



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

Análise do Impacto da Internet das Coisas Militar (IoMT) nas Operações de Campo

José Wesley Mendes de Souza Silva

Orientador: Dr. Éwerton Rômulo Silva Castro



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Cursos Superior de Tecnologia em Telemática

Análise do Impacto da Internet das Coisas Militar (IoMT) nas Operações de Campo

José Wesley Mendes de Souza Silva

Monografia apresentada à Coordenação do Curso de Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Dr. Éwerton Rômulo Silva Castro

Campina Grande, Dezembro de 2025

S586a Silva, José Wesley Mendes de Souza
Análise do impacto da Internet das Coisas Militar (IoMT)
nas operações de campo / José Wesley Mendes de
Souza Silva.. - Campina Grande, 2023.
55 f.: il.

Trabalho de Conclusão de Curso (Graduação em
Tecnologia em Telemática) - Instituto Federal da Paraíba,
2023.

Orientador: Prof. Dr. Éwerton Rômulo Silva Castro

1. Telemática. 2. Internet das coisas - IoT. 3. Tecnologia militar. 4. Cibersegurança. 5. Sistemas de informação
- I. Castro, Éwerton Rômulo Silva. II Título.

CDU 355:004.738

Análise do Impacto da Internet das Coisas Militar (IoMT) nas Operações de Campo

José Wesley Mendes de Souza Silva

Dr. Éwerton Rômulo Silva Castro
Orientador

Msc. Iana Daya Cavalcante Facundo Passos
Membro da Banca

Dr. José Antônio Cândido Borges da Silva
Membro da Banca

Campina Grande, Paraíba, Brasil
Dezembro de 2025

Dedico este trabalho à minha família, pelo amor incondicional e apoio constante.

Aos meus pais, por acreditarem em mim mesmo nos momentos mais difíceis.

*E os meu Amigos Adrian Bruno, Rafael Germano e Mikael Marinho. de alguma forma,
contribuíram para a realização deste sonho acadêmico.*

É patético desistir de algo sem nem mesmo ter tentado.
Misaki Mei - Another

Agradecimentos

Ao meu pai, por me conceder força, saúde e sabedoria para superar os desafios ao longo desta jornada acadêmica. Mesmo não estando mais presente, ele sempre me apoiou em todas as minhas loucuras. Te amo, meu querido pai! À minha mãe, pelo amor incondicional, apoio constante e por acreditar em mim, mesmo nos momentos mais difíceis. Ao meu orientador, Dr. Éwerton Rômulo Silva Castro, pela paciência, dedicação e pelas valiosas orientações que contribuíram significativamente para a realização deste trabalho. Aos professores do curso de Telemática do IFPB – Campus Campina Grande, por compartilharem conhecimento e inspirarem o crescimento profissional e pessoal. Aos meus amigos Adrian Bruno, Rafael Germano e Mikal Marinho, pela parceria, companheirismo e incentivo durante todo o percurso. E, por fim, a todos que, de alguma forma, contribuíram para a concretização deste sonho, o meu mais sincero agradecimento.

Resumo

Analisa-se neste trabalho o impacto da Internet das Coisas Militares (*Internet of Military Things* - IoMT) nas operações de campo, destacando suas aplicações, desafios e tecnologias emergentes associadas. A pesquisa foi conduzida por meio de uma revisão bibliográfica de artigos científicos, livros e publicações recentes, com foco na integração de sensores, *drones*, veículos e sistemas de comando e controle em redes inteligentes. Os resultados apontam que a *IoMT* representa uma das mais relevantes transformações tecnológicas na defesa moderna, ao possibilitar maior eficiência operacional, consciência situacional e capacidade de resposta estratégica. Contudo, desafios como interoperabilidade, cibersegurança, consumo energético e escalabilidade ainda limitam sua implementação plena. Tecnologias como Inteligência Artificial (IA), Aprendizado de máquina (*Machine Learning* - ML), *Blockchain* e Computação de Borda surgem como soluções promissoras para mitigar esses problemas e aprimorar a resiliência das infraestruturas militares conectadas. Assim, conclui-se que a *IoMT* redefine o paradigma das operações militares, deslocando o foco do poder bélico para o poder informacional e para a tomada de decisão baseada em dados.

Palavras-chave: internet das coisas militar; iot; operações de campo; cibersegurança; tecnologias emergentes.

Abstract

This study analyzes the impact of the Internet of Military Things (IoMT) on field operations, highlighting its applications, challenges, and associated emerging technologies. The research was conducted through a literature review of scientific articles, books, and recent publications, with a focus on the integration of sensors, drones, vehicles, and command and control systems into intelligent networks. The results indicate that IoMT represents one of the most significant technological transformations in modern defense, enabling greater operational efficiency, enhanced situational awareness, and improved strategic response capabilities. However, challenges such as interoperability, cybersecurity, energy consumption, and scalability still limit its full implementation. Technologies such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, and Edge Computing emerge as promising solutions to mitigate these issues and enhance the resilience of connected military infrastructures. Thus, it is concluded that IoMT redefines the paradigm of military operations, shifting the focus from purely kinetic power to informational power and data-driven decision-making.

Keywords: internet of military things; iot; field operations; cybersecurity; emerging technologies.

Sumário

Lista de Siglas	xii
Lista de Figuras	xiii
Lista de Quadros	xiv
1 Introdução	1
1.1 Justificativa e Relevância do Trabalho	3
1.2 Objetivos	3
1.2.1 Objetivo Geral	4
1.2.2 Objetivos Específicos	4
1.3 Metodologia	4
1.3.1 A pesquisa foi conduzida em três etapas principais:	4
1.4 Organização do Documento	5
2 Fundamentação Teórica e Resultados	7
2.1 A Evolução da Internet das Coisas (<i>IoT</i>)	7
2.1.1 Da <i>IoT</i> para a Internet das Coisas Militar (<i>IoMT</i>)	9
2.2 Arquitetura e Componentes da IoMT	10
2.2.1 Camada de Aplicação	10
2.2.2 Camada de Comunicação	11
2.2.3 Camada de Processamento	13
2.2.4 Camada de Decisão	14
2.3 Desafios da <i>IoMT</i>	16
2.3.1 Segurança	16
2.3.2 Interoperabilidade	17
2.3.3 Consumo de Energia	18
2.3.4 Escalabilidade	19
2.4 Tecnologias de Apoio e Soluções Emergentes	20
2.5 Perspectivas Futuras	22

3	Resultados	23
3.1	Panorama Geral das Publicações Seleccionadas	23
3.2	Principais Desafios da IoMT	25
3.2.1	Aplicações e Benefícios da <i>IoMT</i> nas Operações de Campo	27
3.2.2	Internet das Coisas de Batalha	29
3.2.3	Resultados do Trabalho	30
4	Considerações Finais e Sugestões para Trabalhos Futuros	32
4.1	Contribuições do Estudo	33
4.2	Sugestões para Trabalhos Futuros	33
4.3	Considerações Finais	33
A	Reportagens sobre IoMT	37
A.1	Figura 4.1	37
A.2	Figura 4.2	38
A.3	Figura 4.3	38
A.4	Figura 4.4	39
	Referências Bibliográficas	40

Lista de Siglas

CCCIIVR	Comando, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento
CID	Confidencialidade, Integridade e Disponibilidade
CN	Computação em Nuvem (<i>Cloud Computing</i>)
CNé	Computação de Névoa (<i>Fog Computing</i>)
DDoS	<i>Distributed Denial of Service</i> (Negação de Serviço Distribuída)
DoS	<i>Denial of Service</i> (Negação de Serviço)
EC	<i>Edge Computing</i> (computação de borda)
IA	Inteligência Artificial (<i>Artificial Intelligence</i>)
IoT	<i>Internet of Things</i> (Internet das Coisas)
IoMT	<i>Internet of Military Things</i> (Internet das Coisas Militares)
IoBT	<i>Internet of Battle Things</i> (Internet das Coisas de Batalha)
ML	<i>Machine Learning</i> (Aprendizado de Máquina)
MANET	<i>Mobile Ad Hoc Networks</i> (Redes Ad Hoc Móveis)
PAAA	Plataformas Aéreas de Alta Altitude
QoS	<i>Quality of Service</i> (Qualidade de Serviço)
RFID	<i>Radio-Frequency Identification</i> (Identificação por Radiofrequência)
SAD	Sistemas de Apoio à Decisão
SDN	<i>Software Defined Networking</i> (Rede Definida por Software)
UAV	<i>Unmanned Aerial Vehicle</i> (Veículo Aéreo Não Tripulado / Drone)
WSN	<i>Wireless Sensor Networks</i> (Redes de Sensores Sem Fio)

Lista de Figuras

2.1	Dispositivos IoT Usados no Cotidiano	8
2.2	evolução da <i>IoT</i>	8
2.3	Indústria 4.0	9
2.4	<i>IoT</i> civil e <i>IoMT</i>	9
2.5	Camadas Principais da <i>IoMT</i>	10
2.6	Camada de Aplicação	11
2.7	Camada de Comunicação	12
2.8	Camada de Processamento	14
2.9	Camada de Decisão	15
2.10	Sistema de Segurança e Vigilância	17
2.11	Integração Entre Sistemas Militares Distintos	18
2.12	Consumo de energia em sistemas IoT em tempo real	19
2.13	Tecnologias Emergentes Aplicadas ao Campo de Batalha	20
3.1	Elaborado pelo Autor, 2025, Levantamentos.	23
3.2	Elaborado pelo Autor, 2025, Levantamentos.	24
3.3	Internet das Coisas de Batalha	30
4.1	Drone Submarino.	35
4.2	Drone da Rússia explode.	35
4.3	Darwin operador de drones FPV kamikaze.	36
4.4	<i>Drone</i> Comando Vermelho.	36

Lista de Quadros

1.1	Resumo dos principais aspectos da IoMT	2
1.2	Organização do Documento	6
2.1	Camadas do sistema IoMT e suas descrições resumidas	16
2.2	Tecnologias Emergentes e Soluções de Apoio	22
3.1	Comparativo entre os Principais Desafios da IoMT	27
3.2	Principais Aplicações e Benefícios da IoMT nas Operações de Campo	29

Capítulo 1

Introdução

Na sociedade contemporânea, a busca por conforto, agilidade e praticidade é uma constante, essa demanda impulsiona a contínua adoção e o desenvolvimento de inovações tecnológicas. Nas últimas décadas, a tecnologia tem evoluído rapidamente visando atender às necessidades da população. Nesse contexto, a Internet das Coisas (*Internet of Things* - IoT) tem se mostrado cada vez mais relevante. Ela possibilita a interação entre dispositivos criando um ecossistema conectado onde a comunicação ocorre em tempo real [Kikuchi 2023]. Essa transformação tecnológica não se limita à dimensão operacional, mas influencia diretamente a formulação de estratégias, a gestão de recursos e a tomada de decisões em situações de conflito.

A revolução digital está mudando profundamente como os militares operam. Novas tecnologias estão redefinindo completamente conceitos como vigilância, comando e controle em meio a conflitos. No centro dessa mudança está o surgimento da Internet das Coisas Militar (*Internet of Military Things* - IoMT). Consiste em um ecossistema tecnológico que conecta tudo: dispositivos inteligentes, sensores, armas e até os próprios soldados em uma rede unificada. Essa rede coleta, processa e compartilha dados em tempo real, criando uma ponte entre o mundo físico e o digital no campo de batalha. Ela é, sem dúvida, um marco divisório na evolução da guerra moderna [Tolba 2020].

Em essência, é a aplicação militar do conceito de IoT. Enquanto a IoT comum conecta eletrodomésticos ou sistemas urbanos para otimizar a nossa vida diária, a IoMT cria uma infraestrutura de interconexão para o ambiente militar. Ela integra desde sistemas de vigilância de grande porte até o equipamento individual de cada combatente, formando uma malha digital que cobre todo o teatro de operações. Essa rede não só captura informações de todos os lados, mas também as transforma em inteligência útil por meio de análises avançadas [Wei 2021]. Essa transformação tecnológica não se limita à dimensão operacional, mas influencia diretamente a formulação de estratégias, a gestão de recursos e a tomada de decisões em situações de conflito.

A importância estratégica fica ainda mais clara quando se observa a natureza dos conflitos atuais. As operações modernas são marcadas por unidades dispersas geograficamente, pela

necessidade de decisões extremamente rápidas e pela busca constante de superioridade de informação. Neste cenário, a capacidade de integrar dados dos mais variados tipos vindos de sensores no solo, *drones*, sistemas de reconhecimento e até de dispositivos vestíveis pelos soldados se torna uma vantagem crítica para o sucesso de uma missão [Wei 2021].

Este capítulo tem como objetivo estabelecer as bases para entender o impacto transformador da IoMT. É analisado sua arquitetura tecnológica, suas aplicações práticas e suas implicações estratégicas. Por meio de uma revisão da literatura especializada e da comparação de implementações já existentes, busca-se identificar tanto as incríveis capacidades habilitadas por essa tecnologia quanto os desafios que ainda impedem seu uso pleno. Esta fundamentação servirá como base para investigações futuras sobre a viabilidade, a eficácia e as consequências reais do uso da IoMT.

A relevância desta análise é importante. Nações tecnologicamente avançadas estão acelerando seus investimentos em IoMT, e a superioridade informacional é cada vez mais tratada como prioritária na doutrina militar moderna. Entender o potencial dessa tecnologia é imperativo não apenas para os profissionais de defesa, mas para todos os envolvidos na formulação de políticas de segurança nacional e de desenvolvimento tecnológico estratégico. Diante desse panorama, torna-se pertinente analisar com profundidade os motivos que justificam a escolha do tema e os impactos que ele pode gerar tanto para o campo militar quanto para a comunidade acadêmica.

