ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 09/23 (September)

Internet of Military Things –Enhancing Military Operations

OVERVIEW

1. Internet of Things (IoT) devices have become pervasive in today's society, with the integration of intelligent digital technologies into our everyday lives. IoT technology has even found its way into the battlefield and to provide real-time situation awareness and command and control. This extension of IoT into military applications, devices and systems is known as Internet of Military Things (IoMT) or Internet of Battlefield Things (IoBT). The use of IoMT and IoBT is premised on the idea that future warfare and military operations will be increasingly complex and multi-faceted, and driven by machine intelligence.

***"Technological innovation can overcome the unknowns and ambiguities of war by providing near-perfect information which allows generals to instantly out-think and out-act their enemies."* – Admiral William Owens, retired Vice Chairman of the Joint Chiefs of Staff United States Sixth Fleet (1994 - 1996)**

WHAT IS THE INTERNET OF MILITARY THINGS?

2. IoMT refers to physical objects in the military domain that are embedded with sensors, software and other technologies that communicate with each other to accomplish a broad range of activities in a more efficient and informed way.

***"It is estimated that IoMT accounts for 7 – 11% of the total IoT market. These include body sensor systems, vehicle electronics, targeting systems, unmanned aerial vehicles and so on."* – Indeema**

HOW CAN THE INTERNET OF MILITARY THINGS ENHANCE MILITARY OPERATIONS?

3. Advanced militaries have invested heavily into C4I systems and infrastructures to collect, analyse and disseminate data. Integrating IoMT into battlefield operations can speed up the Observe, Orient, Decide, Act (OODA) loop of decision-making to enhance operational and response strategies. It also helps to simplify, improve and automate processes. Today, many militaries deployed IoMT in three areas, namely military healthcare, logistics and sense-making.

Military Healthcare

3. Solider health is central to every military in the world. Advances in technology allows IoMT solutions to be incorporated into sensors that are used to monitor soldiers' health and movements so as to identify potential problems and offer immediate solutions to reduce the risk of serious illnesses or injuries.

a. Health Monitoring Devices. Wearable devices on soldiers monitor the health and safety of troops by tracking vital signs such as heart rate, blood pressure, body temperature and detecting harmful chemicals or radiation. Health and safety issues can be identified and pre-empted by the provision of medical supplements, treatment or evacuation from the battlefield if necessary.

b. Telemedicine and Telehealth Services. Interactive video consultations allow soldiers to continue receiving timely medical advice, consultations, medications and even therapy sessions wherever they are. Dispensation of medication can also be automated. For instance, the Singapore Armed Forces is piloting the Medical Dispensary System to reduce the probability of medical errors and to reduce the logistical demands on medical staff. As the System is integrated with the medical records of soldiers, this pilot provides for a seamless dispensation of medication through a MEDBOX – a smart tracker locker – that is made available 24/7.

Logistics Management

4. The use of IoT solutions in the management of military resource helps to achieve end-to-end asset visibility. This allows the swift and efficient allocation of resources for the successful conduct of military operations.

a. Sensors for Asset Management. IoT sensors can be used to track military assets such as weapons, machinery and ammunition through a centralised system. The information gathered can be used for asset utilisation tracking and equipment maintenance, increasing operational efficiency. For example, continuous monitoring of an aircraft engine condition and fuel consumption allows personnel to accurately repair or replace a specific engine part.

b. Sensors for Supply Chain Management. The IoT ecosystem enables military organisations to track the movement of goods and monitor their condition throughout the supply chain. This will allow them to manage inventory levels and reduce wastage. Australia is developing a "Smart Storage Box" that can monitor and track the condition, quantities and movements of supplies in a timelier manner, thereby improving the efficiency and effectiveness of the supply chain.

Sense-making the Battlefield

5. Artificial intelligence, machine learning, big data, robotics and autonomous weapons, amongst others, will shape the character of future warfare and the battlefield. Some refer to

this as the "digital battlefield". IoMT sensors can be deployed across the land, air, sea, below the sea, and even in outer space, and when integrated effectively, helps a military to have full situational awareness and control within complex and diverse conflict zones, make critical decisions, and potentially achieve military superiority.

a. Unmanned Systems for Area Exploration. Analysis of the area where the battle will occur, and the forces of the enemy have always been the basis of military strategy and tactics. Unmanned systems are ideal for area exploration as they can obtain operational data on the state of the battlefield without exposing any personnel to danger.

b. Air Battle Management Systems (ABMS). Air assets such as drones, Unmanned Aerial Vehicles (UAVs), aircraft are able to provide visual data on adversaries in a target area. The information allows commanders to determine if the target area is safe for troops to enter or requires artillery support or other measures. One of the ABMS efforts identified by the US Air Force enables the new F-35 Lightning 11 fighter to connect with the command and control centres, including by turning airborne platforms such as the KC-46 Pegasus tanker into a data link.

