrial communications are quickly expanding, creating a strong demand for spectrum. There are substantial trade-offs between the broadcast, mobile, and space divisions.

FROM VULNERABLE TO OPPORTUNITY OF NETWORK SLICING

Network slicing technology is already available for 5G networks, enabling for the logical and physical separation of network resources to offer service customisation, isolation, and maintenance, as well as multi-tenancy on a common physical network infrastructure. The technology supports multi-tenancy, enhanced network coverage, and provides a solid solution for infrastructure and cloud service providers. Network slicing can be configured on a temporary or permanent basis, for a single user or group, or for various services. The primary goal of the 5G ecosystem is to enable comprehensive mobility and continuous availability in all scenarios. Thus, it is suited for use in military environments. Thus, 5G technology with network slicing enables the following capabilities:

- Enhanced broadband connection everywhere: offering high bandwidth access across the whole operational territory, assuring connectivity of all end devices in the area.

- High user mobility enables broadband support for fast-moving vehicles, such as military convoys on the go.

- The Massive Internet of Things enables broadband connectivity to extraordinarily dense networks of sensors and actuators, including long-range and low-power devices.

- Extreme real-time communication provides ultra-low latency connectivity, such as for IoBT devices.

- Extremely dependable communication with extremely low latency, as well as stable and accessible network connectivity to enable autonomous weapon systems.

- Mission-critical communications that provide connectivity in the case of disasters and crises, as well as the ability to manage abrupt spikes in traffic while remaining resilient.

- ❖ Broadcaster-like service which giving network access to any service that enables, for example, the transmission of patches delivered to firmware upgrades or repair security vulnerabilities.

- ❖ Simple communication that establishes a network connection for producing, setting, and storing basic service information.

- ❖ Multiple connection allows deployed and operated smart devices to connect to the network via a variety of access mechanisms.

REAL PROSPECTS OF CRITICAL CAPABILITIES ADAPTING 5G

The 5G wireless technology aims to deliver more users with faster data speeds, more reliability and availability, ultralow latency, massive network capacity, and a more consistent user experience than previous generations of technology. The performance of 5G networks should be evaluated using three metrics: user bandwidth, device density, and latency. According to a true example, the International Telecommunication Union (ITU) has specified minimum values for these qualities in Recommendation ITU-R M.2083-0. This Recommendation establishes the framework and overall objectives for international mobile telecommunications (IMT) in 2020 and beyond, as well as the framework for its future development, which includes a wide range of capabilities related to intended use scenarios, as well as the continued development of existing IMT capabilities and the development of IMT-2020.

Furthermore, it identifies eight significant categories for capabilities, each with a target to aid in the development of 5G capabilities, known as the International Telecommunication Union's primary objectives for 5G development. These goals can also assist to develop communications capabilities that are now used in the military. 5G offers several benefits to military networks, particularly tactical networks, such as manageability, dynamic spectrum management, plentiful capacity, and low latency.

The standards framework developed by the 3rd Generation Partnership Project6 (3GPP) provides a solid foundation for this, outlining the critical criteria for developing 5G systems and networks. However, this development is separated into stages, with Release 17 scheduled for March 2022. As a result, the framework and standards specified therein will be applicable to all 5G networks, and military-

grade equipment and systems will be able to achieve the ITM-2020 triangle of requirements. The items described in the triangle of needs have the following characteristics:

❖ Enhanced mobile broadband (eMBB). This frequently comprises people-centric IMT services with high traffic bandwidth, high user density, and moderate to medium mobility needs. Its major function is to provide fixed wireless access (FWA) in areas without wired connectivity (usually in operational zones).

❖ Massive machine type communications (mMTC). These communication services are intended for Internet of Things (IoT) applications that employ a large number of connected devices with weak radio connection and require low throughput but significant data transfer capacity over time.

❖ Ultra-reliable and low latency communications (uRLLC). This communication service provides low throughput while also delivering low latency and high availability data services for applications that do not need high throughput but do require a solid connection in a mobile environment. Applications include near real-time human-machine or machine-machine interfaces, such as remote controls, as well as automatic and semi-automatic weapon control systems. These qualities imply that 5G can handle and link significantly more data than previous systems, allowing it to be used in a far greater range of applications, including a wide range of military missions. It is also far more sophisticated, making security a far greater problem than before. To do this, the following systems engineering goals must be met:

- Flat network architecture.
- Separation of the control plane and the data plane.
- All functions in a self-contained unit to support for cloud computing.
- Optimal resource utilisation for network slicing.
- High level coordination.