O IoMT consiste na aplicação da IoT ao ambiente de defesa, conectando sensores, *drones*, veículos, sistemas de armas e soldados em uma rede inteligente. Suas principais aplicações incluem vigilância, logística, comando e controle, além do monitoramento de tropas em campo. Apesar do grande potencial estratégico, a IoMT enfrenta desafios como interoperabilidade entre sistemas, cibersegurança, consumo de energia e escalabilidade. Sua relevância está na capacidade de garantir superioridade informacional, aumentar a eficiência operacional e apoiar a tomada de decisões rápidas, tornando-se um elemento central na guerra moderna. Conforme o Resumo dos principais aspectos da IoMT no Quadro. 1.1

Quadro 1.1: *Resumo dos principais aspectos da IoMT*

Aspecto	Resumo
Tema	Aplicação da IoT no contexto militar (IoMT).
Contextualização	Integra sensores, drones, veículos, armas e soldados em rede.
Aplicações	Vigilância, logística, comando e controle, monitoramento de tropas.
Desafios	Interoperabilidade, cibersegurança, energia, escalabilidade.
Relevância	Garante superioridade informacional e eficácia em operações.

Fonte: Elaborado pelo Autor, 2025.

1.1 Justificativa e Relevância do Trabalho

O avanço das tecnologias digitais tem transformado profundamente a forma como diferentes setores da sociedade operam, e o ambiente militar não é exceção. A chamada IoMT surge como uma das inovações mais promissoras nesse cenário, pois possibilita a integração de sensores, *drones*, veículos, armamentos e combatentes em uma rede inteligente capaz de coletar e compartilhar informações em tempo real. Essa capacidade amplia a eficiência logística, melhora a consciência situacional no campo de batalha e potencializa a tomada de decisão estratégica.

A relevância deste trabalho se justifica, em primeiro lugar, pela atualidade do tema. Conflitos recentes e o crescente uso de *drones* e dispositivos autônomos em operações militares demonstram que a guerra moderna é cada vez mais informacional e tecnológica. Analisar como a IoMT pode impactar diretamente a condução de missões em campo é fundamental para compreender o futuro da defesa e da segurança. Assim, a relevância não se restringe ao campo militar, mas dialoga com questões mais amplas da sociedade contemporânea, como a soberania digital, a proteção de infraestruturas críticas e a segurança de nações em um mundo cada vez mais conectado [Tortonesi 2017].

Além disso, o estudo é relevante do ponto de vista social e estratégico, pois traz reflexões sobre a necessidade de investimentos em pesquisa, segurança cibernética e interoperabilidade tecnológica, temas que afetam não apenas as forças armadas, mas também a soberania e a proteção de países em um mundo cada vez mais conectado.

Por fim, a pesquisa é importante também para a formação acadêmica e profissional do autor, visto que o estudo da IoMT envolve o diálogo entre áreas como redes de comunicação, Computação em Nuvem (CN), inteligência artificial e segurança digital. Dessa forma, o trabalho fortalece a integração entre teoria e prática, contribuindo para o desenvolvimento de competências essenciais no campo da tecnologia.

1.2 Objetivos

Este trabalho tem como objetivo analisar o impacto da Internet das Coisas Militar nas operações de campo, investigando como a integração entre sensores, veículos, *drones* e sistemas de comando pode otimizar a comunicação, aumentar a eficiência tática e fortalecer a tomada de decisão em ambientes de combate. Busca-se compreender de que forma essa tecnologia contribui para a superioridade informacional, a segurança operacional e a coordenação estratégica das forças armadas, destacando suas vantagens, limitações e perspectivas futuras.

1.2.1 Objetivo Geral

Avaliar, com base na revisão bibliográfica sistemática, o impacto da Internet das Coisas Militar nas operações de campo, considerando suas vantagens estratégicas, limitações técnicas e consequências para a eficiência operacional.

1.2.2 Objetivos Específicos

- Contextualizar a evolução da Internet das Coisas e sua adaptação para o cenário militar, originando a IoMT.
- Identificar e descrever as principais aplicações da IoMT em operações de campo, incluindo vigilância, logística, comando e controle.
- Examinar os desafios técnicos relacionados à IoMT, como interoperabilidade, consumo energético, escalabilidade e cibersegurança.
- Analisar soluções tecnológicas emergentes (como inteligência artificial, *blockchain* e arquiteturas resilientes) aplicadas à IoMT.
- Avaliar o potencial da IoMT para redefinir estratégias militares, aumentando a capacidade de resposta e a eficácia em cenários de conflito.
- Indicar lacunas e possibilidades de pesquisas futuras que possam contribuir para o avanço da IoMT em operações militares.

1.3 Metodologia

A presente pesquisa caracteriza-se como exploratória e descritiva, com abordagem qualitativa e fundamentação em revisão bibliográfica. O estudo busca compreender os conceitos, desafios e potencialidades da IoMT, utilizando-se de referências acadêmicas, artigos científicos, livros e publicações em periódicos especializados.

A escolha da metodologia qualitativa deve-se à necessidade de interpretar os impactos da IoMT no ambiente militar de forma contextualizada, considerando aspectos técnicos, estratégicos e operacionais. Foram consultadas bases de dados científicas como *IEEE Xplore*, *SpringerLink*, *ScienceDirect*, *Scopus* e *Google Scholar*, priorizando publicações recentes (dos últimos dez anos) e trabalhos de relevância na área de IoT, IoMT e CCCIIVR (Comando, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento).

1.3.1 A pesquisa foi conduzida em três etapas principais:

A - Levantamento bibliográfico

Foram consultadas bases de dados nacionais e internacionais (*IEEE Xplore*, *SpringerLink*,

ScienceDirect, *Scopus* e *Google Scholar*), bem como livros, artigos de periódicos e trabalhos acadêmicos sobre IoT, IoMT, Internet das Coisas de Batalha (*Internet of Battle Things* - IoBT), CCCIIVR e segurança em redes militares.

B - Seleção e organização das fontes

Os materiais coletados foram organizados em categorias temáticas:

- Conceitos e evolução da IoT e IoMT;
- Arquiteturas e aplicações militares;
- Desafios técnicos (segurança, interoperabilidade, energia, escalabilidade);
- Tecnologias emergentes aplicadas (IA, *blockchain*, redes resilientes).

C - Análise crítica e síntese

Com base na literatura, realizou-se a análise dos impactos da IoMT nas operações de campo, relacionando benefícios estratégicos, limitações e perspectivas futuras. A síntese das informações foi estruturada de modo a fornecer um panorama claro e atualizado sobre o tema, sem recorrer a experimentos práticos ou simulações computacionais.

Assim, a metodologia aplicada permite não apenas compreender o estado atual da IoMT, mas também identificar tendências tecnológicas e apontar direções para pesquisas futuras, mantendo o foco no impacto da tecnologia nas operações militares em campo.

1.4 Organização do Documento

Este trabalho está estruturado em quatro capítulos principais, além de apêndices e referências, organizados de forma a garantir uma leitura lógica e coerente sobre o tema Internet das Coisas Militar e seu impacto nas operações de campo.

Na **Introdução**, apresenta-se o contexto geral do tema, destacando a relevância e justificativa do estudo, os objetivos gerais e específicos, a metodologia utilizada e a estrutura do documento.

Já na **Fundamentação Teórica**, discute-se os principais conceitos e bases teóricas relacionados à IoT e sua adaptação ao contexto militar (IoMT), abordando sua arquitetura, componentes, desafios e tecnologias de apoio. Este capítulo oferece o embasamento técnico e conceitual necessário para a compreensão do estudo.

Em **Resultados**, apresenta e analisa os resultados obtidos por meio da revisão bibliográfica, destacando o panorama das publicações selecionadas, as aplicações da IoMT nas operações de campo, bem como os principais desafios identificados na literatura científica.

No último capítulo **Considerações Finais, e Sugestões para Trabalhos Futuros**, sintetiza as conclusões do estudo, evidenciando as contribuições da pesquisa para a área, além de propor sugestões para trabalhos futuros, indicando possíveis direções de aprofundamento relacionadas à IoMT e sua aplicação em cenários operacionais.

O Quadro 1.2, apresentado sintetiza a estrutura do trabalho, evidenciando a organização dos capítulos e seus respectivos conteúdos. Por meio dessa representação, é possível visualizar de forma clara e objetiva a progressão lógica do estudo, desde a contextualização inicial do tema até a apresentação dos resultados, conclusões e sugestões para trabalhos futuros, facilitando a compreensão da estrutura geral do documento.

Quadro 1.2: *Organização do Documento*

Capítulo	Título	Descrição
Capítulo 1	Introdução	Apresenta a contextualização do tema, a justificativa e relevância do estudo, os objetivos geral e específicos, a metodologia adotada e a organização do documento.
Capítulo 2	Fundamentação Teórica	Discute os conceitos fundamentais relacionados à Internet das Coisas (IoT) e à Internet das Coisas Militar (IoMT), abordando sua evolução, arquitetura, componentes, desafios e tecnologias de apoio.
Capítulo 3	Resultados	Apresenta e analisa os resultados obtidos a partir da revisão bibliográfica, destacando o panorama das publicações selecionadas, as aplicações da IoMT nas operações de campo e os principais desafios identificados.
Capítulo 4	Considerações Finais e Sugestões para Trabalhos Futuros	Sintetiza as conclusões do estudo, evidencia as contribuições da pesquisa e propõe sugestões para trabalhos futuros relacionados à Internet das Coisas Militar e suas aplicações em cenários militares.

Fonte: Elaborado pelo autor (2025).

Capítulo 2

Fundamentação Teórica e Resultados

O Capítulo 2 traz a fundamentação teórica essencial para compreender a IoMT, contextualizando sua origem a partir da IoT civil e detalhando os principais conceitos, arquitetura em camadas, componentes e desafios técnicos enfrentados na integração dessa tecnologia ao setor de defesa. O capítulo explora como as soluções emergentes como inteligência artificial, *blockchain* e computação de borda estão transformando o uso de redes inteligentes nas operações militares, oferecendo uma base sólida para o entendimento estratégico e tecnológico que sustenta as aplicações da IoMT em cenários reais. Além disso, este capítulo apresenta e discute os resultados da pesquisa obtidos por meio da revisão bibliográfica, evidenciando tendências, aplicações, benefícios e limitações identificadas na literatura especializada.

2.1 A Evolução da Internet das Coisas (*IoT*)

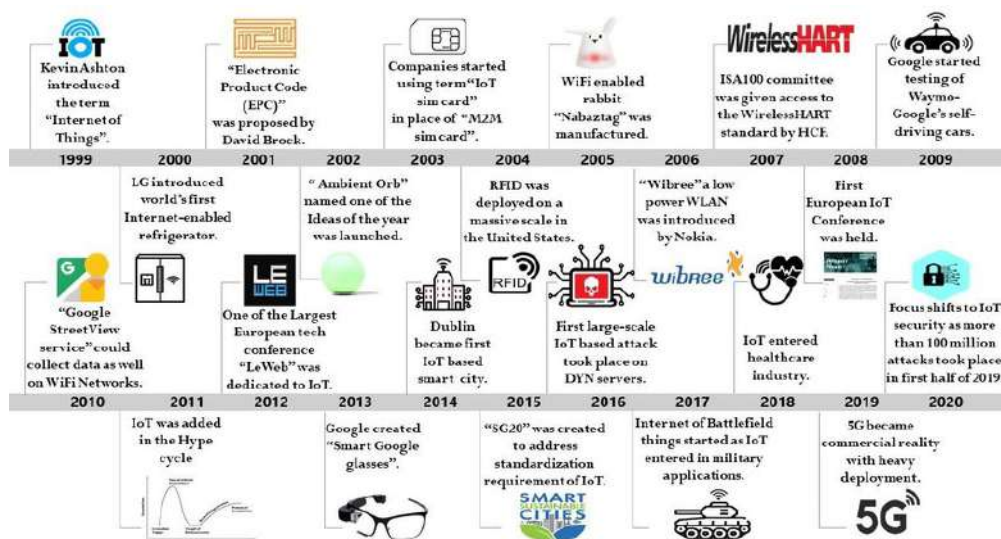
O IoT representa a interconexão de dispositivos físicos por meio da internet, permitindo a coleta, o processamento e a troca de informações em tempo real. Esse conceito emergiu no final da década de 1990, inicialmente voltado para aplicações civis, como automação residencial, cidades inteligentes, saúde digital e logística [Kikuchi 2023]. O avanço das tecnologias de comunicação sem fio, sensores de baixo custo e CN ampliou o alcance da IoT, tornando-a um dos pilares da chamada Indústria 4.0. Contudo, essa expansão trouxe desafios, sobretudo em relação à interoperabilidade, segurança e escalabilidade.

São mostrado na Figura 2.1, exemplos de dispositivos IoT usados no cotidiano, como aparelhos domésticos inteligentes, sensores em cidades inteligentes e logística. evidenciando o uso massivo da conectividade na vida civil. Essa imagem reforça que a IoT nasceu orientada a serviços voltados ao conforto, à automação e à eficiência em ambientes residenciais e urbanos.

Figura 2.1: *Dispositivos IoT Usados no Cotidiano*

<https://builtin.com/articles/iot-devices>.

É mostrado na Figura 2.2, uma visão mais técnica da IoT, apresentando os fluxos de dados entre sensores, redes e serviços em nuvem, além dos desafios de comunicação e integração. Esse diagrama evidencia como a consolidação de padrões de conectividade, computação em nuvem e sensores de baixo custo permitiu que a IoT se tornasse um pilar para sistemas complexos, abrindo caminho para aplicações em setores críticos.

Figura 2.2: *evolução da IoT*

<https://ieeexplore.ieee.org/document/9405669>.

É mostrado na Figura 2.3, o conceito de **Indústria 4.0**, relacionando a IoT à automação avançada, robótica, computação em nuvem e análise de dados em ambientes industriais. Com isso, a figura evidencia que a evolução da IoT ultrapassa o uso doméstico, tornando-se parte central de ecossistemas produtivos inteligentes, o que prepara o terreno para sua adaptação a cenários de alta criticidade, como a Internet das Coisas Militar.

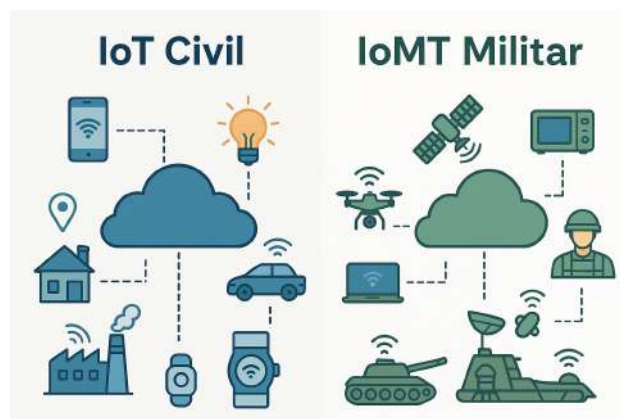
Figura 2.3: *Indústria 4.0*

<https://abracopel.org/blog/o-que-e-industria-4-0/>.

