Defense Technology Interoperability in Complex Systems: A Survey

www.surveyx.cn

Abstract

Defense technology interoperability is critical for enhancing military effectiveness by ensuring seamless integration and communication across diverse systems and nations. This survey explores the integration of advanced technologies, such as Service-Oriented Architectures (SOA) and IoT, into defense systems to improve situational awareness and operational reactivity. It addresses the inefficiencies of traditional command and control systems, proposing a reference model for classifying system interactions and introducing frameworks like the C4ISR Architecture Framework and the Context-Aware Policy-Driven (CAPD) framework to secure information exchange and mitigate cyber threats. The study emphasizes the need for robust cyber defense mechanisms and highlights the evolving U.S.-Singapore cooperation in technology and security. The survey is structured to provide a historical perspective on defense technology evolution, define core concepts, and analyze current interoperability models and frameworks, including DEVS/SOA and DNAB2. It identifies challenges such as technological diversity, standardization issues, security concerns, and integration complexities across nations. Case studies like the U.S.-Singapore collaboration illustrate successful interoperability practices. Future directions involve advancements in AI and machine learning, IoT integration, and strategic collaboration to address ethical, societal, and legal implications. The research underscores the importance of innovation and policy development in achieving interoperability, ensuring defense systems operate cohesively in a complex global security environment.

1 Introduction

1.1 Importance of Interoperability

Interoperability is crucial in defense technology, significantly enhancing military effectiveness through seamless communication and integration across diverse systems. This capability enables coordination among various military branches and allied forces, allowing for adaptive responses to dynamic operational demands [1]. Establishing standards and performance benchmarks is essential for effective interoperability, facilitating the sharing and comparison of security playbooks among organizations.

The integration of advanced technologies, including autonomous assets and AI-driven systems, is vital for improving operational effectiveness and collective military capabilities [2]. Rigorous engineering methods and a comprehensive body of knowledge in Modeling and Simulation (MS) are necessary to support standard operations and enhance simulation interoperability [3]. However, fragmented definitions of interoperability across domains present challenges that hinder the realization of its full benefits [4].