c. Sea Battle Management Systems. Naval assets such as Unmanned Underwater Vehicles (UUVs), unmanned flotillas are able to perform reconnaissance by detecting enemy vessels, discover and terminate underwater mines and also do coastal surveillance to ensure the safe passage of naval or commercial vessels.

d. Ground Battle Management Systems. Wearable/hearable devices connect the soldier to sensors, communications systems, navigation systems, battle management systems, weapons and power sources. These devices allow collection of a variety of data that can be used to identify whether a target is a friend or foe and provide real-time communication, resulting in improved situation awareness and decision making.

e. IoMT in Space Applications. IoT enables a connection between sensors and devices to be made terrestrially and through space. Low orbit satellites known as Satellite IoT or Sat-IoT can cover a lot of unreachable areas, enabling asset tracking and sense-making. The Australian Defence Force expanded their IoMT by partnering with Myriota to tag military assets with ruggedised devices to provide location data through Myriota's network of nano-satellites that is part of a global, space-enabled communications network.

***"If you know the enemy and know yourself, you need not fear the result of a hundred battles."* – According to Sun Tzu**

CHALLENGES OF INTEGRATING INTERNET OF MILITARY THINGS INTO MILITARY OPERATIONS

6. Although IoMT technology has many advantages, militaries will face some challenges during implementation. Listed below are some common IoMT security challenges and recommendations on how to overcome them:

a. Networked IoMT Increases Risk of Cyber Attacks. IoMT devices increases the attack surface area by introducing a wider range of vulnerabilities and entry points for attacks. According to the Australian Cyber Security Centre, common attack vectors include ransomware, phishing, brute force, distributed denial of service (DDoS), compromised credentials, trojans, SQL injections, session hijacking, and man-in-the-middle (MITM) attacks. To combat this, there should be risk mitigating measures in place such as data encryption, anti-jamming and tamper-proofing measures.

b. Unsecured Software. Software in IoMT devices are often not encrypted, making it easy for adversaries to insert malware into the devices. They are often not updated regularly due to intermittent internet connectivity, which means that unpatched software with known vulnerabilities are running for long periods, making them vulnerable to cyber attacks. Militaries should configure their IoMT devices to receive routine device status and software updates, with provisions to stop the updates in adverse conditions.

c. Interoperability Issues. IoMT involves integrating various sensors, devices and platforms from different manufacturers. Command and control between them will be difficult due to the differences in data formats, protocols and standards. Secured open platforms based on open data standards can solve the interoperability issues between the various manufacturers.

d. Inadequate Training. Inadequate training can lead to reduced effectiveness and increase the risk of mistakes or accidents. For example, soldiers who are inexperienced in handling advanced drones or sensors may not carry out their missions properly, resulting in accidents or casualties. Hence, it is important to ensure that personnel are sufficiently trained to carry out their duties effectively.

CONCLUSION

7. The modern battlefield is a complex place comprising the air, land, sea and more recently, cyber domains. IoMT has already weaved its way into all the domains and will continue its development with the advancement of technology. Militaries must learn to adapt and adopt the technology so as to reap the benefits that it can bring.

***"The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life."* – Bill Gates, Co-founder of Microsoft**

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

News Articles

1. Applications of Internet of Things (IoT) in Defence and Military
   [Link: https://www.shiksha.com/online-courses/articles/applications-of-internet-of-things-iot-in-defence-and-military/]

2. IoT for Military: How the Internet of Things Can Benefit the Military - IoT Worlds
   [Link: https://www.iotworlds.com/iot-for-military-how-the-internet-of-things-can-benefit-the-military/]

3. Internet of Medical Things (IoMT) in the Military: How Real-Time Health Monitoring is Maximizing Soldier Performance – International Defense Security & Technology
   [Link: https://idstch.com/technology/biosciences/internet-of-medical-things-iomt-in-the-military-how-real-time-health-monitoring-is-maximizing-soldier-performance/]

4. Challenges and Opportunities of Integrating IoT in Military - Matellio Inc
   [Link: https://www.matellio.com/blog/iot-in-military/]

5. The Internet of Military Things | The Cove
   [Link: https://www.matellio.com/blog/iot-in-military/]

6. The Internet Of Military Things (IoMT): How IoT Is Used In Warfare | Indeema Software
   [Link: https://indeema.com/blog/the-internet-of-military-things-iomt--how-iot-is-used-in-warfare

7. Advancing the Internet of Military Things (IoMT) with Software Defined Radio – COTS Journal
   [Link: https://www.cotsjournalonline.com/index.php/2021/10/13/advancing-the-internet-of-military-things-iomt-with-software-defined-radio/]