2.1.1 Da *IoT* para a Internet das Coisas Militar (*IoMT*)

Já a IoMT pode ser entendida como a adaptação da IoT para o ambiente de defesa. Diferente das aplicações civis, a IoMT opera em cenários de alta criticidade, onde atrasos na comunicação ou falhas de segurança podem comprometer missões e colocar vidas em risco [Wei 2021]. Nesse contexto, a IoMT conecta desde Veículo Aéreo Não Tripulado (*Unmanned Aerial Vehicle* - UAV), veículos autônomos e sensores de campo até sistemas de comando e controle, formando uma rede inteligente voltada à consciência situacional e à superioridade informacional [Kufakunesu, Myburgh e Freitas 2025]. Essa transição entre o uso civil e militar da tecnologia evidencia a capacidade de adaptação da IoT, transformando-se em um recurso crítico para operações de defesa.

São mostrado na Figura 2.4, os ecossistemas da IoT civil e da IoMT, evidenciando como a mesma tecnologia assume funções distintas conforme o contexto. No ambiente civil, a IoT integra dispositivos do cotidiano para automação e melhoria de serviços. Já na IoMT, a tecnologia é aplicada a sistemas críticos de defesa como *drones*, sensores, veículos táticos e satélites, exigindo maior segurança, resiliência e resposta em tempo real.

Figura 2.4: *IoT civil e IoMT*

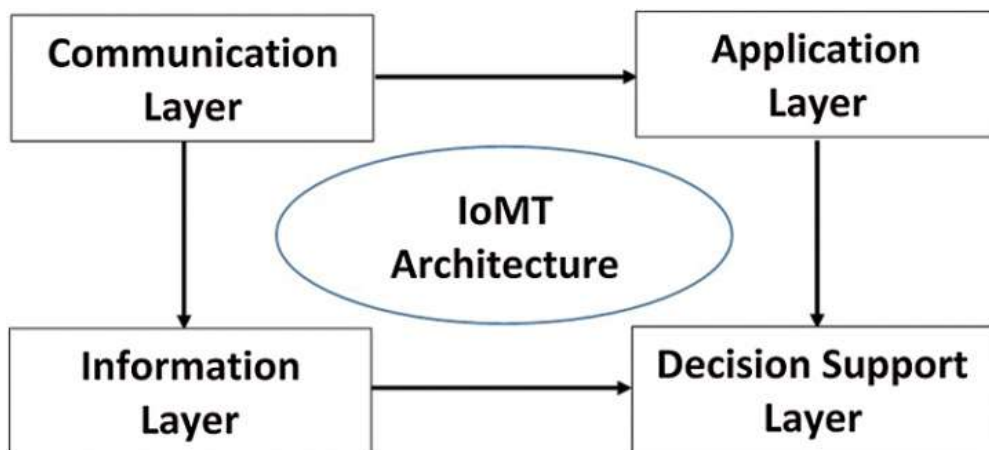
Fonte: Elaborado pelo Autor, 2025.

2.2 Arquitetura e Componentes da IoMT

A IoMT é composta por um conjunto de camadas interligadas que possibilitam a comunicação, o processamento e a tomada de decisões em ambientes militares de forma inteligente e segura. De acordo com [Tolba 2020], a arquitetura da IoMT é estruturada em quatro camadas principais: Comunicação, Processamento, Sensores e Dispositivos à Decisão.

É mostrada na Figura 2.5, a arquitetura em camadas da IoMT em um diagrama esquemático. Este modelo mostra de forma integrada e hierárquica a interação entre os diversos níveis do sistema, essencial para o pleno funcionamento de uma rede militar inteligente. A estrutura é composta por quatro camadas interdependentes: **Aplicação**, **Comunicação**, **Processamento** (ou Informação) e **Decisão**. Cada uma possui funções específicas, mas o seu trabalho conjunto assegura o fluxo contínuo e seguro das informações, desde a área de operações até os centros de comando e controle [Tolba 2020].

Figura 2.5: Camadas Principais da IoMT



<https://www.sciencedirect.com/org/science/article/pii/S1526149220002350>.

2.2.1 Camada de Aplicação

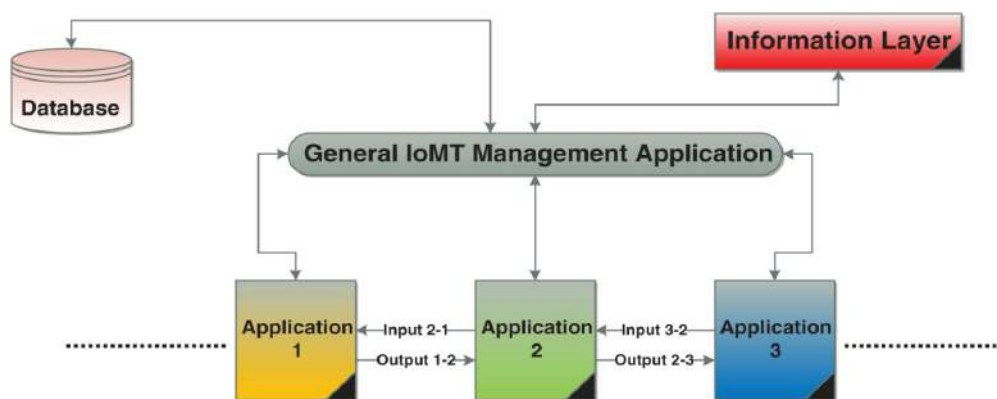
A Camada de Aplicação atua como o nível de integração e orquestração do sistema IoMT, gerenciando as diversas aplicações militares utilizadas em operações de guerra, como sistemas de vigilância, controle de armamento, gestão logística e comunicações táticas. Seu objetivo principal é unificar essas aplicações heterogêneas em uma plataforma coordenada, permitindo que operem de forma sinérgica e compartilhem dados de maneira eficiente através de interfaces padronizadas.

Esta camada é composta por uma aplicação de gerenciamento geral que controla e orquestra todas as aplicações individuais, uma base de dados central ou distribuída que armazena informações essenciais sobre entradas e saídas de cada aplicação, fluxos de dados, prazos de processamento e prioridades operacionais, e mecanismos de integração que permitem a troca automática de mensagens entre sistemas. A camada também define hierarquias de prioridade

baseadas no contexto tático em situações de múltiplas ameaças, aplicações defensivas são automaticamente priorizadas, garantindo respostas imediatas a cenários críticos e mantendo a eficácia operacional mesmo sob condições adversas [Tolba 2020].

É mostrado na Figura 2.6, um diagrama que representa a Camada de Aplicação da arquitetura IoMT. É apresentado como os sistemas militares incluindo vigilância, controle de armamentos, logística e comunicações são integrados em uma plataforma unificada e coordenada. As setas indicam o fluxo de dados entre as aplicações e os bancos de dados centrais, destacando os processos de priorização e sincronização em cenários com múltiplas ameaças.

Figura 2.6: *Camada de Aplicação*



<https://www.sciencedirect.com/org/science/article/pii/S1526149220002350>.

2.2.2 Camada de Comunicação

A Camada de Sensores e Comunicação atua como o elo entre os dispositivos físicos e a infraestrutura de rede que interliga todos os elementos do ambiente militar. Segundo [Tolba 2020], essa camada compreende a integração de diferentes redes como Redes de Sensores Sem Fio (*Wireless Sensor Networks* - WSN), Identificação Por Radiofrequência (*Radio-Frequency Identification* - RFID), Redes Ad Hoc Móveis (*Mobile Ad Hoc Networks* - MANET) e Satélites e Plataformas Aéreas de Alta Ititude (PAAA). Seu principal objetivo é garantir que as informações capturadas pelos sensores sejam transmitidas de forma rápida, segura e contínua, mesmo em ambientes com conectividade limitada. Em campo de batalha, onde falhas de comunicação podem comprometer missões inteiras, a arquitetura precisa oferecer tolerância a falhas e múltiplos caminhos alternativos de transmissão. Assim, utiliza-se o conceito de Sistema de Cobertura Tolerante a Falhas, em que redes distintas se complementam para manter a comunicação ativa. Outro desafio enfrentado por esta camada é a interoperabilidade entre diferentes tecnologias e padrões de comunicação. Para isso, são aplicadas técnicas de encapsulamento e tradução de cabeçalhos, possibilitando que pacotes de dados sejam compreendidos entre sistemas heterogêneos. A segurança também é um fator crítico, exigindo criptografia de dados, autenticação de nós e protocolos de comunicação resistentes a interferências e ataques. Portanto, a camada de sensores e comunicação é o esqueleto da IoMT,

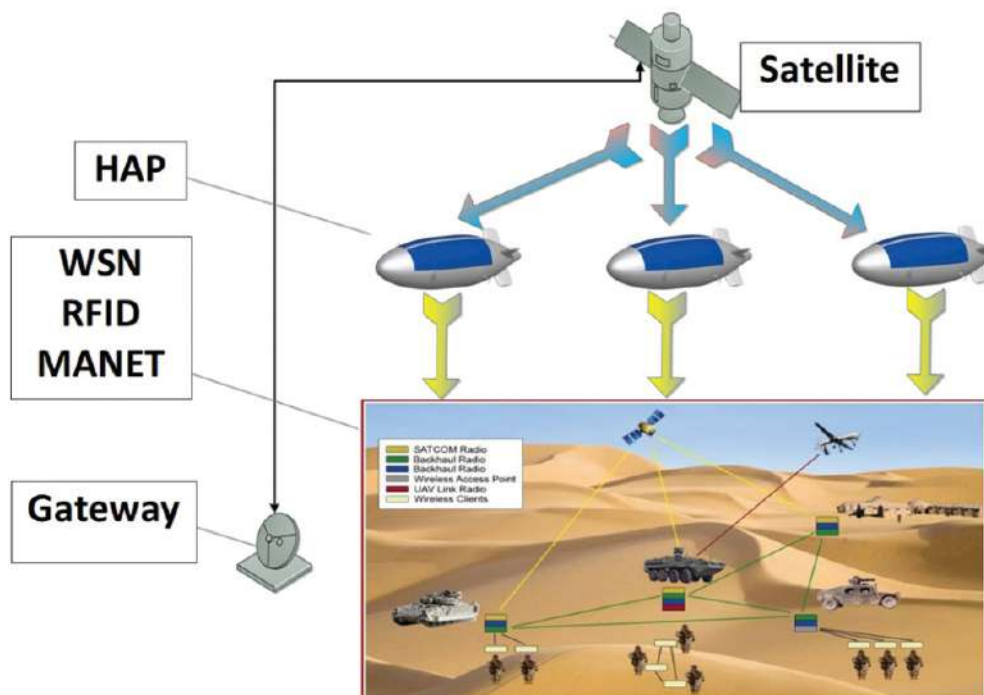
sustentando o fluxo de informações vitais que garantem consciência situacional, coordenação estratégica e vantagem tática. A integração de tecnologias complementares, como redes de sensores sem fio, redes móveis MANET, RFID e sistemas satelitais, possibilita a criação de redundância e diversificação das rotas de comunicação. Além disso, protocolos adaptativos e mecanismos de roteamento dinâmico são implementados, permitindo a reconfiguração automática das rotas diante de obstáculos ou falhas detectadas no ambiente.

O uso de algoritmos de IA embarcada contribui para o monitoramento em tempo real da qualidade do sinal, identificação de falhas e sugestão de alternativas viáveis para manter o fluxo de dados. A adoção de técnicas de encapsulamento e tradução de protocolos reforça a interoperabilidade entre dispositivos e sistemas heterogêneos presentes nas operações. Por fim, a aplicação de criptografia robusta e autenticação dos nós garante a confiabilidade e segurança das comunicações, mesmo diante de cenários adversos.

Essas abordagens tornam a camada de comunicação da IoMT mais robusta e preparada para contornar as limitações impostas por ambientes desconhecidos, proporcionando maior eficiência e confiabilidade nas operações militares que dependem desses recursos tecnológicos.

A Figura 2.7, representa a Camada de Comunicação, também denominada Camada de Sensores e Comunicação. Essa camada contempla as redes WSN, RFID, MANET e PAAA, responsáveis pela interconexão entre sensores, *drones* e satélites. O diagrama evidencia a interoperabilidade entre os diferentes sistemas e a existência de múltiplos caminhos de comunicação em ambientes militares, ressaltando aspectos como tolerância a falhas e redundância nas rotas de transmissão, fundamentais para garantir a confiabilidade e a continuidade das operações.

Figura 2.7: *Camada de Comunicação*



2.2.3 Camada de Processamento

A Camada de Processamento, também chamada de Camada de Informação, é o núcleo da arquitetura IoMT, responsável por transformar os dados brutos provenientes dos sensores em informações úteis, estruturadas e priorizadas. Nesse nível, ocorre a organização, filtragem, compressão, abstração e classificação das informações, com o objetivo de reduzir a sobrecarga de dados sem comprometer a qualidade e a precisão das análises. Devido à natureza dinâmica das operações militares, essa camada precisa lidar com grandes volumes de dados em tempo real, exigindo alto desempenho computacional e algoritmos otimizados de gerenciamento, [Tolba 2020]. Propõem um sistema de filas de prioridade composto por seis classes, em que dados críticos como detecção de inimigos ou alertas de ataque têm precedência máxima, enquanto dados menos urgentes são processados posteriormente. Esse mecanismo de priorização é essencial para garantir a Qualidade de Serviço (*Quality of Service* - QoS) em situações de congestionamento de rede. Além disso, técnicas de compressão e abstração reduzem o consumo de energia e melhoram a eficiência da transmissão. A segurança também é central, os dados passam por mecanismos de validação e criptografia antes de seguir para as camadas superiores. Assim, a Camada de Processamento atua como um filtro inteligente que assegura a entrega das informações certas, no momento certo, às unidades de comando e controle, favorecendo a rapidez e a precisão das decisões estratégicas.

