The Internet of Military Defense Things: State-of-the-Art, Challenges, Future Evolution and Revolutionary Applications

Publication Date	Manuscript Submission Deadline
First Quarter 2025	**30 September 2024**

Special Issue of the IEEE Internet of Things Magazine

Call for Papers

The widespread adoption of technology, such as cloud computing, mobile communication, sensor networks, and artificial intelligence, poses significant challenges and opportunities for military defense and national security. In the current technological landscape, the use of Internet of Things (IoT) technologies has the potential to greatly enhance capabilities and fundamentally change the speed, scale, adaptability, and efficiency of defense and national security operations. The adoption of IoT will enhances situational awareness by connecting various components such as soldiers, military vehicles, ships, tanks, aircrafts, satellites, and Unmanned Aerial Vehicles (UAVs).

However, the defense and national security environments, such as patrolling battlefields along safeguarding borders, surveillance, and providing advanced military training, pose particular difficulties. Moreover, the increasing diversity and interconnectivity of networked components, including combat attire, helmets, weaponry, and other equipment, that collect and transmit instantaneous data to military bases, present additional complexities for military defense and national security systems.

In order to tackle these challenges, it is crucial to develop innovative and practical methods that can accurately depict the present situation, understand emerging trends, and offer predictive analytics in a wide range of defense and national security contexts that are constantly evolving. Achieving success in military operations relies heavily on possessing capabilities that facilitate dominance through technological adaptability, consistent speed, and a holistic, intelligent, autonomous, secure, and tactical system that surpasses the combined effectiveness of its individual components while also overcoming the constraints of inter-human communication and cognition. In light of the above, it becomes evident that the distinct characteristics of military defense and national security environments present significant obstacles for IoT systems, distinguishing them from their civilian counterparts.

First and utmost, any failure or compromise may be life threatening and/or highly destructive. Second, IoT systems operating in hostile environmental contexts similar to

those mentioned above, are prone to hoax as well as to repetitive physical and cyber-attacks. Under such circumstances, adversaries' often devastating unforeseen locations may compromise IoT systems and exploit potential opportunities to intensify resulting damages. To this end, commercially available communication devices, networks, and cloud data centers are doomed to become unreliable. Disruption tolerance, data losses, and struggles to maintain connectivity in continuously and rapidly changing heterogeneous battle scenes are the rule rather than the exception. As such, IoT systems for military operations and national security are required to exhibit high flexibility, dynamism, and adaptability; hence, capable of incorporating additional devices, communication networks, and their protocols and standards in a real-time manner.

The IoT Magazine is soliciting high-quality, novel, innovative and impact-oriented manuscripts that: *a*) describe in depth and/or breadth real-world military defense and national security IoT deployments, applications and technologies that align with the above-elaborated special issue, *b*) present actual experiences in analyzing the benefits of IoT and resolving contextual defense and national security-related challenges, *c*) develop and share best practices, vision realizations and lessons learned from IoT deployments in such environments, and *d*) establish guiding principles for technical, experimental and operational successes. Topics of interest may include, but are not limited to:

- **Security and Privacy in IoMDT:** Addressing issues in securing military smart bases and IoT networks, including encryption, authentication, intrusion detection, and cyber threat countermeasures in battlefield environments.
- **IoT in Military Logistics:** Explore how IoT is enhancing military logistics, including supply chain management, asset tracking, and real-time equipment, vehicle, and resource monitoring.
- **IoT-Enabled Surveillance and Reconnaissance:** Discuss the role and new capabilities of IoT devices, such as UAVs, Unmanned Underwater Vehicles (UUVs), Unmanned Surface Vessels (USVs), autonomous robots, sensors, and cameras, in enhancing military surveillance, reconnaissance, and situational awareness capabilities.
- **IoMDT for Soldier Enhancement:** Explore how IoT devices and wearables are being used to enhance soldier performance, safety, and health on the battlefield.
- **IoMDT for Soldier Training:** Investigate XR/VR/AR IoT devices for the utilization of real-and-virtual integrated settings and develop effective training simulations for military personnel in special missions.
- **Energy-Efficient IoMDT:** Discuss energy-efficient IoT solutions for military applications, such as optimizing power usage in remote sensors and IoT devices to extend mission duration.
- **Edge Computing in Military IoT:** Explore the use of edge computing in military IoT systems to process data closer to the source, reducing latency and improving real-time decision.
- **AI and Machine Learning in IoMDT:** Examine how artificial intelligence and machine learning algorithms are being applied to military IoT data for Valuable