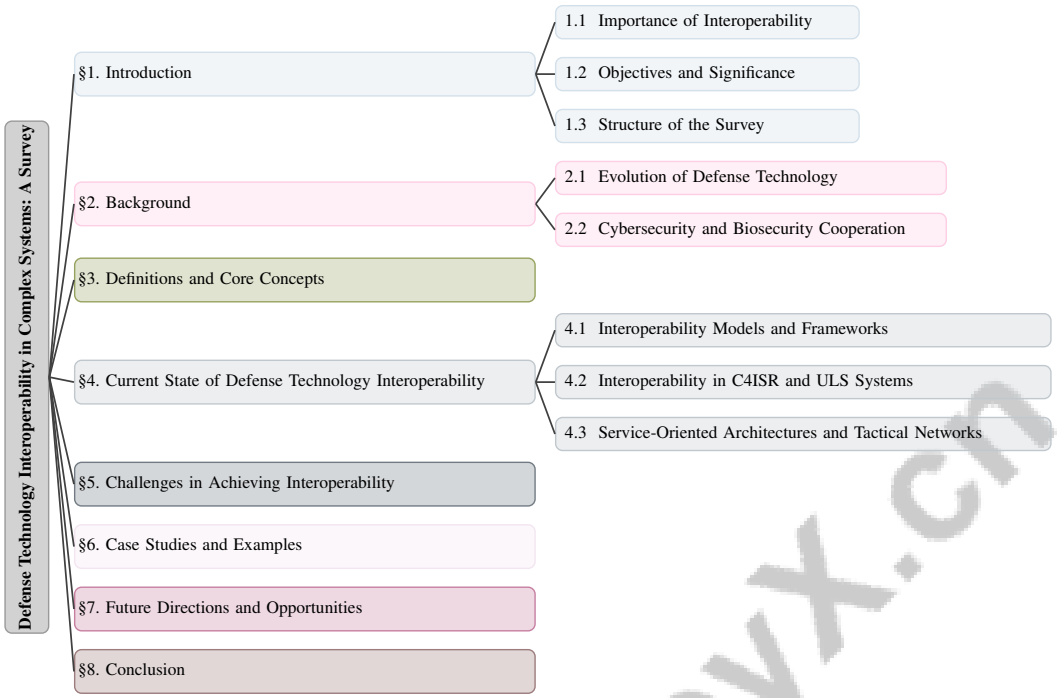


Figure 1: chapter structure

1.2 Objectives and Significance

This paper aims to investigate the integration of advanced technologies, particularly Service-Oriented Architectures (SOA), into military defense systems. This integration enhances situational awareness and responsiveness in military operations by leveraging a modular and interoperable framework that addresses the complexities of modern warfare, including cyber and unmanned tactics. The research underscores the need for a scalable command and control infrastructure that enables commanders to effectively plan, monitor, and execute missions remotely, even in constrained communication environments [5, 6, 7, 8]. Additionally, it proposes a reference model to classify system interactions based on information transport and processing, addressing IoT interoperability challenges.

The introduction of the C4ISR Architecture Framework facilitates Verification, Validation, and Accreditation (VVA) processes, which are critical for interoperability needs [6]. A context-aware, policy-driven framework (CAPD) is proposed to secure information exchange within the Internet of Battlefield Things (IoBT), mitigating cyberattack risks [9]. Furthermore, addressing the absence of an architectural maturity model for ULS system interoperability is essential for effective software engineering in complex environments [10].

The study emphasizes robust cyber defense mechanisms, such as Autonomous Cyber Defense (ACyD), to counter sophisticated cyber threats [11]. It also analyzes the evolving U.S.-Singapore cooperation on technology and security in defense, cyber, and biotech domains, which is crucial for national security amid shifting geopolitical dynamics [12]. The development of the Situational Understanding Explorer (SUE) platform aims to enhance coalition situational understanding in contested environments [13]. Additionally, the introduction of the Cop mechanism seeks to improve protocol enforcement among autonomous actors in complex systems, addressing existing limitations [14].

This study's significance lies in its comprehensive approach to tackling multifaceted interoperability challenges in defense technology. By introducing innovative models and frameworks, the paper advances military capabilities and facilitates seamless operations across various platforms and coalitions. This contribution is vital in modern warfare, where integrating advanced technologies such as blockchain, Software-Defined Networking (SDN), and SOA is essential for creating cohesive and adaptable tactical networks. Focusing on intelligent mission collaboration and the convergence of information and communication technologies (ICT), the research addresses contemporary military

AI-generated, for reference only.

complexities, ensuring defense forces are prepared for future digital battlefields [2, 15, 16, 8, 7]. This research not only strengthens military effectiveness but also fosters innovation and collaboration within the defense technology sector.

1.3 Structure of the Survey

The survey is structured to address the complexities of defense technology interoperability, beginning with an introduction that highlights interoperability's critical role in enhancing military effectiveness while outlining the study's objectives and significance. The background section provides a historical perspective on the evolution of defense technology toward interoperability, emphasizing significant developments and milestones in military technology integration [17]. It also underscores the importance of a unified definition to overcome interoperability challenges [4].

The third section elucidates essential terms such as 'interoperability', 'complex systems', and 'defense technology', establishing a foundational understanding through an ontology-based approach to model-based systems engineering (MBSE) [18]. The current state of defense technology interoperability is scrutinized, showcasing existing systems and technologies, including interoperability models and frameworks [1], and their implementation in C4ISR and ULS systems.

The survey further explores interoperability challenges, identifying primary issues such as technological diversity, standardization, security concerns, and integration complexity across nations and platforms. This analysis includes discussions on integrating blockchain technology with other ICT technologies, forming a comprehensive defense strategy termed DNAB2 [16]. Case studies illustrate successful interoperability in defense operations, emphasizing U.S.-Singapore collaborative efforts and frameworks like DEVS/SOA in command and control systems.

In the penultimate section, future directions and opportunities are examined, discussing advancements in AI and machine learning, IoT and cybersecurity integration, and the role of strategic collaboration and policy development [2]. The survey concludes by summarizing key findings, reiterating interoperability's importance in defense technology, and discussing implications for future research and policy development.The following sections are organized as shown in Figure 1.

2 Background

2.1 Evolution of Defense Technology

The evolution of defense technology underscores the pursuit of interoperability amid growing military system complexity. The adoption of advanced architectures like Service-Oriented Architecture (SOA) addresses the limitations of traditional middleware, which often overlook application-layer interoperability [19]. Ultra-Large-Scale (ULS) systems further highlight challenges in defining and operating expansive systems essential for interoperability [10]. The C4ISR Architecture Framework represents a pivotal development, structuring military applications to enhance interoperability [6]. However, the diversity of rule-based systems necessitates common interfaces for cohesive system integration [20].