Na Camada de Processamento, a classificação dos dados desempenha um papel essencial para garantir que as informações provenientes dos sensores sejam organizadas de forma eficiente e coerente com as necessidades operacionais. Para isso, são aplicadas diversas técnicas que trabalham de maneira integrada, contribuindo para reduzir a sobrecarga da rede, otimizar o tempo de resposta e assegurar que informações críticas cheguem rapidamente às camadas superiores [Tolba 2020].

A primeira técnica utilizada é a filtragem, responsável por eliminar dados redundantes, ruídos e informações irrelevantes. Essa etapa garante que apenas os dados úteis sigam para o processamento, evitando desperdício de energia e de capacidade de transmissão. Em seguida, a compressão reduz o volume dos dados, tornando a comunicação mais eficiente sem comprometer a qualidade das informações transmitidas [Tolba 2020].

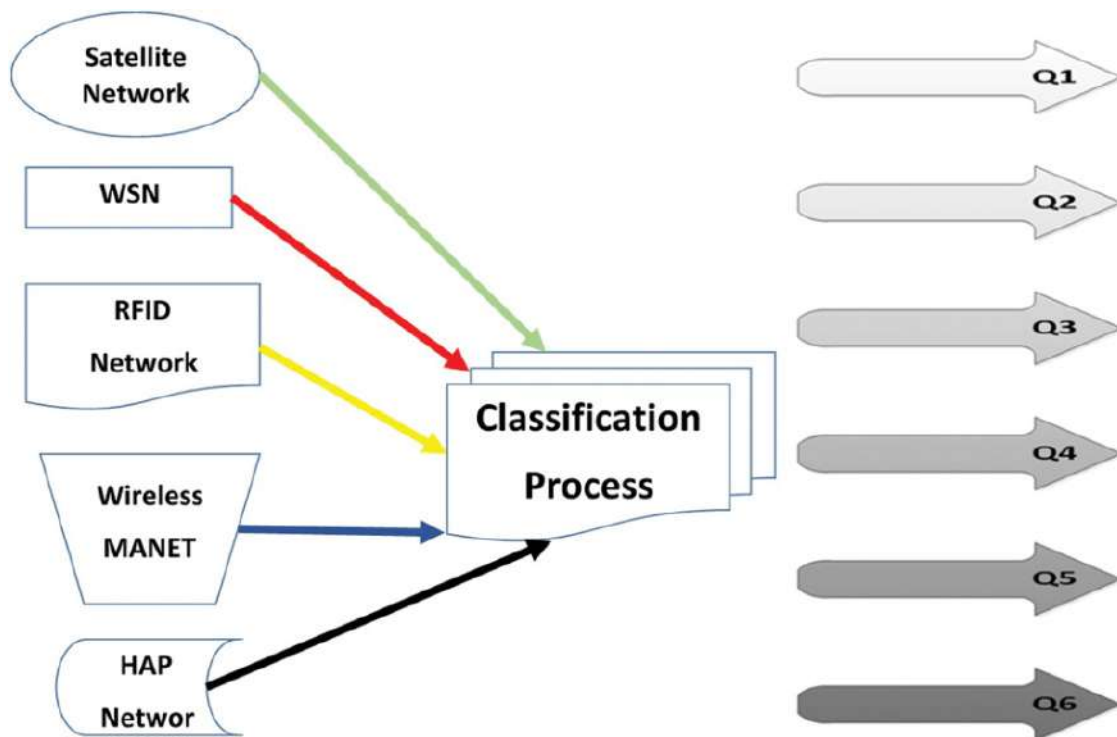
Outra técnica fundamental é a abstração, que transforma dados brutos em informações estruturadas e compreensíveis, facilitando a análise posterior. A classificação propriamente dita ocorre por meio da organização dos dados em categorias de acordo com sua natureza e relevância operacional. Esse processo é associado a um sistema de filas de prioridade, proposto por [Tolba 2020], composto por seis classes distintas. Nesse modelo, informações críticas como alertas de ataque ou detecção de inimigos recebem prioridade máxima, enquanto dados administrativos ou de baixa urgência são colocados em níveis inferiores.

A priorização funciona como o núcleo da classificação, garantindo que, em cenários de congestionamento ou limitações de largura de banda, os dados mais importantes sejam processados e encaminhados primeiro. Dessa forma, a camada atua como um filtro inteligente,

capaz de selecionar, organizar e encaminhar as informações adequadas ao momento operacional [Tolba 2020].

Na Figura 2.8, é apresentada a Camada de Processamento (ou de Informação). O diagrama exibe o fluxo de dados capturados pelos sensores sendo filtrados, classificados e priorizados. Mostra filas de prioridade (dados críticos, táticos, administrativos etc.), além de algoritmos de compressão e criptografia para reduzir consumo de energia e manter a qualidade do serviço.

Figura 2.8: *Camada de Processamento*



<https://www.sciencedirect.com/org/science/article/pii/S1526149220002350>.

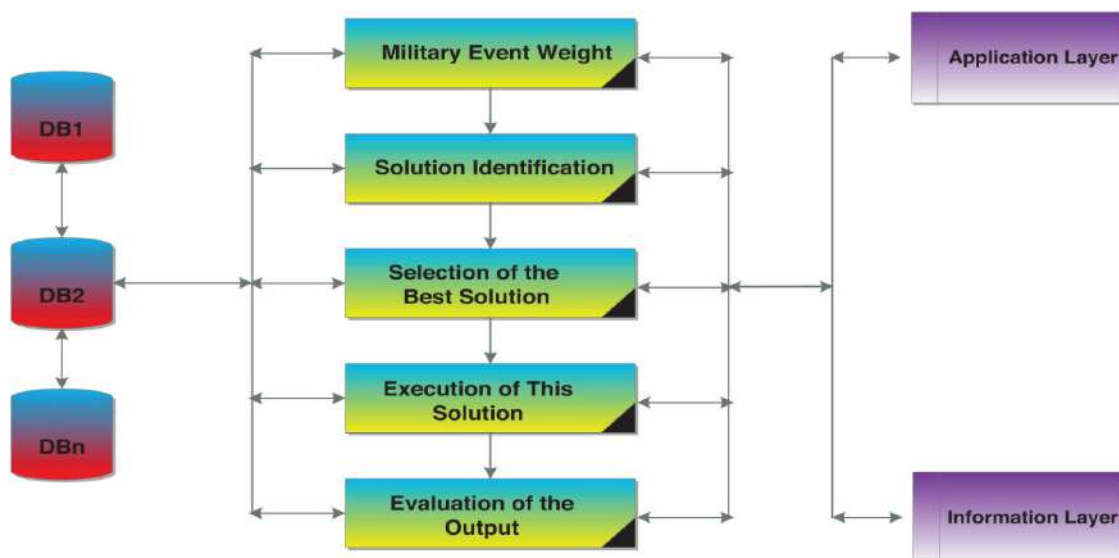
2.2.4 Camada de Decisão

A Camada de Decisão é o ponto culminante da arquitetura IoMT, onde as informações processadas são transformadas em conhecimento e ações concretas. Sua função é auxiliar comandantes e sistemas autônomos na tomada de decisões rápidas, seguras e embasadas em dados. Essa camada utiliza tecnologias de Sistemas de Apoio à Decisão (SAD), IA e modelagem preditiva para analisar cenários, avaliar riscos e sugerir as melhores estratégias operacionais. Segundo o modelo proposto por [Tolba 2020], o processo decisório é dividido em cinco etapas: **ponderação do evento**, **identificação de soluções**, **escolha da alternativa ideal**, **execução** e **avaliação do resultado**. Esse ciclo contínuo garante que cada decisão seja ajustada conforme o contexto de batalha, aumentando a adaptabilidade do sistema. Além disso, a Camada de Decisão depende fortemente da integração com a Camada de Aplicação e com os bancos de dados distribuídos, que armazenam informações históricas

e parâmetros táticos. Entre os principais desafios dessa camada estão o excesso ou falta de informações, a identificação incorreta de problemas e a superconfiança nos resultados das simulações. Portanto, mecanismos de validação cruzada e aprendizado adaptativo são essenciais para minimizar erros. Em suma, a Camada de Decisão é o cérebro do ecossistema IoMT, responsável por transformar dados em ações coordenadas, conferindo às forças armadas uma vantagem decisiva em ambientes de guerra centrados na informação [Tolba 2020].

É mostrado na Figura 2.9, um Diagrama da Camada de Decisão. Mostra o ciclo decisório em cinco etapas: Identificação do Evento → Geração de Alternativas → Escolha da Melhor Opção → Execução → Avaliação. Inclui blocos de Sistemas de Apoio à Decisão com Inteligência Artificial e *Machine Learning*, simbolizando a tomada de decisão autônoma e adaptativa em tempo real.

Figura 2.9: *Camada de Decisão*



<https://www.sciencedirect.com/org/science/article/pii/S1526149220002350>.

É resumido no Quadro 2.1 como o sistema IoMT é organizado em quatro camadas principais. A camada de aplicação integra e gerencia diferentes aplicações militares. A camada de comunicação realiza a transmissão dos dados entre dispositivos, assegurando continuidade e segurança em ambientes adversos. A camada de processamento filtra, comprime e prioriza os dados, facilitando a análise e a tomada de decisão, além de exigir alta performance. Por fim, a camada de decisão utiliza inteligência artificial e *machine learning* para transformar dados em ações, incluindo modelagem preditiva, avaliação de risco e validação.

Quadro 2.1: *Camadas do sistema IoMT e suas descrições resumidas*

Camadas	Descrição resumida
Camada de Aplicação	Responsável pela integração e orquestração do sistema IoMT, gerenciando diversas aplicações militares.
Camada de Comunicação	Assegura a transmissão de dados entre dispositivos e infraestrutura (WSN, MANET, RFID e satélites), garantindo continuidade, múltiplos caminhos e segurança, mesmo em ambientes adversos.
Camada de Processamento de Informação	Realiza filtragem, compressão e priorização dos dados, reduzindo a sobrecarga e preparando as informações para análise e tomada de decisão, exigindo alto desempenho e qualidade de serviço (QoS).
Camada de Decisão	Suporta sistemas de apoio à decisão baseados em IA e ML, transformando informações em ações, incluindo modelagem preditiva, avaliação de riscos e validação.

Fonte: Elaborado pelo Autor, 2025.

2.3 Desafios da *IoMT*

Os desafios da IoMT envolvem principalmente **Segurança**, **Interoperabilidade**, **Consumo de Energia** e **Escalabilidade**. A segurança é um ponto crítico, pois os dispositivos trocam informações sigilosas que podem ser alvo de ataques cibernéticos. A interoperabilidade exige a integração de diferentes sistemas e tecnologias, o que nem sempre é simples. O consumo de energia também é um desafio, já que muitos dispositivos operam em locais remotos com recursos limitados. Por fim, a escalabilidade demanda redes e infraestruturas capazes de suportar o crescente número de dispositivos conectados [Mezrioui 2017]. Superar esses desafios é essencial para garantir o uso eficiente e seguro da IoMT em operações militares.

2.3.1 Segurança

A cibersegurança é um dos maiores pontos de vulnerabilidade da IoMT, já que a expansão da rede amplia a superfície de ataque. A coleta, transmissão e processamento de dados estratégicos tornam o sistema um alvo altamente atrativo para ciberataques. Entre as principais ameaças estão ataques de Negação de Serviço (*Denial of Service - DoS*) e Negação de Serviço Distribuída (*Distributed Denial of Service - DDoS*), *spoofing* (falsificação de identidade) e inserção de *malwares* em dispositivos de campo. Como os dados da IoMT frequentemente envolvem informações críticas de inteligência e logística, sua violação pode comprometer

a segurança nacional, sabotando operações inteiras [Tortonesi 2017]. Dessa forma, garantir a Confidencialidade, Integridade e Disponibilidade (CID) das informações é um requisito essencial para manter a confiança e a resiliência da infraestrutura militar conectada.

É mostrado na Figura 2.10, um cenário militar conectado, destacando como dispositivos, sensores e sistemas inteligentes podem ser usados para detectar e responder a ameaças em tempo real. Ela reforça a importância da segurança cibernética, mostrando que a IoMT amplia a capacidade de vigilância, mas também aumenta a superfície de ataque, exigindo maior proteção contra invasões e interferências.

Figura 2.10: *Sistema de Segurança e Vigilância*



<https://www.businessinsider.com/>.

2.3.2 Interoperabilidade

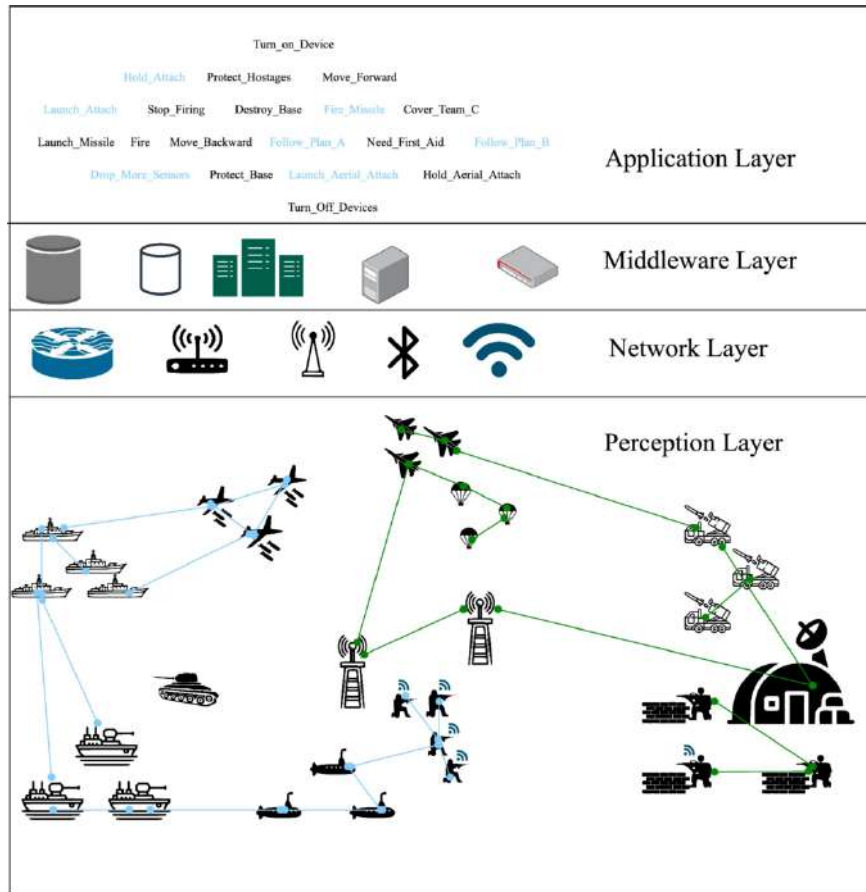
A interoperabilidade refere-se à capacidade de diferentes dispositivos, sistemas e plataformas se comunicarem e funcionarem de forma integrada, independentemente de seus fabricantes ou tecnologias utilizadas [West 2016]. No contexto da IoMT, este é um desafio crítico, pois os equipamentos militares muitas vezes são produzidos por fornecedores distintos e utilizam protocolos variados. A ausência de padronização internacional pode comprometer a eficiência das operações conjuntas, dificultando a troca de informações em tempo real. Esse problema se agrava em missões multinacionais, onde a integração de sistemas legados e novas tecnologias precisa ocorrer sem perda de confiabilidade ou de velocidade. Assim, a interoperabilidade é um requisito fundamental para assegurar que toda a rede de dispositivos militares funcione como um ecossistema unificado.