Vehicle or Human Identification, Unmanned Vehicle Control, intercepted communications translation, improvised explosive device detection, improving the efficiency of logistics operations, predictive analytics, anomaly detection, emergency response and autonomous decision-making.

- **Interoperability and Standards:** Discuss the importance of interoperability and standards in IoMDT systems to ensure seamless integration of devices and data across different military branches and allied forces.
- **Ethical and Legal Considerations:** Explore the ethical and legal implications of deploying IoT technologies in military contexts, including data privacy, accountability, and adherence to international laws of armed conflict.
- **Case Studies and Deployments:** Share real-world case studies and deployments of IoMDT systems in military operations, highlighting their effectiveness and lessons learned.
- **Resilience and Robustness:** Discuss strategies for making IoMDT systems resilient to physical and cyberattacks, anti-jamming, GPS denied environments, Adversarial AI in IoMDT, ensuring they can operate in adverse conditions and withstand hostile actions.
- **Human-Machine Teaming:** Explore the evolving role of humans in military IoT systems, emphasizing the importance of effective human-machine collaboration and trust-building.
- **Environmental Monitoring, Adaptation and Safety:** Highlight how IoT sensors are used for environmental monitoring and adaptation, including tracking climate changes, predicting natural disasters, and optimizing military responses as well as ensuring public safety.
- **IoMDT in Urban Warfare:** Discuss the unique challenges and opportunities of deploying IoT technologies in urban warfare scenarios, where densely populated environments present complex challenges.
- **Future Trends and Innovations:** Discuss IoMDT trends like 5G, 5G+, and 6G mobile network integrations, satellite and terrestrial network integrations (Space-Air-Ground-Sea Integrated Networks), hypersonic weapon communication, quantum encryption, and bio-inspired IoT technologies for tactical, military, and emergency applications.
-

Submission Guidelines

Articles should be general, independent of technical and business specialty and intended to an audience consisting of all members of the IoT community and especially experts involved in the military defense and national security world at all of the academic, industrial and governmental level. Manuscripts are expected to add to the knowledge base or best practices of the IoT community. Authors are asked to strive to make their papers understandable by the general IoT practitioner. Mathematical material should be avoided; instead, references to papers containing the relevant mathematics should be

provided. Authors are encouraged to use color figures and submit multimedia material along with their articles for review. We encourage practice and implementation works. Editors may provide a quick response to the papers that may not fit this SI.

Authors should target 4,500 words or less (from introduction through conclusions, excluding figures, tables, and captions), or six (6) pages. Figures and tables should be limited to a combined total of six (6). The number of archival references for an original submission is not to exceed fifteen (15).

Manuscripts should conform to the standard format as indicated in the Information for Authors section of the Paper Submission Guidelines.

All manuscripts to be considered for publication must be submitted by the deadline through the magazine's Manuscript Central site. For further questions or inquiries, please contact the corresponding Guest Editors.

Important Dates

Manuscript Submission Deadline: September 30, 2024
First Round of Review Deadline: October 30, 2024
Authors' Revision Deadline: November 30, 2024
Final Decision Notification: December 15, 2024
Final Manuscript Submission Deadline: December 30, 2024
Publication Date: First Quarter 2025

Guest Editors

Maurice J. Khabbaz (Lead GE)
American University of Beirut, Lebanon

Abdellah Chehri (Co-Lead GE)
Royal Military College of Canada

Holger Claussen
Tyndall National Institute, Ireland

Nhien-An Le-Khac
University College Dublin, Ireland

Van-Linh Nguyen
National Chung Cheng University, Taiwan

Benoit Debaque
Thales Communications and Security SAS, Canada