Achieving syntactical and semantical interoperability, especially among legacy systems using disparate protocols, remains a significant challenge [21]. This historical context emphasizes the need for adaptable interoperability solutions akin to programming language evolution [22]. Advancements such as blockchain integration in military logistics exemplify efforts to enhance interoperability [16]. The incorporation of autonomous assets within the Internet of Battlefield Things (IoBT) augments capabilities but introduces cybersecurity challenges, reflecting the dual nature of technological advancement [9]. Software-Defined Networking (SDN) in tactical environments further refines defense technology for greater interoperability [15].

Addressing semantic interoperability among discrete systems is crucial for effective cross-platform communication [23]. New design models promoting scalability, reusability, and interoperability reflect ongoing efforts to enhance defense technology [8]. Collaborative initiatives, such as U.S.-Singapore efforts, advance defense technology integration with cybersecurity and biosecurity, marking significant strides in military technology [12].

Challenges also arise from heterogeneous modeling languages complicating data interoperability [18]. Overcoming the absence of a unified interoperability definition, with over 117 distinct interpretations,

is crucial for innovation and efficiency [4]. Standardized security playbooks enhance interoperability across diverse platforms and systems [1]. Conceptual interoperability issues in Modeling and Simulation (MS) systems continue to impede effective communication, underscoring historical challenges in achieving interoperability [3].

2.2 Cybersecurity and Biosecurity Cooperation

Advancements in cybersecurity and biosecurity are integral to defense technology interoperability, crucial for safeguarding operations against emerging threats. Autonomous Intelligent Malware (AIM) exemplifies evolving cybersecurity challenges, necessitating robust defense mechanisms to protect interconnected systems [11]. AIM's capability to autonomously adapt poses significant risks, demanding advanced security protocols to ensure interoperability across defense platforms.

Cybersecurity is critical for addressing integration challenges from diverse IoT technology layers in defense systems. IoT fragmentation presents barriers to seamless interoperability, underscoring the need for comprehensive strategies to secure data exchange across heterogeneous systems [24]. Effective cybersecurity measures protect sensitive information and maintain network integrity, facilitating the integration of advanced technologies in military operations.

Biosecurity's growing importance in defense technology interoperability is evident as nations confront biological threats affecting military personnel and operational effectiveness. U.S.-Singapore collaboration enhances regional epidemiological surveillance and biosecurity capabilities, bolstering preparedness against pandemics and biological risks [12, 1]. Integrating biosecurity measures into defense systems is vital for protecting military assets and personnel, supporting mission readiness and effectiveness. Collaborative efforts in cybersecurity and biosecurity are essential for developing resilient defense systems that adapt to evolving threats, enhancing military operations' interoperability and effectiveness.

In the context of advancing military operations, understanding the nuances of defense technology interoperability is paramount. This review paper explores various dimensions of this critical area, particularly focusing on the integration of artificial intelligence and the necessity for semantic alignment across diverse systems. As illustrated in Figure 2, the hierarchical structure of defense technology interoperability is depicted, emphasizing key terminology and core concepts. This figure not only underscores the importance of seamless operation across these varied systems but also highlights how such integration can significantly enhance situational awareness and decision-making processes in military contexts. By examining these elements, we can better appreciate the complexities and challenges that lie ahead in achieving effective interoperability.

3 Definitions and Core Concepts

3.1 Key Terminology

Grasping defense technology interoperability requires an understanding of several essential terms. 'Interoperability' refers to the ability of diverse systems and organizations to operate together seamlessly, particularly within command and control (C2) systems and Modeling and Simulation (MS) environments, ensuring smooth cross-platform operations [5].

'Semantic interoperability' tackles the challenge of exchanging meaningful information between systems that use different protocols and standards, ensuring that shared data is both syntactically and semantically aligned to enhance communication and integration [23].

The 'Internet of Battlefield Things (IoBT)' describes the network of interconnected autonomous assets and sensors in military operations, which enhances situational awareness and operational efficiency [9]. This underscores the growing complexity of defense systems, where IoT technologies are crucial for operational interoperability.

'Coalition situational understanding' is vital for interoperability among military forces, facilitating shared awareness and coordinated actions in joint operations. AI/ML capabilities are leveraged to process and interpret data from multiple sources, improving decision-making processes [13].