A interoperabilidade na IoMT depende cada vez mais da adoção de padrões internacionais. Apesar de ainda ser um desafio consolidar normas globais que permitam a integração eficiente entre diferentes dispositivos e sistemas, já existem avanços significativos na direção da padronização. Soluções como *middleware* adaptativo e redes definidas por *software* estão facilitando a comunicação entre plataformas distintas, e a tendência é que a harmonização internacional desses padrões seja fundamental para operações militares conjuntas, seguras e eficazes.

Na Figura 2.11, apresenta-se um diagrama técnico com integração entre sistemas militares distintos. Ela evidencia a necessidade de interoperabilidade entre dispositivos, redes

e plataformas de diferentes fabricantes. Mostra visualmente como a falta de padronização pode prejudicar o fluxo contínuo de informações em operações conjuntas.

Figura 2.11: *Integração Entre Sistemas Militares Distintos*



<https://link.springer.com/article/10.1007/s43926-025-00093-w>.

2.3.3 Consumo de Energia

O consumo de energia é outro desafio relevante, principalmente porque grande parte dos dispositivos utilizados em operações militares é alimentado por baterias. Em ambientes hostis e de difícil acesso, o reabastecimento energético é limitado, e isso impacta diretamente a autonomia dos equipamentos. Além disso, protocolos avançados de segurança, criptografia e processamento de dados exigem maior consumo energético, o que reduz o tempo de operação em campo [Mezrioui 2017]. A falta de soluções energéticas eficientes pode comprometer a durabilidade dos sensores e dispositivos, afetando a continuidade das missões. Por isso, novas abordagens, como o uso de baterias de longa duração, protocolos de baixo consumo e fontes alternativas de energia, são essenciais para garantir a funcionalidade da IoMT em operações prolongadas.

A Figura 2.12, traz um conceito visual de dispositivos IoT operando em tempo real, simbolizando a alta demanda energética em sistemas conectados. Ela remete ao desafio da autonomia dos sensores e equipamentos utilizados.

Figura 2.12: *Consumo de energia em sistemas IoT em tempo real*

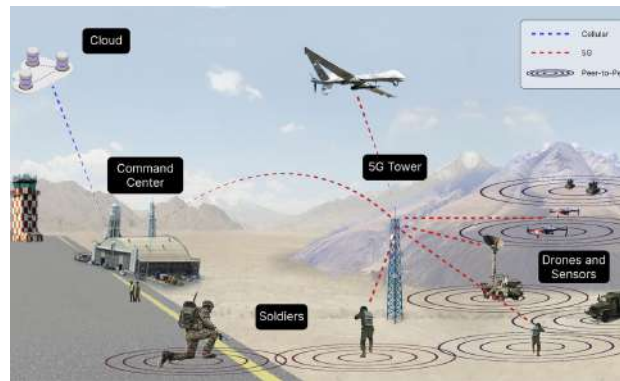


<https://artificialpaintings.com/es/blog/tag/tiempo-real/page/3/>.

2.3.4 Escalabilidade

A escalabilidade diz respeito à capacidade da rede IoMT de se expandir sem perder eficiência, confiabilidade ou estabilidade. Em cenários militares, o número de dispositivos conectados cresce exponencialmente desde *drones* e sensores de campo até veículos autônomos e sistemas de monitoramento. [Mezrioui 2017] Esse crescimento massivo aumenta a complexidade de gerenciamento da rede, podendo gerar lentidão, instabilidade e vulnerabilidades de segurança. Caso não seja bem planejada, a escalabilidade limitada pode transformar a IoMT em uma rede difícil de administrar, tornando-se um ponto de falha em situações críticas. Logo, é necessário desenvolver arquiteturas resilientes (estruturas de sistemas projetadas para continuar operando, mesmo diante de falhas, ataques, perdas de comunicação ou condições adversas) e protocolos adaptativos que mantenham a performance mesmo diante da expansão do ecossistema.

É mostrada a Figura 2.13, o uso combinado de IoT, IA e tecnologias emergentes aplicadas ao campo de batalha. Representa um ambiente militar altamente conectado, com múltiplos dispositivos inteligentes operando simultaneamente, evidenciando o desafio da escalabilidade das redes IoMT diante do rápido crescimento do número de sensores e sistemas em operação.

Figura 2.13: *Tecnologias Emergentes Aplicadas ao Campo de Batalha*

<https://militaryembedded.com/ai/deep-learning/iot-ai-and-the-future-battlefield>.

2.4 Tecnologias de Apoio e Soluções Emergentes

As tecnologias de apoio e as soluções emergentes têm papel essencial na consolidação e segurança da IoMT. Entre elas, destacam-se a Inteligência Artificial (*Artificial Intelligence*) e o Aprendizado de Máquina (*Machine Learning* - ML), que permitem a detecção de anomalias, a análise preditiva e a resposta rápida a ataques cibernéticos, garantindo maior eficiência e autonomia nas operações [Elshweikh 2022]. A tecnologia *blockchain* surge como ferramenta de segurança e rastreabilidade, assegurando a integridade e autenticidade dos dados trocados entre dispositivos militares [Keshk 2024]. Além disso, as redes resilientes e os protocolos adaptativos oferecem comunicação contínua mesmo em ambientes hostis, reforçando a robustez da infraestrutura [Shirvani 2022]. Outra inovação relevante é a Computação de Borda (*Edge Computing* - EC), que possibilita o processamento de informações localmente, reduzindo a latência e garantindo decisões em tempo real, mesmo com conectividade limitada [Tolba 2020]. Essas soluções, quando integradas, fortalecem o ecossistema da IoMT e ampliam sua confiabilidade em cenários de missão crítica.

Dentro da IA, uma das áreas de maior destaque é o ML. Consiste em um conjunto de técnicas que permitem que algoritmos aprendam a partir de dados históricos, reconhecendo padrões e realizando previsões ou classificações sem a necessidade de programação explícita para cada tarefa. Em outras palavras, o sistema se aperfeiçoa continuamente quanto mais informações processa, tornando-se mais preciso e eficiente ao longo do tempo. [Elshweikh 2022].

Tanto a IA como ML permitem detecção de anomalias, análise preditiva e resposta a ataques em tempo real. A IA pode ser definida como o ramo da ciência da computação que busca desenvolver sistemas capazes de simular comportamentos inteligentes, reproduzindo aspectos do raciocínio humano, como aprendizado, tomada de decisão e adaptação a novas situações. Diferente de *softwares* convencionais, que seguem regras rígidas previamente programadas, a IA é capaz de analisar dados, identificar padrões e ajustar seu funcionamento

de forma dinâmica, aproximando-se de um processo cognitivo.

a) Inteligência Artificial e Machine Learning: IA e o ML representam o núcleo das soluções emergentes aplicadas à IoMT. A principal contribuição dessas tecnologias está na capacidade de processar grandes volumes de dados provenientes de sensores, *drones* e dispositivos em campo, identificando padrões, anomalias e tendências operacionais. [Wei 2021] demonstra que algoritmos de IA são empregados em SAD, capazes de avaliar variáveis como topografia, movimentação inimiga e condições climáticas, fornecendo recomendações táticas em tempo real. Já o ML é amplamente utilizado na detecção de ameaças cibernéticas, em que modelos supervisionados e não supervisionados aprendem a reconhecer comportamentos suspeitos e ativar respostas automáticas de defesa. Em suma, IA e ML não apenas automatizam tarefas, mas também aumentam a previsibilidade e a precisão das decisões estratégicas, reduzindo o tempo de reação em ambientes dinâmicos.

b) Blockchain e Segurança da Informação: O *Blockchain* vem sendo apontado como uma das tecnologias mais promissoras para reforçar a segurança e a integridade dos dados em sistemas IoMT. Sua estrutura descentralizada permite o registro imutável das transações realizadas entre dispositivos, dificultando tentativas de adulteração ou falsificação de informações [Mezrioui 2017]. Além disso, o uso de contratos inteligentes (*smart contracts*) garante a autenticação automatizada de nós na rede, eliminando a necessidade de intermediários e reduzindo o risco de ataques de invasão. [Tolba 2020] enfatiza que a aplicação do *Blockchain* em redes militares cria um ambiente de confiança distribuída, essencial para comunicações seguras entre unidades e veículos autônomos.

c) Computação em Nuvem, Borda e Névoa: A CN continua sendo uma base indispensável para o armazenamento e processamento massivo de dados militares, porém, sua dependência de conectividade estável limita o uso em operações de campo. Por essa razão, a literatura destaca a adoção de modelos híbridos, como a EC e a *Fog Computing* (Computação de Névoa - CNé), que descentralizam o processamento para mais próximo da fonte dos dados [Kufakunesu, Myburgh e Freitas 2025]. Essa abordagem reduz a latência e aumenta a confiabilidade em cenários com restrições de rede. Além disso, permite que decisões críticas sejam tomadas localmente, sem a necessidade de enviar todas as informações para centros de comando distantes um diferencial essencial em combates de curta duração ou sob interferência de sinal.

d) Redes Resilientes e Arquiteturas Adaptativas: A resiliência da IoMT está diretamente ligada ao desempenho de suas infraestruturas de comunicação. As redes MANET e WSN são amplamente adotadas por sua capacidade de autoconfiguração e adaptação em ambientes instáveis. Elas garantem que os dispositivos mantenham a comunicação mesmo diante de falhas, ataques ou perda de nós intermediários [Tolba 2020]. De acordo com [Wei

2021], essas redes, quando combinadas com algoritmos de roteamento dinâmico e IA embarcada, criam um sistema de cobertura tolerante a falhas, permitindo continuidade de operação mesmo em condições extremas. Essa característica é considerada um dos pilares da guerra informacional moderna, em que a redundância e a adaptabilidade da rede determinam o sucesso das missões.

O Quadro 2.2 apresenta as tecnologias emergentes que fortalecem a IoMT, incluindo IA, ML, *Blockchain*, EC e redes MANET/WSN. Elas permitem automação, segurança de dados, processamento local e comunicação resiliente, tornando as operações militares mais eficientes e seguras.

Quadro 2.2: *Tecnologias Emergentes e Soluções de Apoio*

Tecnologia	Função Principal	Benefícios Estratégicos	Referências
Inteligência Artificial (IA)	Análise e tomada de decisão autônoma.	Redução do tempo de resposta e precisão nas estratégias.	Wei (2021); Tolba (2020)
Machine Learning (ML)	Aprendizado adaptativo e detecção de anomalias.	Identificação precoce de ameaças e otimização de desempenho.	Wei (2021)
Blockchain	Registro descentralizado e autenticação segura.	Integridade dos dados e confiabilidade entre unidades.	Mezrioui (2017); Tolba (2020)
Edge/Fog Computing	Processamento local distribuído.	Redução de latência e maior autonomia operacional.	Kufakunesu et al. (2025)
Redes MANET/WSN	Comunicação autônoma e resiliente.	Continuidade da rede em cenários críticos e falhas.	Tolba (2020); Wei (2021)

Elaborado por J. Wesley (2025), com base em [Wei 2021; Tolba 2020] e [Mezrioui 2017].

2.5 Perspectivas Futuras

O futuro da IoMT aponta para a consolidação de sistemas autônomos, inteligentes e distribuídos, capazes de operar com mínima intervenção humana. A integração de IA, *blockchain* e computação em borda tende a aumentar a resiliência e a confiabilidade das operações militares [Shirvani 2022]. Além disso, espera-se a criação de padrões internacionais de interoperabilidade para reduzir a fragmentação tecnológica e viabilizar coalizões militares mais eficientes.

Capítulo 3

Resultados

3.1 Panorama Geral das Publicações Seleccionadas

A Figura 3.1, mostra um gráfico de pizza que sintetiza a proporção total das publicações para cada termo analisado. Observa-se que o termo IoT representa aproximadamente 57,1% (579.139) de todo o material encontrado (1.013.462 resultados), reforçando sua predominância. Em seguida, aparece IoT *Security*, com cerca de 21% (212.816), destacando o crescente interesse em temas ligados à segurança em ambientes conectados. Os termos IoT *of Battle* e *Drone* apresentam proporções moderadas, enquanto IoT *Military* possui a menor participação, com apenas 2,8% (28.656), evidenciando a limitação de estudos específicos sobre esse tópico.