The 5G spectrum from 470 MHz onwards includes the sub-6GHz band and the millimetre wave border band, which is where we truly need the eMBB. The considerations on spectrum for 5G services deployment as per the NDCP 2018 are as follows:

- **Immediate**.
  - Announce 700 MHz, 3.5 GHz, 26 GHz and 28 GHz as 5G bands.
  - Wave bands be opened free for two years for trials and indigenous R&D.
- **Mid Term**.
  - Open 600 MHz, L Band, 31 GHz and 38 GHz bands for 5G.
  - 38 GHs (37.0 to 43.5 GHz) band be opened free for two years for indigenous R&D.
- **Long Term**.
  - Study 3600-3700 MHz band for meeting midlevel 5G spectrum requirements.

The most common question regarding smart cities is how sophisticated they are. These are analogous to Centres of greatness (C's of E), when it is hard to quantify what defines greatness. As a result, a datum level must be defined for a smart city. The communication needs for a smart city or smart cantonment must also be quantified. When 5G is adopted, it will create new revenue prospects. Globally, the number of active IoT connections is expected to reach 21.5 billion, with the Global IoT Market value projected at $1600 billion USD by 2024-25. For example, in India, M2M/IoT is expected to reach 5 billion connections by 2022.

Some of these commercially proven 5G applications may potentially be tailored to the Armed Forces' specific requirements. Security is a critical component of 5G, and 5G 19 addresses various security concerns, including Identity Management, Platform Security, Building Trustworthy Clouds, Data Integrity, Security Assurance, 5G Security, and IoT Security. The Armed Forces must ensure that they engage in all discussions around 5G security challenges, since if they do not communicate their specific security requirements, they will wind

up paying whatever security is provided. To the maximum extent feasible, the Armed Forces must preserve continuity in the person in charge of 5G and its security aspects, regardless of how many times he has worked in a given appointment during his service.

Civil Street has been home to telecom standards professionals for the past two decades. Countries who have converted their data into a standardised format that can be utilised to run an AI engine are ahead. While India, for example, has launched a project called the Digital Broadband Index of Readiness for multiple states, the Armed Forces may consider creating a Digital Index of Readiness for various formations within their separate services. Only when the armed forces have been digitised will they be able to crunch numbers and provide services. This is a specific field that requires consistency. The Armed Forces would benefit from forming a Special Team to monitor and train for future 5G technical events, as well as to assure technology continuity and sustainability.

A reference model for the 3GPP Release 15 framework, developed in 2018, describes the architecture of 5G systems. The 5G system design contains the following network functions (NF):

- 5G Next Generation NodeB (5G gNB).
- Access and Mobility Management Function (AMF).
- Authentication Server Function (AUSF).
- Centralized Unit (CU).
- Data Network (DN).
- Distributed Unit (DU).
- Network Exposure Function (NEF).
- Network Repository Function (NRF).
- Network Slice Selection Function (NSSF).
- New Radio (NR).
- Policy Control Function (PCF).
- Radio Access Network (RAN).
- Session Management Function (SMF).
- Unified Data Management (UDM).
- User Equipment (UE).
- User Plane Function (UPF).

The NCO team offered a number of systems for the Malaysian future soldier, including BSS, BMS, ADCNRS, and others, each with its own intra communication system. For a particular battlefield system application. Now that 5G is available, it can handle all of the connectivity requirements for various battle field applications. Due to the incredible speed and bandwidth afforded by 5G, the need for

separate intra-communication networks for each of these military applications may be reconsidered.

So the only element that has to be studied and debated here is that the frequency ranges in which 5G operates are now sub-6 GHz bands, often 3 GHz and higher, and the distances are becoming progressively short. This implies that a far greater number of base stations would be required in a certain region than the existing configuration. Domain specialists from the Army's Corps of Signals, as well as other Subject Matter Specialists (SMEs) from the other two services, will analyse how this dense BTS deployment will be carried out on the battlefield. The Army's Tactical Communication System (TCS) is now being evaluated, and a new communication system based on 5G may be considered for development. The Air Force-based technology looks to be well established and might benefit from an upgrade to 5G. When at sea, the Navy does not require mobile communications and instead relies on satellite communication to meet its demands. However, given the Army's tremendous need for sensors, communications, systems, and weapon platforms, 5G is the way to go. Domain specialists from the Royal Signal Corps may do a thorough investigation of how 5G might be utilised for peacetime and operational communications, among other things. 5G is the future, and 50 million gadgets will soon be connected through it.

When it comes to 5G spectrum, the technologies employed by the defence to deliver various services and purposes are not publicly available. When the same spectrum band is used for military and commercial purposes, a guard band is needed in the middle. This wastes a significant amount of spectrum that may have been better utilised if properly planned. If the military begins to employ the same set of commercially available technologies, there will be no waste of spectrum, and it will be used more effectively and efficiently.