Additionally, 'artificial intelligence' in defense refers to AI-driven systems that augment human capabilities in diagnostics and operational planning. AI integration is key to improving interoperability by enabling efficient data processing and analysis [2].

A comprehensive understanding of these terms is critical for navigating the complexities of integrating diverse military systems. This foundational knowledge aids in addressing the varied definitions of interoperability across domains, as highlighted in recent studies. Establishing a universal definition can foster global collaboration and innovation, while advances in AI and software-defined networking enhance data analytics and communication in multi-domain operations. Adopting service-oriented architectures in tactical environments can mitigate limitations posed by constrained communication media. A unified interoperability approach promotes effective system integration and enhances decision-making in coalition operations [2, 15, 1, 7, 4].

3.2 Core Concepts of Interoperability

Interoperability in defense technology centers on integrating advanced modeling frameworks and AI methodologies to bolster military capabilities and ensure cohesive operations across diverse systems. A pivotal element is the implementation of the Discrete Event System Specification (DEVS) formalism, which supports net-centric modeling and simulation frameworks, addressing interoperability challenges in complex defense environments [5]. DEVS provides a standardized method for system representation and interaction, essential for coordinated operations of diverse military systems.

Moreover, integrating explainable AI and ML techniques, alongside symbolic AI, is crucial for building trust and enhancing interoperability among coalition partners. This integration supports the development of systems capable of executing complex tasks while delivering transparent and interpretable outputs, thereby facilitating collaborative decision-making in joint operations [13]. Trust in AI-driven decisions is fundamental for maintaining effective communication and coordination among allied forces, a cornerstone of successful interoperability.

These core concepts highlight the need for advanced technological frameworks and methodologies, such as explainable AI and unified interoperability definitions, to address the complex interoperability challenges in defense systems. By promoting a cohesive understanding across fields and improving human-machine collaboration through intelligence augmentation, these approaches significantly enhance seamless integration and decision-making in multi-domain operations involving multiple partners [4, 2]. Enhancing the collaboration of disparate systems contributes significantly to the operational effectiveness and strategic capabilities of military forces, enabling swift and effective responses to dynamic operational demands.

4 Current State of Defense Technology Interoperability

Category	Feature	Method
Interoperability Models and Frameworks	Standardization and Templates	AMMF-ULS[10], CMTS[1]
	Ontology and Semantic Integration	CAPD[9], GOPPRRE[18]
	Behavioral and Structural Interoperability	MC[19]
Service-Oriented Architectures and Tactical Networks	Decentralized Coordination	COP[14]
	Interoperability and Flexibility	SOA[8], DEFII[17], TSI[7]

Table 1: This table provides a comprehensive summary of various interoperability models and frameworks relevant to defense technology. It categorizes these models into two primary domains: Interoperability Models and Frameworks, and Service-Oriented Architectures and Tactical Networks, detailing specific features and methods employed to enhance communication and operational efficiency in military environments.

In the context of the current landscape of defense technology interoperability, it is essential to explore the various models and frameworks that underpin these efforts. These frameworks not only provide a structured approach to understanding interoperability but also highlight the methodologies employed to facilitate seamless integration among diverse defense systems. Table 1 presents a detailed classification of interoperability models and frameworks, highlighting their features and methods pertinent to advancing defense technology interoperability. Additionally, Table 4 presents a detailed comparison of interoperability frameworks, showcasing their distinct features and methodologies

AI-generated, for reference only.

relevant to advancing defense technology interoperability. The subsequent subsection delves into specific interoperability models and frameworks, examining their roles in enhancing communication, coordination, and overall operational effectiveness within military environments.

4.1 Interoperability Models and Frameworks

Method Name	Architectural Frameworks	Integration Techniques	Technological Adaptations
DEVS/SOA[5]	Devs/soa Framework	Service Oriented Architecture	Devs Formalism
DEFII[17]	Digital Engineering Framework	Ontology-aligned Data	Semantic Web Technologies
AMMF-ULS[10]	Maturity Model Framework	-	-
CAPD[9]	Context-aware Framework	Ontology-based Approach	Knowledge Graphs
GOPPRRE[18]	Meta-meta Model	Unified Syntax	Owl Representation
CMTS[1]	Cyber Threat Intelligence	Metadata Template	Machine-processable Metadata
MC[19]	Mediating Connector	Mediating Connector Patterns	Semantic Web Technologies

Table 2: Summary of Interoperability Models and Frameworks in Defense Systems. This table presents various methods employed to achieve interoperability, highlighting their architectural frameworks, integration techniques, and technological adaptations. The information underscores the diverse approaches and technologies leveraged to address interoperability challenges in modern military operations.