Proporção Total de Resultados por Termo Pesquisado

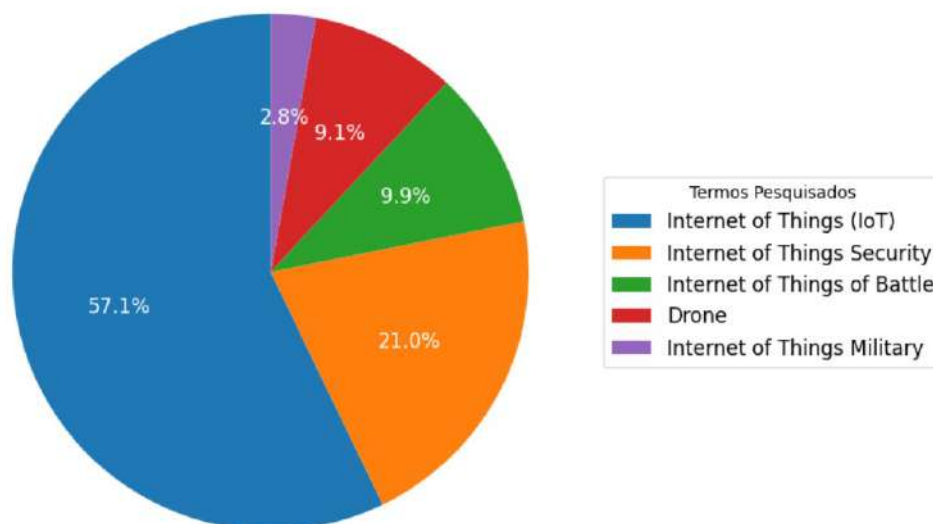


Figura 3.1: Elaborado pelo Autor, 2025, Levantamentos.

A revisão bibliográfica realizada sobre a IoMT revelou um campo de estudo em plena expansão, caracterizado pela integração crescente entre tecnologias de comunicação, senso-

riamento e inteligência computacional no contexto de defesa. Foram analisadas publicações disponíveis em bases científicas de relevância internacional, como *IEEE Xplore*, *Springer-Link*, *ScienceDirect*, *Scopus* e *Google Scholar*, com foco em estudos publicados entre 2017 e 2025. Desse conjunto, foram selecionados 12 artigos científicos com maior aderência aos objetivos desta pesquisa, evidenciando o predomínio de estudos acadêmicos na composição da fundamentação teórica adotada.

O levantamento mostrado na Figura 3.2, identificou que a maioria dos trabalhos recentes concentra-se em arquiteturas de comunicação seguras, sistemas de apoio à decisão e infraestruturas de comando e controle distribuídas (743.269, publicações realizadas entre 2017 e 2025). Cerca de 36,3% das publicações revisadas abordam a aplicação direta da IoT no ambiente militar, enquanto aproximadamente 10,5% exploram aspectos de segurança e interoperabilidade, e os 53,1% restantes tratam de soluções emergentes, como o uso de IA, ML e *Blockchain* na mitigação de riscos e otimização de processos operacionais.

Proporção Total de Publicações por Categoria

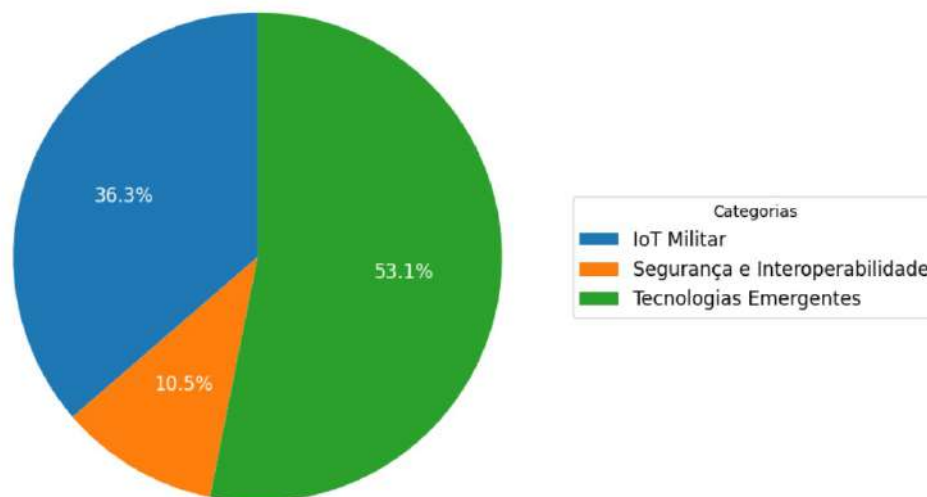


Figura 3.2: *Elaborado pelo Autor, 2025, Levantamentos.*

De modo geral, observou-se que a literatura apresenta uma convergência teórica em torno do conceito de superioridade informacional, entendida como a capacidade de coletar, processar e distribuir informações com maior velocidade e precisão do que o adversário [Tolba 2020]. Essa noção aparece como o eixo central da maioria dos estudos, evidenciando que o diferencial competitivo nas operações militares modernas não reside apenas na força bélica, mas principalmente na eficiência do fluxo de dados e na inteligência aplicada às decisões táticas.

Outro aspecto relevante identificado é a ênfase crescente em sistemas autônomos e infraestruturas distribuídas, que visam reduzir a dependência de centros de comando fixos. Trabalhos recentes [Wei 2021; Kufakunesu, Myburgh e Freitas 2025], destacam a importância de redes MANETs e WSNs como pilares para a comunicação descentralizada em campo

de batalha, garantindo resiliência mesmo em cenários de falha parcial de conectividade.

As publicações também revelam uma tendência de integração entre sensores, *drones* e veículos terrestres, compondo ecossistemas híbridos capazes de compartilhar informações em tempo real. Essa abordagem, denominada por alguns autores de Internet das Coisas de Batalha (*Internet of Battle Things* - IoBT), representa uma ramificação direta da IoMT voltada à automação e coordenação autônoma de dispositivos em ambiente *hostil*.

Além disso, nota-se um avanço significativo nas discussões sobre cibersegurança. Autores como [Mezrioui 2017] e [Tortonesi 2017] ressaltam que a proteção das redes militares conectadas é um dos maiores desafios da era digital, dado o elevado risco de ataques DoS e DDoS em sistemas críticos. Esse tópico aparece de forma recorrente, indicando que a segurança da informação é tratada como elemento transversal em todas as camadas da arquitetura IoMT desde os sensores até os sistemas de decisão.

Por fim, o panorama geral evidencia que a literatura sobre IoMT ainda se encontra em estágio de consolidação, com abundância de pesquisas conceituais e prototipais, mas escassez de validações empíricas em ambientes reais. Essa constatação reforça a importância deste trabalho, que busca sistematizar os conhecimentos existentes e identificar os principais avanços, limitações e tendências que moldam o desenvolvimento da IoMT no cenário militar contemporâneo.

3.2 Principais Desafios da IoMT

A análise dos estudos selecionados evidencia que, embora a IoMT apresente elevado potencial estratégico, sua implementação em ambientes reais enfrenta um conjunto expressivo de desafios técnicos, operacionais e de segurança. Esses obstáculos, frequentemente inter-relacionados, limitam a escalabilidade das soluções e comprometem a confiabilidade das operações militares baseadas em conectividade distribuída.

Os quatro principais eixos de dificuldade mais citados na literatura são: **Interoperabilidade, Cibersegurança, Consumo de Energia e Escalabilidade** [Mezrioui 2017; Tolba 2020; Tortonesi 2017]. Cada um desses fatores representa um gargalo crítico no desenvolvimento e na consolidação de sistemas IoMT em larga escala.

a) A **Interoperabilidade** é apontada como um dos maiores desafios para a consolidação da IoMT. Diferentes fabricantes, protocolos de comunicação e padrões de criptografia resultam em sistemas fragmentados que dificultam a integração entre dispositivos. Essa limitação compromete a fluidez dos dados e a coordenação tática das unidades em campo. [Tolba 2020] destaca que, em operações conjuntas entre forças de defesa, a ausência de um padrão unificado de interoperabilidade gera atrasos no compartilhamento de informações e falhas de sincronização entre sensores e plataformas autônomas. Trabalhos recentes [Kufakunesu, Myburgh e Freitas 2025] sugerem que o uso de *middleware* adaptativo e de Rede Definida

por *Software (Software Defined Networking - SDN)* pode mitigar parte desse problema, permitindo a tradução automática entre protocolos distintos e a adaptação dinâmica do tráfego de dados.

b) A **Cibersegurança** é o eixo mais recorrente nas publicações sobre IoMT, sendo tratada como o ponto mais sensível da arquitetura. Como os dispositivos militares estão conectados a redes sem fio e expostos a interferências externas, tornam-se alvos potenciais de ataques cibernéticos. [Mezrioui 2017] e [Tortonesi 2017] observam que ataques DoS, DDoS e tentativas de interceptação de dados representam riscos concretos em missões críticas. A natureza descentralizada da IoMT amplia a superfície de vulnerabilidade, exigindo protocolos criptográficos robustos, autenticação multifatorial e mecanismos de detecção em tempo real. Alguns estudos propõem a aplicação de *blockchain* e aprendizado de máquina para fortalecer a defesa cibernética, por meio da validação descentralizada das transações e da detecção automática de anomalias em fluxos de dados [Wei 2021].

c) Amplamente documentado é o **Consumo Energético** elevado dos dispositivos embarcados, especialmente em operações de longa duração. A necessidade de manter sensores, câmeras e módulos de comunicação ativos constantemente aumenta a demanda energética e reduz a autonomia dos sistemas [Tolba 2020]. A literatura aponta que a eficiência energética é crucial, sobretudo em ambientes remotos ou hostis, onde a substituição de baterias é inviável. Estratégias como redes de energia hierarquizadas, transmissão adaptativa e o uso de fontes de energia alternativas (como solar e cinética) têm sido estudadas para mitigar esse problema [Kufakunesu, Myburgh e Freitas 2025].

d) A **Escalabilidade** também surge como um desafio significativo, relacionado à capacidade de as redes IoMT suportarem o crescimento exponencial de dispositivos conectados sem comprometer o desempenho. À medida que novas unidades, sensores e veículos autônomos são adicionados à rede, aumenta-se a complexidade da gestão de dados e o risco de sobrecarga de comunicação [Wei 2021]. A literatura propõe soluções baseadas em arquiteturas em nuvem híbrida e EC, que permitem descentralizar o processamento de dados e reduzir a latência. No entanto, há consenso de que ainda faltam padrões consolidados para garantir a escalabilidade segura e eficiente da IoMT em cenários militares de grande porte.

É apresentado o Quadro 3.1 os principais desafios da IoMT, sintetizando os aspectos discutidos anteriormente e Também aponta soluções tecnológicas, como o uso de *blockchain*, IA, *Edge Computing* e SDN.

Quadro 3.1: *Comparativo entre os Principais Desafios da IoMT*

Desafio	Descrição	Consequências Operacionais	Soluções Propostas
Interoperabilidade	Dificuldade de integração entre diferentes protocolos e dispositivos.	Falhas na comunicação entre unidades e atrasos em decisões táticas.	Middleware adaptativo, SDN e padronização de protocolos.
Cibersegurança	Vulnerabilidade a ataques cibernéticos (DoS, DDoS, interceptação).	Comprometimento da integridade dos dados e falhas em missões.	Criptografia avançada, Blockchain e IA para detecção de anomalias.
Consumo de Energia	Alta demanda energética de sensores e transmissores em campo.	Redução da autonomia operacional e perda de conectividade.	Fontes alternativas, redes hierarquizadas e transmissão inteligente.
Escalabilidade	Dificuldade de expansão da rede com estabilidade e baixa latência.	Congestionamento e queda de desempenho em redes complexas.	Cloud híbrida, Edge Computing e controle distribuído.

Adaptado de [Mezrioui 2017], [Tolba 2020] e [Kufakunesu, Myburgh e Freitas 2025].

3.2.1 Aplicações e Benefícios da *IoMT* nas Operações de Campo

A literatura especializada demonstra que a *IoMT* vem transformando significativamente a maneira como as forças armadas conduzem suas operações de campo. Essa tecnologia permite a interconexão inteligente de sensores, veículos, *drones*, sistemas de comando e combatentes, criando uma rede autônoma capaz de coletar, processar e compartilhar informações em tempo real [Wei 2021]. Os estudos revisados convergem ao destacar que a *IoMT* proporciona avanços expressivos em **Vigilância, Logística, Comando e Controle**, bem como no **Monitoramento de Tropas e Apoio à Decisão Estratégica**.

a) Vigilância e Reconhecimento: Uma das aplicações mais recorrentes da *IoMT* está no campo da vigilância e reconhecimento tático. Sensores embarcados em *drones*, veículos terrestres e dispositivos vestíveis permitem o monitoramento contínuo de áreas de interesse, fornecendo dados em tempo real sobre movimentações inimigas, condições ambientais e rotas de patrulha. [Tolba 2020] descreve que o uso WSN possibilita uma vigilância perimetral mais precisa e de baixo custo, ampliando a consciência situacional do comando militar. Em missões de reconhecimento, essa integração reduz o risco humano e acelera a tomada de decisão, já que as informações são processadas e distribuídas automaticamente entre as unidades conectadas.

b) Logística e Gerenciamento de Recursos: A IoMT também tem se mostrado essencial na otimização da cadeia logística militar, um setor historicamente complexo e sujeito a falhas. Por meio de sensores RFID e módulos de rastreamento, é possível monitorar em tempo real o deslocamento de equipamentos, munições e suprimentos, garantindo maior controle sobre o fluxo de materiais [Wei 2021]. [Kufakunesu, Myburgh e Freitas 2025] apontam que o uso de plataformas de dados integradas reduz perdas logísticas e melhora a previsão de reabastecimento, minimizando atrasos em operações críticas. Além disso, a análise preditiva aplicada a esses dados permite antecipar falhas de equipamentos e realizar manutenção preventiva, evitando quebras inesperadas durante missões.

c) Comando, Controle e Coordenação: Outra aplicação central está nas áreas de Comando, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento (CCCI-IVR). A IoMT permite a coordenação entre múltiplas unidades em campo, estabelecendo uma infraestrutura de comunicação confiável e descentralizada. Segundo [Tolba 2020], o uso de redes MANET possibilita que soldados, veículos e *drones* troquem informações mesmo na ausência de uma infraestrutura fixa. Essa comunicação dinâmica aumenta a resiliência operacional e a capacidade de resposta em tempo real, fatores cruciais em ambientes de combate altamente voláteis. Adicionalmente, a aplicação de SAD integrados à IoMT fornece aos comandantes uma visão consolidada do campo de batalha, permitindo análises preditivas, simulações táticas e respostas automatizadas em situações emergenciais.

d) Monitoramento de Tropas e Saúde Operacional: A IoMT também se destaca no monitoramento biométrico e fisiológico de soldados em campo. Dispositivos vestíveis equipados com sensores podem registrar sinais vitais, níveis de fadiga, temperatura corporal e até mesmo indicadores de estresse. Essas informações são transmitidas para centros de comando, onde algoritmos de ML analisam padrões e alertam sobre possíveis riscos à saúde ou à eficiência do combatente [Wei 2021]. Essa capacidade de acompanhamento contínuo não apenas aumenta a segurança individual, mas também possibilita o redesenho tático das missões conforme o estado físico das tropas, contribuindo para a tomada de decisões mais humanas e eficientes.

