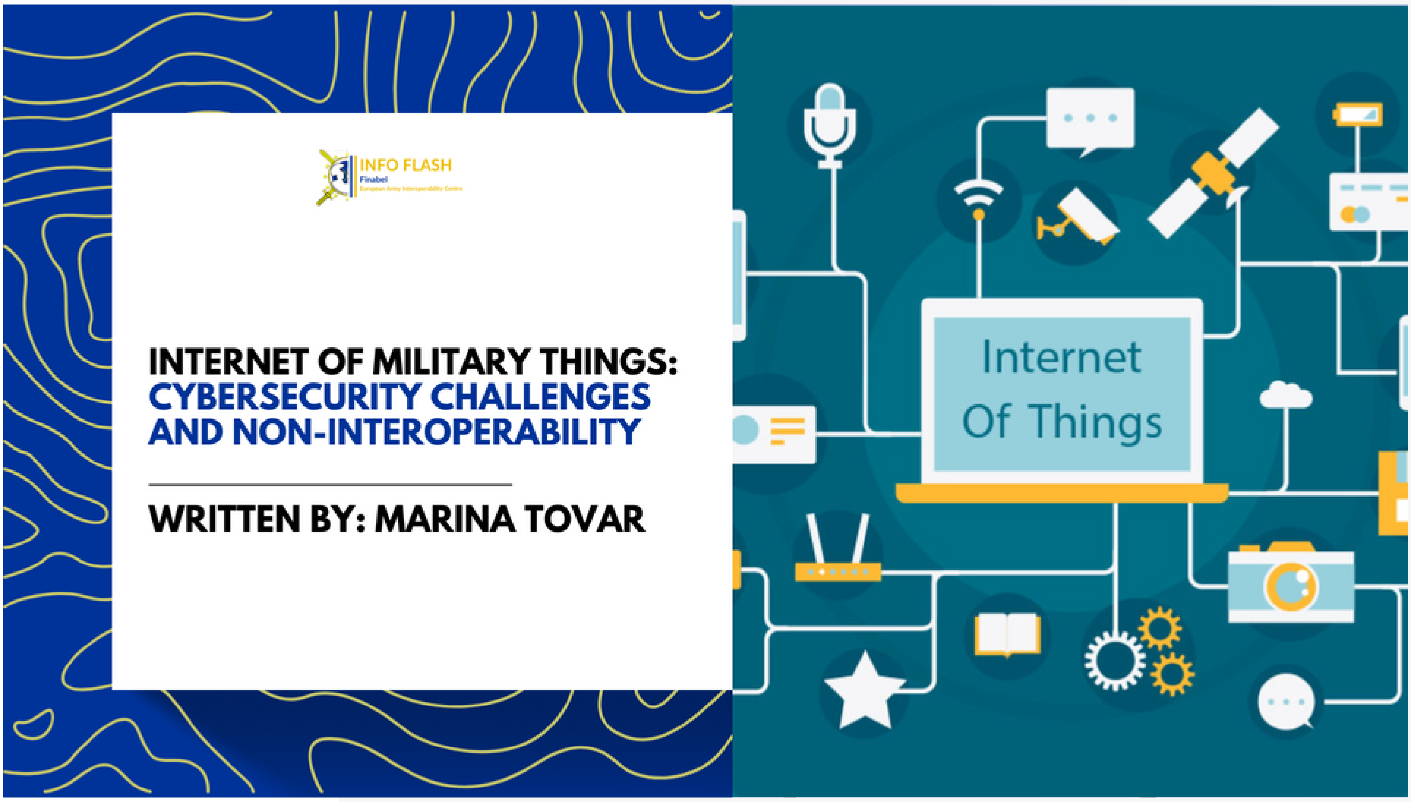
INFO FLASH
Finabel
European Army Interoperability Centre

FINABEL - THE EUROPEAN ARMY INTEROPERABILITY CENTRE

MARCH 2024



INFO FLASH
Finabel
European Army Interoperability Centre

# INTERNET OF MILITARY THINGS: CYBERSECURITY CHALLENGES AND NON-INTEROPERABILITY

WRITTEN BY: MARINA TOVAR

**WRITTEN BY**
MARINA TOVAR

**EDITED BY**
MANFRED SINTORN

**SUPERVISED BY**
SYUZANNA KIRAKOSYAN

## Introduction

The Internet of Military Things (IoMT) presents widespread opportunities, including enhanced efficiency, real-time decision-making, and improved situational awareness. The IoMT is “driven by military informationization requirement and information technology development. It consists of an information system capturing the physical attributes and state information of military people, equipments and materials by various information sensing means, connecting all kind of operation elements and environment elements as an organic whole by standard communication protocols to process, control and apply intelligently” (Yushi et al., 2018: 632).