Interoperability in defense systems is achieved through a myriad of models and frameworks, each designed to address the intricate requirements of modern military operations. The C4ISR Architecture Framework is a cornerstone of these efforts, categorizing research into operational, systems, and technical architecture views, thereby supporting Verification, Validation, and Accreditation (VVA) processes essential for seamless communication and operation across diverse platforms [22].

Service-Oriented Architecture (SOA) is another pivotal model, utilizing loosely-coupled web services to enhance command and control operations. This architecture allows disparate systems to interact seamlessly, thereby improving operational efficiency and coordination in battlefield scenarios [5]. The Mediating Connector pattern further addresses behavioral mismatches between components, ensuring effective communication and integration, which is crucial for achieving interoperability [5].

The DEFII framework employs Semantic Web Technologies to enhance data integration and interoperability in Digital Engineering, providing a structured approach to achieve these goals [17]. Additionally, the DEVS/SOA framework integrates Modeling and Simulation (MS) with SOA to enhance interoperability among systems, leveraging established standards for cohesive operations [5].

The Architectural Maturity Model Framework for Ultra-Large-Scale (ULS) Systems Interoperability (AMMF-ULS) offers a structured approach to assess the capabilities of ULS systems, providing a comprehensive evaluation of interoperability capabilities and identifying areas for improvement [10]. Furthermore, the DNAB2 framework integrates blockchain technology into defense logistics, presenting a significant development in enhancing interoperability [16].

The Context-Aware Policy-Driven (CAPD) framework introduces an ontology-based approach for knowledge sharing and reasoning. By integrating context awareness and policy-driven access control, CAPD enhances existing models by providing a more dynamic and adaptable framework for interoperability [9]. The GOPPRRE ontology serves as a formalized approach that integrates different Model-Based Systems Engineering (MBSE) languages using a unified syntax and data structure, further improving interoperability in defense systems [18].

In tactical environments, a layered Software-Defined Networking (SDN) framework comprising application, control, forwarding, and orchestration planes facilitates efficient management and orchestration of network resources, thus supporting interoperability [15]. Moreover, the CMTS model provides a standardized template for integrating and managing course of action playbooks, serving as a model for achieving interoperability in defense systems [1].

The integration of High Level Architecture (HLA) with Model-Driven Architecture (MDA) as discussed by Tolk, along with the use of standards like UML, XML, and CORBA, further exemplifies the models employed to enhance interoperability among simulation systems [22]. Collectively, these models and frameworks offer robust solutions for achieving interoperability in defense systems, addressing the diverse challenges posed by modern military operations and technological advancements.

Table 2 provides a comprehensive overview of the interoperability models and frameworks utilized in defense systems, detailing their architectural frameworks, integration techniques, and technological adaptations.

As shown in Figure 3, The current state of defense technology interoperability is a complex and multifaceted domain that requires a comprehensive understanding of various interoperability models and frameworks. As illustrated in the accompanying figures, these models and frameworks encompass a wide range of elements and interactions. The first figure presents a geometric representation, highlighting the delineation between "inside" and "outside" areas, which can symbolize the boundaries and interfaces that must be navigated for effective interoperability. The second figure offers a more holistic view by depicting the interconnections between cultural, programmatic, social, constructive, operational, and vital elements, emphasizing the multifaceted nature of interoperability in defense technology. This diagram underscores the importance of considering diverse aspects that influence interoperability. Finally, the third figure provides a sequence diagram that details the communication process between a Windows Messenger client and a Jabber Messenger server through a mediating connector, demonstrating the technical intricacies involved in achieving seamless communication across different platforms. Together, these figures illustrate the diverse approaches and considerations necessary to address the challenges of interoperability in defense technology, highlighting the importance of robust models and frameworks to facilitate seamless integration and communication among various systems and components. [23, 10, 19]

4.2 Interoperability in C4ISR and ULS Systems

Interoperability within Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems and Ultra-Large-Scale (ULS) systems is crucial for enhancing military operations' effectiveness and adaptability. The co-development of niche capabilities, particularly in C4ISR and unmanned systems, underscores the current practices in defense technology interoperability [12]. These systems require seamless integration to ensure that information is accurately collected, processed, and disseminated across different platforms and allied forces.