É descrito o Quadro 3.2 as principais aplicações e benefícios da IoMT nas operações de campo, como vigilância em tempo real, rastreamento logístico, comando e controle integrados e monitoramento biométrico das tropas. Essas aplicações resultam em maior consciência situacional, economia de recursos e decisões mais precisas.

Quadro 3.2: *Principais Aplicações e Benefícios da IoMT nas Operações de Campo*

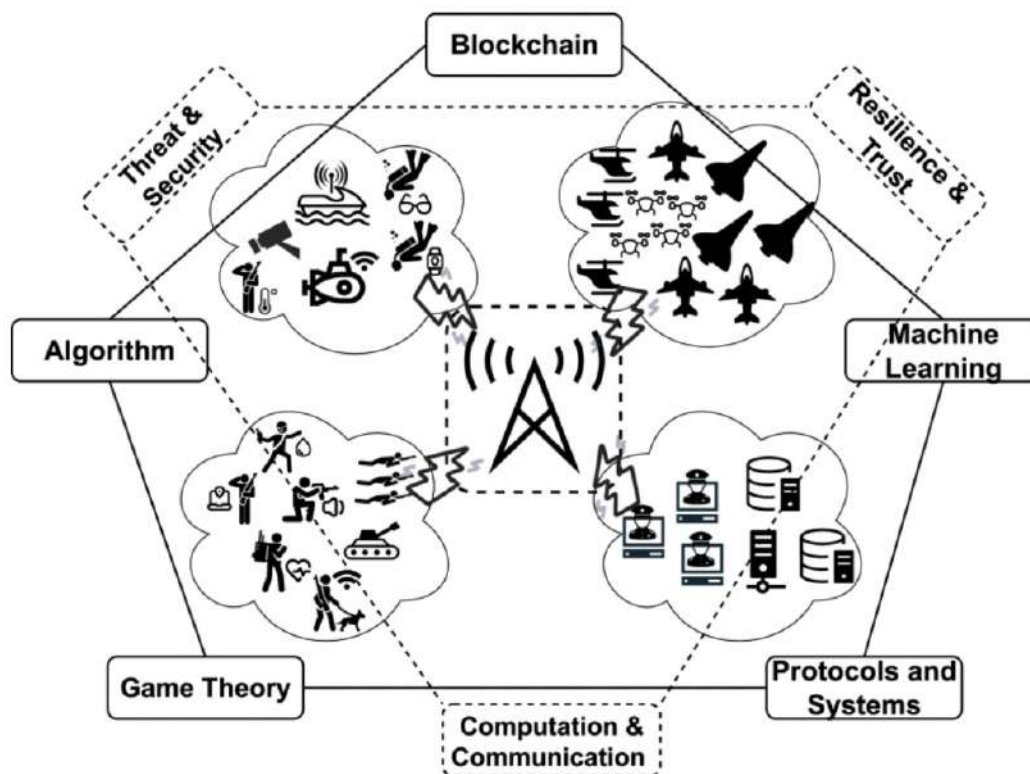
Área de Aplicação	Descrição da Aplicação	Benefícios Identificados	Referências Principais
Vigilância e Reconhecimento	Uso de UAVs, sensores terrestres e satélites para monitoramento em tempo real.	Ampliação da consciência situacional e redução de riscos humanos.	Tolba (2020); Wei (2021)
Logística Militar	Rastreamento de suprimentos e manutenção preventiva com RFID e IA.	Redução de perdas, economia de recursos e previsibilidade logística.	Kufakunesu et al. (2025)
Comando e Controle (CC-CIIVR)	Integração de comunicações e decisões via redes MANET e SAD.	Maior coordenação e resposta tática rápida em campo.	Tolba (2020); Mezrioui (2017)
Monitoramento de Tropas	Acompanhamento biométrico e análise preditiva de desempenho.	Proteção à saúde e otimização do posicionamento das forças.	Wei (2021)

Elaborado pelo Autor, 2025, com base em [Tolba 2020; Wei 2021] e [Kufakunesu, Myburgh e Freitas 2025].

3.2.2 Internet das Coisas de Batalha

A IoMT representa uma vertente da IoT voltada ao setor militar, unindo sensores, dispositivos e sistemas inteligentes para aprimorar o monitoramento, a comunicação e o suporte à tomada de decisões em operações de defesa. Enquanto a IoMT fornece a infraestrutura tecnológica geral e os protocolos de integração, a IoBT aplica esses recursos de forma crítica no campo de batalha, permitindo tomada de decisão em tempo real, maior consciência situacional e operações coordenadas. Assim, IoBT pode ser vista como a implementação prática e estratégica da IoMT em cenários de conflito, unindo IA, comunicação segura e automação para otimizar eficiência e segurança militar.

A Figura 3.3, mostra integração entre IA, *Blockchain*, Computação de Borda, e fluxo de dados desde sensores até centros de comando, com camadas de segurança e validação por *blockchain*, análise inteligente na borda e sincronização em nuvem. Demonstra como tecnologias emergentes se conectam para fortalecer a resiliência das operações militares.

Figura 3.3: *Internet das Coisas de Batalha*

<https://ieeexplore-ieee-org.ez291.periodicos.capes.gov.br/document/10636816>.

3.2.3 Resultados do Trabalho

Os resultados obtidos a partir da análise bibliográfica revelam que a IoMT representa uma das mais importantes transformações tecnológicas no contexto da defesa contemporânea. Sua implementação amplia as capacidades operacionais das forças armadas ao integrar, em um único ecossistema, sensores inteligentes, veículos autônomos, plataformas aéreas e SAD, consolidando o conceito de guerra centrada na informação [Tolba 2020; Wei 2021].

De maneira geral, os estudos revisados demonstram que a IoMT contribui de forma significativa para o fortalecimento da superioridade informacional, oferecendo vantagens em velocidade de comunicação, precisão de dados e tomada de decisões estratégicas. Essa superioridade é alcançada por meio da integração contínua de tecnologias emergentes, que tornam possível a criação de redes militares autônomas, seguras e adaptáveis.

Contudo, as pesquisas também deixam evidente que a IoMT ainda se encontra em processo de consolidação, com desafios substanciais relacionados à interoperabilidade, cibersegurança, consumo energético e escalabilidade [Mezrioui 2017; Kufakunesu, Myburgh e Freitas 2025]. A ausência de padrões universais de comunicação e a vulnerabilidade a ataques cibernéticos permanecem como os principais entraves à adoção plena da tecnologia em missões críticas.

Por outro lado, o avanço de soluções emergentes, como IA, ML, *Blockchain* e EC, vem oferecendo caminhos promissores para superar essas limitações. Tais tecnologias possibilitam a análise inteligente de dados em tempo real, a autenticação descentralizada de informações e a resiliência das comunicações, fatores que aumentam a confiabilidade e reduzem os riscos operacionais.

No campo prático, as aplicações analisadas demonstram que a IoMT é capaz de aprimorar substancialmente áreas críticas das operações militares, como vigilância, logística, comando e controle, e monitoramento de tropas. O uso de sensores embarcados e redes MANET permite a coleta de dados precisos em campo, garantindo eficiência tática e segurança estratégica. Além disso, sistemas de apoio à decisão alimentados por IA têm se mostrado essenciais para acelerar respostas em ambientes de combate complexos.

Esses resultados confirmam que a IoMT redefine o paradigma das operações militares, deslocando o foco tradicional do poder de fogo para o poder da informação. As forças armadas que dominarem essa integração tecnológica tendem a conquistar maior efetividade operacional, capacidade de previsão e autonomia estratégica frente aos desafios da guerra moderna.

Por fim, observa-se que, apesar das limitações atuais, a tendência é de crescimento exponencial das pesquisas e aplicações práticas da IoMT, impulsionadas por avanços contínuos em redes seguras, inteligência distribuída e arquitetura de dados militares. Assim, este estudo contribui para a compreensão crítica do estado atual da IoMT, oferecendo uma base sólida para investigações futuras e para o desenvolvimento de soluções cada vez mais robustas e sustentáveis no campo da defesa.

Capítulo 4

Considerações Finais e Sugestões para Trabalhos Futuros

O presente estudo teve como objetivo analisar o papel da IoMT nas operações de campo, destacando suas aplicações, desafios e tecnologias emergentes associadas. A partir da revisão bibliográfica realizada, foi possível constatar que a IoMT representa uma das principais evoluções tecnológicas no contexto da defesa moderna, ao permitir a integração inteligente de dispositivos, sensores, veículos autônomos e sistemas de comando em uma rede cooperativa e descentralizada.

Os resultados obtidos demonstram que a IoMT possibilita uma transformação significativa na forma como as forças armadas conduzem suas operações, ampliando a consciência situacional, otimizando o gerenciamento logístico e fortalecendo a capacidade de resposta estratégica. Essa integração de sistemas conectados e inteligentes promove maior precisão nas decisões táticas, reduzindo falhas humanas e aumentando a eficiência operacional.

Entretanto, a pesquisa também evidenciou que a implementação prática da IoMT ainda enfrenta obstáculos relevantes. Entre os principais, destacam-se os problemas de interoperabilidade, que dificultam a comunicação entre diferentes plataformas; os riscos cibernéticos, que ameaçam a integridade dos dados; e as restrições energéticas, que limitam a autonomia de dispositivos em campo. Esses desafios reforçam a necessidade de padrões tecnológicos unificados, políticas robustas de cibersegurança e investimentos contínuos em fontes alternativas de energia.

Além disso, observou-se que o avanço da IoMT está diretamente associado à adoção de tecnologias emergentes, como IA, ML, *Blockchain*, Computação de Borda e redes resilientes. Essas ferramentas têm se mostrado fundamentais para aprimorar a segurança, a eficiência e a adaptabilidade das infraestruturas militares conectadas, oferecendo novos caminhos para a guerra centrada na informação.

Portanto, conclui-se que a IoMT não deve ser compreendida apenas como uma evolução tecnológica, mas como um marco estratégico na transformação digital das forças armadas. Sua adoção amplia as fronteiras do comando e controle, proporcionando às instituições mi-

litares um poder informacional capaz de redefinir a natureza das operações no século XXI.

4.1 Contribuições do Estudo

Este trabalho contribui para o entendimento da IoMT ao reunir e sistematizar informações sobre sua arquitetura, desafios, aplicações e tecnologias de apoio. A análise consolidada permitiu identificar os principais fatores críticos de sucesso para sua implementação, bem como as lacunas existentes na literatura acadêmica e técnica. Assim, o estudo serve como referência conceitual para pesquisadores e profissionais da área de defesa interessados em explorar o potencial da conectividade e da inteligência distribuída no campo militar.

4.2 Sugestões para Trabalhos Futuros

Como continuidade desta pesquisa, recomenda-se o desenvolvimento de estudos experimentais e empíricos que validem as soluções apresentadas em cenários reais de operação. A aplicação prática de protótipos IoMT, aliada à coleta de métricas de desempenho e segurança, permitirá avaliar de forma mais precisa a efetividade das tecnologias emergentes discutidas neste trabalho.

Outra sugestão é a realização de pesquisas comparativas entre diferentes arquiteturas de rede e protocolos de comunicação, com o intuito de identificar padrões que favoreçam a interoperabilidade e a resiliência dos sistemas militares conectados. Além disso, investigações sobre fontes alternativas de energia, como microgeradores e painéis fotovoltaicos integrados a dispositivos IoMT, podem oferecer soluções sustentáveis e de maior autonomia para operações prolongadas.

Por fim, sugere-se o aprofundamento do estudo sobre o impacto ético e estratégico da IoMT, considerando questões como privacidade de dados, dependência tecnológica e autonomia de decisão em sistemas autônomos. Esses temas tornam-se cada vez mais relevantes à medida que a guerra moderna se desloca para ambientes altamente automatizados e digitalizados.

4.3 Considerações Finais

A IoMT representa uma das inovações mais disruptivas da era digital, redefinindo as fronteiras entre homem, máquina e informação. A aplicação desse conceito no ambiente militar demonstra o potencial transformador das tecnologias de conectividade inteligente, permitindo que sensores, veículos, *drones* e sistemas de comando cooperem em rede para garantir superioridade informacional, eficiência logística e tomada de decisão em tempo real.

Os resultados obtidos ao longo desta pesquisa evidenciam que a IoMT não apenas otimiza processos operacionais, mas inaugura uma nova fase na condução de missões de defesa. A integração de dispositivos autônomos, associada ao uso de IA, ML e Computação de Borda, confere às forças armadas maior capacidade de resposta, adaptabilidade e precisão estratégica, tornando as operações mais seguras, ágeis e sustentáveis. Assim, o poder bélico dá lugar ao poder da informação elemento central das guerras modernas baseadas em dados.

Por outro lado, o estudo também revelou que a implementação plena da IoMT ainda encontra barreiras significativas. Problemas de interoperabilidade, vulnerabilidades cibernéticas, limitações energéticas e ausência de padronização internacional dificultam a consolidação de sistemas verdadeiramente integrados e resilientes. Tais desafios exigem esforços coordenados entre instituições militares, centros de pesquisa e indústria tecnológica para o desenvolvimento de soluções interoperáveis, sustentáveis e alinhadas às normas de segurança cibernética.

Além disso, o avanço da IoMT levanta novas reflexões de ordem ética e estratégica. Questões como a autonomia de sistemas letais, a proteção de dados sensíveis e a dependência de algoritmos autônomos precisam ser debatidas à luz do direito internacional e dos princípios humanitários. A transformação digital da guerra impõe, portanto, um equilíbrio entre inovação tecnológica e responsabilidade moral.

Em termos acadêmicos, este trabalho contribui ao sintetizar a literatura existente e estruturar uma análise crítica sobre os desafios e perspectivas da IoMT, fornecendo uma base conceitual sólida para futuras investigações. No campo prático, reforça a importância de investir em tecnologias emergentes e em políticas de segurança digital que assegurem a soberania informacional e a autonomia estratégica das nações.