Within the European Union, potential IoMT applications in Member States' armed forces and EU Common Security and Defence Policy (CSDP) missions are substantial, for example, in streamlining logistics and optimising the allocation of resources. Simultaneously, the IoMT brings significant challenges, such as cybersecurity vulnerabilities, and IoMT devices lack common standards ensuring interoperability. These challenges necessitate proactive measures and robust regulatory frameworks to mitigate vulnerabilities and handle threats while ensuring IoMT integrity and reliability.

It will analyse the cybersecurity vulnerabilities of IoMT devices and how these can threaten operational security. It then explores the lack of interoperability standards in IoMT-connected devices and argues the need to develop and ensure a common framework. The conclusion prescribes policy recommendations for facilitating operational security and common standards in the IoMT.

## Cybersecurity vulnerabilities

The IoMT can enhance tactical and operational situational awareness and information superiority. However, this enhancement comes at a cost, as IoMT-utilising equipment and battlefield internet usage bring wide cybersecurity vulnerabilities. The interconnected nature of IoMT devices, where sensors and communication devices employed by troops are intertwined, means that systems' security breaches can compromise operational security and complicate or cripple operations.

The high number of different IoMT devices connected to the same network provides hostile actors with abundant potential points of entry to IoMT networks (Lamas et al., 2016). In a military context, network complexity and the risks borne from the number of points of entry are amplified by the diversity of networked components, which can include everything from personal equipment to weapons systems and vehicles. Multiple points of entry and interconnected systems mean that the variety of static and dynamic biometrics collected come with a notable threat of data theft, which could be used for impersonation and to access the wider IoMT network (Butun et al., 2019).

Malicious actors can also exploit IoMT devices that lack regular security updates and patches. Once compromised, devices can be used as pivot points into the network, where one compromised system can be leveraged to compromise an entire network and all devices connected to it. If vulnerabilities are not quickly patched out, an unauthorised actor might be able to modify the device's firmware, gain persistent access, continuously leech data, or launch attacks to permanently or temporarily cripple networks and devices (Lakhani, 2021). Compromised IoMT devices could also have even broader battlefield implications, such as the attacker assuming control of a growing and increasingly impactful arsenal of semi-autonomous systems (Cameron, 2018).

Data integrity challenges are also a clear threat for IoMT devices as they directly impact missions with clear risks in operational effectiveness and military personnel safety. Tampering the data gathered and relied on by the IoMT could severely affect decision-making: the manipulation of a soldier's health monitoring system could lead decisions being made based on incorrect information on troop status (Cameron, 2018). IoMT devices may also provide inaccurate readings or flawed diagnostics, where incorrect data could lead to incorrect medical treatment and tactical decisions (Cameron, 2018). For instance, a temperature sensor on a military vehicle malfunctioning and reporting adverse conditions could cause delays and inappropriate gear adjustments.

As for data integrity, the attacker could intentionally alter sensor data to disrupt the operation through jamming, spoofing or injection attacks, intercepting or manipulating transmitted data. Attackers could, for instance, compromise Unmanned Aerial Vehicles (UAVs) and have them transmit false coordinates to ground forces. The cybersecurity aspect of UAVs is a severe limitation, as UAVs are especially vulnerable to cyberattacks due to drone-operator communications (Dahiya & Garg, 2019). Because UAVs often carry a wide array of sensory equipment and tend to be remote-controlled, they are also vulnerable to a wide array of attacks, such as command and control data link jamming and spoofing, navigational sensor jamming and spoofing, and tapping video or photo links (Dahiya & Garg, 2019).