Stakeholders from the Malaysian Armed Forces Headquarters must actively participate in various talks related to the finalisation of security standards to ensure that their concerns are addressed from the start. According to reports, special future development meetings are held on a regular basis to generate various telecom standards. An entity known as the 5G think tank should create 5G security rules to ensure that security is built into radios and network components from the beginning. Attendees include members of the military, security, police, marine, and other related departments.

While the Malaysian Armed Forces (MAF) may discuss security issues within the context of 5G, they will be represented at the top table where such decisions are made, making internal arguments considerably more valuable because they must be heard rather than answered. For example, Malaysia's Department of Transport is working hard to create and enforce 5G security requirements. Furthermore, because the Malaysian telecom industry is regulated, all businesses follow highly strict security measures. All telcos have SOPs and adhere to highly rigorous protocols, as seen by visits to the Airtel experience centre and the NOCC in NCR. Because of the strict organisational need of posting officers every 2-3 years, no officer in the MAF would be able to keep up with the rapid developments in the telecom business unless he is interested in the topic. As a result, the MAF may consider providing security services for its networks. The MAF also must ensure that they engage in all discussions around 5G security challenges, since if they do not communicate their specific security requirements, they will wind up paying whatever security is provided.

For the greatest extent feasible, the MAF must ensure that the individual in command of 5G and its security and communication components stay in place. Security as a service necessitates expertise in the Indian sector. Requirements SLAs can be signed with industry representatives, including parts from the 123 Cyber Security Act, and they will comply. 5G Recommendations for the Armed Forces. A few tips and proposals tailored to the Armed Forces are provided below:

- **Specify Critical Requirements (CR)**. Assess the demands of arms and services such as combat, combat support, combat service support, and static establishments for their service requirements.

- **Evaluating Critical Capabilities (CC)**. 5G is from MTC to uRLLC to evaluate how do these technologies relate to the demands and drones are used to deploy reconnaissance components.

- **Utilising Digitisation Aspects**. Use Network Function Virtualization (NFV) and SDN to customise the network to the specific needs of Armed Forces users and operational duties. Requires a high level of digitization and is especially useful for doing remote procedures.

- **Maximise Data for Sense Making**. Create a data repository that includes a common Armed Forces data interchange to allow Big Data Analytics for improving combat

effectiveness, projections, and response timings. Could be beneficial to the logistics corps.

❖ **Forming Esprit de Corps**. Form a Special Team to monitor, train, and participate in future technological events. Establish a working relationship with Malaysia's military sector to encourage mutual assistance. It will establish an armed forces ecosystem and agency to develop services for various users on Armed Forces networks, such as wireless devices and tiny yet sturdy form factors.

❖ **Enhancing Abroad the War Spectrum**. Rationalisation of multiple spectrum bands for access and backhaul to improve MBB coverage in a short time frame and deliver fibre-like capacity connection.

HOLISTIC STRATEGIC, OPERATIONAL AND TACTICAL LEVEL PLANNING FOR FUTURE SOLDIER

The MAF is now identifying potential security vulnerabilities to the country posed by the usage of fifth-generation (5G) cellular mobile technology, which must be embraced in the country. Thus, every new technology from overseas, particularly 5G, should be evaluated to establish whether it is acceptable for usage in the country. However, we cannot just emulate other countries in terms of adopting new technology. Not all technologies are beneficial. We are convinced that the Ministry of Communications and Multimedia is undertaking research on this, and the MAF has its own methods for studying new technologies. Among the items that needed consideration, such as 5G, was handling new technology if its usage contained components of cyber-attacks and obtaining sensitive information. In order to avoid such hazards, we must take adequate precautions; while to strengthen the credibility of our future soldiers, we must be wary of the 5G technology that China is now developing, as it has the potential to trigger cyber and digital security threats against the country.

VITAL REQUIREMENT OF SATELLITE COMMUNICATION CAPABILITIES

The data processed and stored in the CoBT may also be transported to the CoMT via 5G networks, however due to its large size, multiple communication methods are usually used. 5G non-terrestrial networks expand the use of 5G NR technology and its benefits for non-terrestrial platforms. The on-air 5G NR architecture enables mobile network operators to provide 5G-based services in locations where

terrestrial networks are unavailable or long distances must be covered. These solutions provide the essential services without requiring any intermediate protocols or technological adjustments. 5G NTNs can be supplied via satellite, High Altitude Platform Stations (HAPS), or any other aircraft capable of carrying the NTN payload.