Conclui-se, assim, que a IoMT não é apenas uma tendência tecnológica, mas um novo paradigma operacional para as forças armadas do século XXI. Seu desenvolvimento contínuo moldará o futuro da defesa global, onde a integração entre conectividade, IA e análise de dados se tornará o principal vetor de vantagem competitiva e segurança nacional. O desafio está em transformar esse potencial em uma realidade eficiente, ética e sustentável, consolidando a informação como o mais valioso recurso estratégico das operações militares modernas.

Reportagens

Como mostrado em diversas reportagens Apêndice A, a IoMT apresenta aplicações reais.

- Na Figura 4.1 mostra *drone* submarino ucraniano *TOLOKA*, apresentada durante a exposição *Brave1 Defense Tech Valley*. este modelo *TLK-1000*. Demonstra a aplicação da IoMT no ambiente naval de defesa, integrando sensores e sistemas autônomos para ampliar a superioridade informacional e operacional das forças armadas. (A.1)

Figura 4.1: *Drone Submarino.*



CNN [Portugal 2025].

- Na Figura 4.2, tem-se o momento em que um *drone* de origem russa explode próximo a um prédio residencial em *Sumy*, Ucrânia. O evento demonstra o uso tático de *drones* como armas autônomas em ambientes urbanos, evidenciando o impacto direto da IoMT em conflitos armados modernos e os desafios de segurança e defesa contra ataques remotos. (A.2)

Figura 4.2: *Drone da Rússia explode.*



CNN [Brasil 2025]

- Na Figura 4.3, *Darwin*, jovem operador de *drones FPV kamikaze* da 92^a Brigada do Exército da Ucrânia, durante uma missão de combate. Os *drones FPV* equipados com IoMT são apresentados como ferramentas essenciais para ataques de precisão,

vigilância e operações estratégicas, revelando como a tecnologia transforma o campo de batalha por meio da automação e inteligência embarcada. (A.3)

Figura 4.3: *Darwin operador de drones FPV kamikaze.*



[Net 2024]

- A Figura 4.4, reportagem sobre a **megaoperação policial nos complexos do Rio de Janeiro**, na qual integrantes do **Comando Vermelho** utilizaram *drones* para lançar explosivos contra forças de segurança. Esse cenário ilustra a crescente intensificação do uso de sistemas aéreos não tripulados como armas adaptáveis para múltiplas missões, ressaltando os desafios relacionados ao controle do espaço aéreo, à cibersegurança e à segurança pública.(A.4)

Figura 4.4: *Drone Comando Vermelho.*



CNN [Brasil 2025].

Apêndice A

Reportagens sobre IoMT

Este apêndice apresenta reportagens selecionadas relacionadas ao uso da IoMT.

A.1 Figura 4.1

Segundo reportagem da [Portugal 2025], a Ucrânia apresentou um novo *drone* submarino. A Ucrânia mostrou ao mundo pela primeira o *TOLOKA*, o seu novo *drone* submarino de grandes dimensões, durante a exposição *Brave1 Defense Tech Valley*, em *Lviv*, a 19 de setembro. A nova gama de *drones* tem três tamanhos diferentes e promete colocar vários dilemas à marinha russa do Mar Negro. O modelo que prendeu os olhos de todos os presentes na feira de armamento é o *TLK- 1000*. Com 12 metros de comprimento e a capacidade de atingir alvos a dois mil quilómetros com uma enorme carga explosiva de cinco mil quilos, esta nova arma ucraniana apresenta-se como o equipamento ideal para atacar navios de grandes dimensões, portos e infraestruturas estratégicas, como a ponte de *Kerch*, que liga a península ocupada da Crimeia ao território russo. Mas o impressionante *drone* submarino, que se parece com um submarino de pequenas dimensões, é acompanhado de duas variantes menores para outro tipo de missões. A principal é o *TLK-200*, uma munição operada por um piloto capaz de conduzir missões furtivas debaixo de água, através de um sistema de propulsão elétrico, que permite a este *drone* operar sem ser detetado pelas defesas russas. Esta versão foi concebida para missões de curta distância, a menos de 100 quilómetros do local do lançamento. No entanto, tem uma autonomia que permite aos seus dois motores elétricos operar durante 15 dias. Os operadores do *TLK-200*, que tem quase três metros de comprimento, têm ao seu dispor uma câmara térmica e capacidades defensivas contra guerra eletrónica. A terceira variante é conhecida como *TLK-400* tem um motor híbrido que lhe permite operar a maiores distâncias e durante mais dias, mas também transportar uma quantidade superior de explosivos. Em declarações aos jornalistas da *RBC-Ukraine*, os representantes da empresa revelaram que estes *drones* podem também ser adaptados para outro tipo de missões, como a destruição de minas navais, deteção acústica de inimigos

ou até mesmo o mapeamento do fundo do mar. "Os nossos *drones* detetam, classificam e neutralizam minas subaquáticas de forma independente, aumentando significativamente a segurança e a eficiência das operações marítimas", disse a empresa. Apesar de não o dizer diretamente, as forças armadas ucranianas deram a entender que esta nova arma vai ser incorporada no seu arsenal. "As Forças Armadas da Ucrânia receberão em breve uma série de novos sistemas, incluindo *drones*, barcos não tripulados, complexos robóticos terrestres e equipamentos de guerra eletrônica", disseram os militares [Portugal 2025].

A.2 Figura 4.2

A reportagem relata um *drone* de origem russa explodiu nas proximidades de um prédio residencial na cidade de *Sumy*, localizada no nordeste da Ucrânia, resultando em pelo menos nove pessoas feridas, conforme informaram autoridades locais. [Brasil 2025], O evento foi registrado por testemunhas e autenticado por agências de notícias internacionais. Além deste ataque, a região de *Chernihiv* também foi alvo de ofensivas russas no mesmo dia, ocasionando pelo menos quatro mortes e deixando milhares de moradores sem eletricidade e água. Desde o início do conflito, em fevereiro de 2022, a Rússia intensificou ataques utilizando *drones* e mísseis, controlando aproximadamente um quinto do território ucraniano. As consequências diretas dessa ofensiva são milhares de mortes, principalmente entre civis ucranianos, e mais de um milhão de pessoas afetadas entre mortos e feridos.

A.3 Figura 4.3

Reportagem narra a experiência de "*Darwin*", um jovem piloto ucraniano de 21 anos especialista em *drones kamikaze FPV* da 92ª Brigada do Exército da Ucrânia. [Net 2024] Segundo autoridades do país, os *drones First-Person View* (FPV) tornaram-se a principal arma de combate das forças ucranianas contra os russos.

Com escassez de projéteis de artilharia e foguetes, os militares ucranianos passaram a adotar pesadamente *drones FPV*, que têm alto impacto tático, atacando tanques, veículos blindados e soldados russos. O ministro das indústrias estratégicas da Ucrânia, *Alexander Kamyshin*, destacou que há um projeto para produzir mais de 1 milhão desses *drones* até o fim do ano, buscando reduzir ainda mais o custo por baixa inimiga.

A matéria relata que essas aeronaves não tripuladas serão em breve equipadas com *IA*, tornando-as menos vulneráveis às defesas russas. O jornalista acompanhou *Darwin* e sua equipe por mais de 20 horas em missão praticamente na linha de frente, evidenciando a relevância destes operadores na evolução dos combates atuais na Ucrânia.

A.4 Figura 4.4

Durante uma megaoperação policial nos complexos da Penha e do Alemão, no Rio de Janeiro, integrantes da facção **Comando Vermelho** utilizaram *drones* para lançar bombas como reação à ação das forças de segurança. A operação, considerada a maior da história do estado, envolveu cerca de 2.500 policiais civis e militares e buscava cumprir 100 mandados de prisão contra membros da facção, após mais de um ano de investigação. [Brasil 2025] Até o momento, mais de 80 pessoas foram presas, ao menos 64 mortes foram confirmadas, armas e veículos apreendidos, e houve impactos significativos em serviços locais de saúde e educação, incluindo o fechamento de escolas e unidades de saúde. A ação visou reprimir a expansão territorial do Comando Vermelho e capturar lideranças criminosas dentro e fora do estado.

Referências Bibliográficas

[Akter 2022] AKTER, R. Toward secure and reliable internet of military things: Architecture and challenges. In: *IEEE International Conference on Communications (ICC)*. [s.n.], 2022. Disponível em: <<https://ieeexplore.ieee.org/document/9778246>>. 41

[Brasil 2025] BRASIL, C. *Drone Comando Vermelho*. 2025. Acesso em: 08 out. 2025. Disponível em: <<https://www.cnnbrasil.com.br/nacional/sudeste/rj/video-em-reacao-a-operacao-drone-do-cv-arremessa-bombas-em-comunidade/>>. 36, 39, 41

[Brasil 2025] BRASIL, C. *Drone da Rússia explode perto de prédio na Ucrânia*. 2025. Acesso em: 08 out. 2025. Disponível em: <<https://www.cnnbrasil.com.br/internacional/veja-o-momento-em-que-drone-da-russia-explode-perto-de-predio-na-ucrania/>>. 35, 38, 41

[Elshweikh 2022] ELSHWEIKH, A. A. Artificial intelligence for cybersecurity in the internet of battle things. *IEEE Access*, 2022. Disponível em: <<https://ieeexplore.ieee.org/document/9855671>>. 20, 41

[Guitton 2021] GUITTON, M. J. Fighting the locusts: Implementing military countermeasures against drones and drone swarms. *Scandinavian Journal of Military Studies*, v. 4, n. 1, p. 26–36, 2021. Disponível em: <<https://sjms.nu/articles/10.31374/sjms.53>>. 41

[Keshk 2024] KESHK, M. Blockchain-enabled security solutions for internet of military things. *IEEE Internet of Things Journal*, 2024. Disponível em: <<https://ieeexplore.ieee.org/document/10636816>>. 20, 41

[Kikuchi 2023] KIKUCHI, A. Y. Internet das coisas (iot): Um estudo de aplicações e desafios tecnológicos. *Revista Interface Tecnológica*, 2023. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/pt_BR/article/view/1211/674>. 1, 7, 41

[Kufakunesu, Myburgh e Freitas 2025] KUFAKUNESU, R.; MYBURGH, H.; FREITAS, A. D. The internet of battle things: A survey on communication challenges and recent solutions. *Discover Internet of Things*, v. 5, n. 3, p. 1–18, 2025. Disponível em: <<https://link.springer.com/article/10.1007/s43926-025-00093-w>>. 9, 21, 24, 25, 26, 27, 28, 29, 30, 41

[Mezrioui 2017] MEZRIOUI, A. Energy-efficient protocols for secure iot in military applications. *IEEE Sensors Journal*, 2017. Disponível em: <<https://ieeexplore.ieee.org/document/7921973>>. 16, 18, 19, 21, 22, 25, 26, 27, 30, 41

[Net 2024] NET, D. *Drone FPV*. 2024. Acesso em: 08 out. 2025. Disponível em: <<https://www.defesanet.com.br/vant/acompanhe-o-as-darwin-de-uma-unidade-de-drone-fpv-kamikaze-ucraniana/>>. 36, 38, 41

[Portugal 2025] PORTUGAL, C. *Ucrânia mostra o novo drone submarino — um dos maiores de sempre que ameaça a ponte de Kerch*. 2025. Acesso em: 08 out. 2025. Disponível em: <<https://cnnportugal.iol.pt/guerra/ucrania/ucrania-mostra-o-novo-drone-submarino-um-dos-maiores-de-sempre-que-ameaca-a-ponte-de-kerch/20250922/68d19592d34ee0c2fed06645>>. 35, 37, 38, 41

[Shirvani 2022] SHIRVANI, M. H. Cybersecurity techniques for iot integration in combat systems. *Computers & Security*, 2022. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S2542660522001214>>. 20, 22, 41

[Tolba 2020] TOLBA, S. e. Cybersecurity issues in internet of things (iot): A survey. *Journal of Network and Computer Applications*, 2020. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1526149220002350>>. 1, 10, 11, 13, 14, 15, 20, 21, 22, 24, 25, 26, 27, 28, 29, 30, 41

[Tortonesi 2017] TORTONESI, M. Security challenges in the internet of things: Military perspective. In: *IEEE Military Communications Conference (MILCOM)*. [s.n.], 2017. Disponível em: <<https://ieeexplore.ieee.org/document/7845503>>. 3, 17, 25, 26, 41

[Wei 2021] WEI, P. A survey on internet of military things: Architectures, applications, and security challenges. *IEEE Access*, 2021. Disponível em: <<https://ieeexplore.ieee.org/document/9317321>>. 1, 2, 9, 21, 22, 24, 26, 27, 28, 29, 30, 41

[West 2016] WEST, B. J. A reliable and scalable architecture for internet of military things. In: *IEEE International Conference on Military Communications*. [s.n.], 2016. Disponível em: <<https://ieeexplore.ieee.org/document/7756279>>. 17, 41

[Tolba 2020] [Kikuchi 2023] [Akter 2022] [Guitton 2021] [Kufakunesu, Myburgh e Freitas 2025] [Wei 2021] [Shirvani 2022] [Tortonesi 2017] [West 2016] [Keshk 2024] [Elshweikh 2022] [Mezrioui 2017] [Portugal 2025] [Brasil 2025] [Net 2024] [Brasil 2025]

	INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
	Campus Campina Grande - Código INEP: 25137409
	R. Tranquilino Coelho Lemos, 671, Dinamérica, CEP 58432-300, Campina Grande (PB)
	CNPJ: 10.783.898/0003-37 - Telefone: (83) 2102.6200

Documento Digitalizado Ostensivo (Público)

Entrega de trabalho de conclusão de curso

Assunto:	Entrega de trabalho de conclusão de curso
Assinado por:	Jose Silva
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Ostensivo (Público)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- Jose Wesley Mendes de Souza Silva, DISCENTE (202411210034) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE, em 15/01/2026 20:19:39.

Este documento foi armazenado no SUAP em 15/01/2026. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifpb.edu.br/verificar-documento-externo/> e forneça os dados abaixo:

Código Verificador: 1731629
Código de Autenticação: 550df4653c