In C4ISR systems, interoperability is achieved through the integration of advanced architectures like Service-Oriented Architecture (SOA) and Semantic Web Technologies. "These frameworks facilitate the seamless sharing and processing of information across diverse systems, significantly improving situational awareness and decision-making capabilities in real-time by integrating machine-readable course of action playbooks with cyber threat intelligence, and leveraging advanced artificial intelligence for enhanced human-machine collaboration in multi-domain operations." [1, 2]. The use of SOA, in particular, allows for the flexible adaptation of services, ensuring that diverse systems can communicate and operate cohesively in dynamic environments.

Ultra-Large-Scale (ULS) systems, which are distinguished by their vast scale and intricate architecture, introduce significant interoperability challenges due to their complexity and the diverse communication protocols involved. These challenges are exacerbated by the lack of a unified definition of interoperability across various domains, which complicates collaboration and innovation. To address these issues, it is essential to develop robust architectural frameworks and maturity models that facilitate seamless integration and dynamic translations among disparate systems, thereby enhancing the overall interoperability of ULS systems without requiring extensive re-engineering efforts. [21, 10, 4, 3]. The Architectural Maturity Model Framework for ULS Systems Interoperability (AMMF-ULS) provides a structured approach to evaluate and enhance the interoperability of these systems. This framework assesses the maturity of architectural practices and identifies areas for improvement, ensuring that ULS systems can effectively integrate with other defense technologies.

Moreover, interoperability in these systems is facilitated by the adoption of standardized communication protocols and data formats, which enable the seamless exchange of information across different platforms and nations. Collaborative efforts, such as those between the U.S. and Singapore, highlight the importance of strategic partnerships in advancing interoperability practices in C4ISR and ULS systems [12]. These partnerships foster innovation and technological advancements, ensuring that defense systems remain agile and responsive to emerging threats and operational demands.

Method Name	Interoperability Focus	Technological Integration	Flexible Architecture
TSI[7]	Real-time Service	Lightweight Soa Stack	Adaptable Frameworks
COP[14]	General Interoperability	Lgi Framework	Decentralized Controllers
DEFII[17]	Semantic Web Technologies	Ontology-aligned Data	Tool-agnostic Nature
SOA[8]	Enhance Interoperability	Soa Principles Integration	Flexible, Scalable System

Table 3: Overview of Methods for Enhancing Interoperability in Defense Systems through Service-Oriented Architectures and Tactical Networks. This table summarizes various methodologies, focusing on their interoperability objectives, technological integration strategies, and architectural flexibility, highlighting their contributions to seamless communication and collaboration in defense operations.

4.3 Service-Oriented Architectures and Tactical Networks

Service-Oriented Architectures (SOAs) and tactical networks play a pivotal role in facilitating interoperability within defense systems, particularly in resource-constrained environments. The TACTICS method exemplifies this by focusing on enhancing communication and service exchange, thereby addressing the specific challenges encountered in tactical settings [7]. By leveraging SOA principles, defense systems can achieve a higher degree of flexibility and adaptability, allowing for seamless integration and cooperation among various military technologies and platforms.

The integration of decentralized controllers and monitoring systems, as demonstrated by the Cop mechanism, further underscores the importance of SOAs in achieving interoperability among autonomous actors in complex systems. This approach enhances the ability of diverse systems to operate cohesively, ensuring that autonomous entities can effectively communicate and collaborate within the broader defense network [14].

Moreover, the DEFII framework illustrates the application of SOA in digital engineering, utilizing a graph data structure to provide a flexible, tool-agnostic means of accessing data across various engineering tools [17]. This capability is crucial for maintaining a consistent and authoritative source of information, which is essential for effective decision-making and coordination in defense operations.

Tactical networks, when integrated with SOA, provide a robust infrastructure for supporting dynamic and scalable defense operations. These advanced tactical networks leverage Software-Defined Networking (SDN) and artificial intelligence (AI) to facilitate real-time data exchange and communication across diverse platforms and domains, significantly enhancing situational awareness and operational efficiency in multi-domain operations. By integrating edge computing resources and ensuring interoperability among heterogeneous systems, these networks address critical challenges in security and data management, thereby optimizing collaborative decision-making in complex environments [2, 16, 15, 1, 13]. The combination of SOA and tactical networks thus represents a comprehensive approach to achieving interoperability, ensuring that defense systems can adapt to the evolving demands of modern military operations.