Regarding the convergence of satellite and terrestrial networks, satellite-terrestrial networks can be implemented in a variety of ways, including general, software-defined network (SDN), information-centric network (ICN), and content delivery networks (CDN)-based. 5G networks applied in CoBT environments have numerous benefits, but they also raise a number of security concerns. Providing adequate security is also a major challenge for IoT devices used in military operations. From an operational safety aspect, it is vital to guarantee the safety of the equipment or systems used, since damage to the equipment or systems can have a substantial impact on the entire operation and potentially endanger the lives of many personnel. CoBT thinks that vulnerabilities or threats at all levels of the system might have a negative impact on operations, not only on user devices.

CONCLUSION

New types of private sector communications technology and information services solutions offer opportunities for military applications that can considerably improve the efficacy of military operations. Connecting IoT devices, which are becoming more ubiquitous in the military environment, to the cloud, for example, may provide real-time operational situational awareness in order to achieve and maintain information supremacy, hence contributing to successful operations. The isolated 5G technology described in this study provides a strong foundation for this, assuring complete data security for military applications by separating military networks from public networks.

This essay has thus offered a satisfactory solution to various research concerns by proving that 5G technology may be used to build a durable, trustworthy, high bandwidth system with low network latency that can be deployed on a range of combat platforms. Furthermore, a private 5G network enables high mobility, dependable, and secure communications for battle command and control administration, as well as other support functions. As a result, we can say that we provided a satisfactory answer to the other issue, albeit it is important to highlight that private network deployment is associated with high installation costs and a heavy workload for the operating people. Network slicing can be an excellent alternative if a separate 5G private network is not

required. However, a logical layer may be built by virtualizing the present public network to create a more suited environment for military operations. This virtualized network enables the integration and deployment of battlefield and military IoT devices in cloud architecture. The built system will meet all of the requirements for any technical solution used in an operational context. Overall, it determined that it has successfully identified basic security vulnerabilities for various components of 5G technology in military settings, which might have a substantial impact on overall system operation.

In a recent article, many academics proposed strategies to defend Cloud of Things solutions, offering technical and technological solutions that may aid in the creation and maintenance of a secure network in a military cloud environment. However, not all innovations, such as 5G, will benefit the armed forces, since hybrid warfare and future warfare industries demonstrate rapid development in the use of new and cutting-edge technology. Throughout the history of warfare, superior and cutting-edge technologies have also increased the possibility of catastrophic technology. The vulnerability may stem from a disparity between social or public specifications and military specifications. The adoption of 5G in the armed forces, so-called future soldiers, necessitates extensive study and military specification certification.

REFERENCES

Abdul Rahim Andul Rahman, Saharudin Ab Rashid, Noor Raihan Ab Hamid (2018), *Agility and Digitalization Compentency in Logistics 4.0 in Military Setting: The Challenge Risks and Oppoturnities*, Asian Journal of Social Science Research, Vol. 1 (2)

Anshu Bhardwaj (2020), *5G for Military Communications*, Procedia Computer Science, Vol. 171, pp: 2665-2674

Arun Teja Polcumpally, Bibaswan Bose (2022), *Analysis of 5G and Future Prospects for the Indian Armed Forces*, Center for Security Studies

Luis Bastos, Germano Capela, Alper Koprulu and Gerald Elzinga (2021), *Potential of 5G Technologies for Military Application*, ICMCIS, pp: 1-8

M Malik (2021), *5G for Military Communication: Automation of Kill Cycle*, ICTAI, pp: 285-290

Navjid Singh Bedi (2019), *5G, IoT & IT's Relevance for the Armed Forces,* CENJOWS

Pal Gronsund, Andreas Gonzales, Kashif Mahmood (2020), *5G Service and Slice Implimentation for a Military Use Case*, IEEE (ICC Workshop), pp: 1-6

P Skokowski, JM Kelner, K Malon (2022), *Jamming and Jamming Mitigation for Selected 5G Military Scenarios*, Procedia Computer Science, Vol 205, pp: 258-267

Rojeena Bajracharya, Rakesh Shrestha, Syed Ali Hassan, Hejoon Jung, Hyundong Shin (2023), *5G and Beyond Private Military Communication: Trend, Requirements, Challenges and Enablers*, IEEE Access

Toby Redshaw (2021), *Strategic Significance of 5G for Special Operations of the Future*, Strategic Latency Unleashed, Vol 293

Dasar Revolusi Perindustrian Keempat (IR 4.0) Malaysia

Dasar Keselamatan Negara (2021 – 2025)

Sustainable Development Goal Indicator 2030 (SDG 30)

Kertas Putih Pertahananan

Plan Army4NextG (2021-2050)

Sistem Pengurusan Strategik Tentera Darat (2021 – 2025) (SPS TD)

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

ISSN 0128-0171
9 770128 017006