### Non-existence of interoperability standards in IoMT

The European Union has no specific legislation regulating the Internet of Military Things, though there are broader regulations impacting technology and security. The EU Cybersecurity Strategy (European Commission, 2022) addresses the technological limitations associated with the IoMT to provide operational capacity to prevent, deter, and respond to threats while ensuring resilience and European technological sovereignty (European Commission, 2022). However, the EU's Internet of Things Policy does not include or focus on military applications, and there are no initiatives to harmonise European interoperability standards for the IoMT. EU Defence policy is a nigh-exclusive Member State competency, and this means that decisions related to military technology, including IoMT applications, are predominantly made at a national level. Core to the member state tendency here is that EU Member States tend to oppose delegations of sovereignty in the CSDP, which complicates EU cooperation in defence (Csernatoni, 2021).

The IoMT involves integrating a diverse set of devices, systems, and platforms ranging from sensors to medical equipment, often from different manufacturers (Cameron, 2018). A lack of standardisation complicates data exchanges, and differences in practices and the use of non-cross-compatible software hinders interoperability (Malik et al., 2020). Hence, the lack of standardisation may delay or hamper real-time data sharing, leading to delays, glitches, and inefficiencies.

IoMT devices handle critical operational data, and ensuring these devices can exchange data without compromising safety or security is essential. If interoperability issues prevent timely transmission, data exchange could be compromised. Troops rely on data from various devices to make informed decisions. When devices cannot communicate, information gaps occur, threatening the operational security of deployed personnel and complicating decision-making (Fraga-Lamas et al., 2016). Coupled with a lack of standardisation complicates data exchange as devices have different communication protocols, user interfaces, and sensors, resulting in non-interoperable and unwieldy systems (Lakhani, 2021).

## Concluding Remarks and Recommendations

Cybersecurity challenges remain a core problem for IoMT networks as interconnected devices offer multiple entry points for malicious actors, risking operational security. Furthermore, data-related risks remain at the core of the cybersecurity challenges. The implications of tampering with IoMT data could lead to incorrect decision-making, while the problems of data exchange associated to a lack of interoperability standards could hinder effective communication.

For the EU, there is a clear need to foster innovation and promote interoperable standards to harness the full potential of the Internet of Things without facing undue risk. Therefore, the EU should put forward guidelines that ensure interoperability and promote policies like standardised interfaces, compatible communication, and encryption systems, to reduce complexity in IoMT maintenance and improve cross-device integration.

## Bibliography

Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644. https://arxiv.org/pdf/1910.13312.pdf

Cameron, L. (2018, January 3). Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT. Institute of Electrical and Electronics Engineers Computer Society. https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

Csernatoni, R. (2021, February 1). The evolving role of the European External Action Service in Security and Defense. Carnegie Europe. https://carnegieeurope.eu/publications/85980

Dahiya, S., & Garg, M. (2020). Unmanned aerial vehicles: Vulnerability to cyberattacks. In Proceedings of UASG 2019: Unmanned Aerial System in Geomatics 1 (pp. 201-211). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-37393-1_18

European Commission. (2022). The Cybersecurity Strategy. European Commission https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

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. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5087432/

Lakhani, A. (2021, June 7). Examining Top IoT Security Threats and Attack Vectors. Fortinet. https://www.fortinet.com/blog/industry-trends/examining-top-iot-security-threats-and-attack-vectors

Malik, M. I., McAteer, I. N., Hannay, P., Ibrahim, A., Baig, Z., & Zheng, G. (2020). Cyber security for network of things (NoTs) in military systems: challenges and countermeasures. In Security Analytics for the Internet of Everything (pp. 231-249). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003010463-14/cyber-security-network-things-nots-military-systems-muhammad-imran-malik-ian-noel-mcateer-peter-hannay-ahmed-ibrahim-zubair-baig-guanglou-zheng

Yushi, L., Jiang, F., & Hui, Y. (2012). Study on Application Modes of Military Internet of Things (MIOT). Institute of Electrical and Electronics Engineers International Conference on Computer Science and Automation Engineering (CSAE). https://doi.org/10.1109/CSAE.2012.6273031