As shown in **??**, The current state of defense technology interoperability is increasingly characterized by the integration of service-oriented architectures and tactical networks, as illustrated in the provided examples. The first example, "Strategic and Tactical Communication Infrastructure in a Military Environment," showcases a schematic representation of a military communication system that delineates the strategic/operational domain from the tactical domain. This visual distinction underscores the complexity and necessity of seamless communication between the Joint Command and Control (JCC) and various tactical units. On the other hand, the "ESB (Enterprise Service Bus) Architecture" example highlights the role of an Enterprise Service Bus as a pivotal component in integrating diverse service providers and consumers within military networks. By acting as a bridge, the ESB facilitates interoperability among different programming environments such as .NET, Java, and BPEL, thereby enabling efficient and cohesive operation across different technological platforms. Together, these examples emphasize the critical importance of robust communication infrastructures and adaptable service architectures in enhancing the operational effectiveness of modern military forces [7, 8]. Table 3 presents a comprehensive comparison of methods aimed at improving interoperability in defense systems, emphasizing the role of Service-Oriented Architectures and tactical networks in facilitating effective communication and integration across diverse military technologies.

Feature	C4ISR Architecture Framework	Service-Oriented Architecture (SOA)	DEFII Framework
Integration Technique	Operational Systems Views	Loosely-coupled Services	Semantic Web Technologies
Architectural Framework	Vv	a Processes	Command And Control
Digital Engineering			
Technological Adaptation	Seamless Communication	Web Services	Data Integration

Table 4: This table provides a comparative analysis of three prominent frameworks used in defense technology interoperability: the C4ISR Architecture Framework, Service-Oriented Architecture (SOA), and the DEFII Framework. It highlights their integration techniques, architectural frameworks, and technological adaptations, offering insights into their respective roles in enhancing communication and coordination within military systems.

5 Challenges in Achieving Interoperability

5.1 Technological Diversity and Standardization Issues

Interoperability in defense systems is hampered by technological diversity and a lack of standardized protocols. The complexity arises from varying interoperability definitions and the challenge of establishing consistent standards in a rapidly evolving landscape. As military systems integrate advanced technologies like service-oriented architectures, a comprehensive framework is necessary to bridge gaps, enhance collaboration, and facilitate seamless information exchange [4, 7, 25, 8]. The heterogeneity of devices and communication protocols complicates integration, while differing models and terminologies increase costs and obscure mutual understanding.

In tactical settings, unreliable connectivity and resource-constrained mobile devices exacerbate integration challenges. The absence of a cohesive strategy to manage diverse rule engines and specifications impedes interoperability, reflecting broader issues in establishing universal standards critical for communication and innovation [4, 20, 25]. Behavioral diversity among system components leads to protocol mismatches that current solutions inadequately address.

Integrating Modeling and Simulation (MS) standards into frameworks like C4ISR is challenging due to a lack of common architectural standards. Ultra-Large-Scale (ULS) systems highlight the limitations of existing Information Systems Architecture (ISA) frameworks, necessitating advanced architectural maturity models for better integration across domains [21, 10, 3, 5, 4]. This challenge parallels those in artificial intelligence, where incompatibility between symbolic and subsymbolic AI/ML systems hinders insight sharing and collaborative decision-making.

Current methods, including blockchain-based smart contracts, face latency and scalability issues, while geopolitical factors complicate these challenges, as seen in Singapore's strategic balancing amid U.S.-China tensions [12]. These challenges underscore the need for standardized frameworks and unified approaches to manage the diverse technological landscape in defense operations.

5.2 Security Concerns and Cyber Threats

Security concerns and cyber threats significantly impede interoperability in defense systems, threatening the integrity and functionality of operations. Cyberattacks on Internet of Battlefield Things (IoBT) systems can disrupt sensor operations and mislead commanders, compromising situational awareness [9]. Autonomous Intelligent Malware (AIM) poses a formidable threat to command and control systems, necessitating robust defenses against adaptive cyber threats [11].

Service-Oriented Architectures (SOA) introduce potential security vulnerabilities that adversaries can exploit, emphasizing the need for secure and resilient network architectures [8]. Blockchain technology offers potential solutions to cybersecurity threats, particularly in untrusted environments where data integrity is crucial [16].

Trust calibration among coalition partners using diverse AI systems is a critical security concern. Effective trust management ensures secure AI-driven system collaboration without compromising interoperability [13]. Machine learning techniques can enhance standards' adaptability and security, improving resilience in interoperability frameworks [25].

An ontology-based approach for Model-Based Systems Engineering (MBSE) can address security concerns by improving communication and integration across modeling languages. This is vital for

maintaining secure defense operations and safeguarding sensitive information [18]. These security concerns and cyber threats highlight the need for robust cybersecurity measures and trust management strategies to enhance interoperability in defense systems.

5.3 Complexity of Integration Across Nations and Platforms

Integrating defense systems across nations and platforms is complex due to diverse technological landscapes and security requirements in international collaborations. This complexity is evident in integrating autonomous systems like Autonomous Intelligent Cyber Agents (AICAs) with existing infrastructures, hindered by varying technological standards and legacy systems [11].

The integration of Internet of Things (IoT) applications complicates interoperability due to the fragmented nature of IoT technologies, creating research gaps in developing frameworks accommodating diverse IoT functionalities [24]. Specialized security requirements across environments necessitate secure communication and data exchange across platforms. The Idempotent Publish/Subscribe Messaging Environment (IPSME) offers a robust integration framework but faces hurdles due to diverse security needs [21].

Implementing formal standards like the Discrete Event System Specification (DEVS) underscores interoperability challenges, particularly with legacy systems that may not support modern standards. The DEVS formalism provides a structured approach to system representation but requires overcoming technical and operational barriers for integration [5].

Addressing these challenges requires clear and consistent interoperability definitions. Developing universal standards enhances collaboration by providing a common language and framework, facilitating effective integration of systems from different nations and platforms [4]. This approach fosters innovation and collaboration, essential for advancing global defense capabilities.

6 Case Studies and Examples

The exploration of interoperability in defense operations is best understood through specific examples of successful collaborations, such as the partnership between the United States and Singapore. This relationship has evolved over 55 years from a focus on defense technology procurement to a comprehensive partnership addressing cybersecurity and biosecurity challenges. By co-developing capabilities in C4ISR and unmanned systems, Singapore has become a regional hub for non-traditional security threats, enhancing bilateral cooperation in Southeast Asia amid geopolitical tensions [12, 4, 1, 3]. This partnership highlights the strategic importance of bilateral cooperation in facilitating military capability enhancement and technological integration.

6.1 U.S.-Singapore Collaborative Efforts

The U.S.-Singapore collaboration showcases interoperability achievements in cybersecurity and biosecurity, adapting to emerging security threats through effective bilateral cooperation [12]. This partnership underscores the role of strategic alliances in fostering innovation and addressing complex threats, thereby reinforcing interoperability across national borders. A key component is the implementation of conformance service models, including universal, mediated, and localized conformance, which ensure efficient communication and operation across diverse systems [25]. The integration of these models within the partnership demonstrates the potential for standardized frameworks to enhance operational effectiveness and strategic coordination.

Moreover, the integration of the Course of Action Playbook (CMTS) into platforms like the MISP threat intelligence platform exemplifies successful interoperability practices. This integration improves threat intelligence sharing and utilization, enhancing situational awareness and response capabilities in joint operations [1]. The U.S.-Singapore collaboration highlights the importance of advanced technological frameworks and strategic partnerships in overcoming interoperability challenges and enhancing defense operations globally.

6.2 DEVS/SOA Framework for Command and Control

The DEVS/SOA framework significantly advances interoperability in command and control systems by integrating Modeling and Simulation (MS) technologies with Service-Oriented Architecture (SOA) principles. This integration decouples software components from hardware constraints, promoting adaptable command and control functionalities [8]. The Tactical Services Infrastructure, as demonstrated by the TACTICS framework, enhances tactical radio network capabilities to provide and consume services, crucial for maintaining interoperability in dynamic, resource-constrained environments [7].

The DEVS/SOA framework architecture supports multiple rule engines in distributed environments through a unified interface, enhancing management and interaction capabilities of command and control systems [20]. This is critical for resolving mismatches between disparate systems, as shown by the Mediating Connector's application in addressing messaging protocol interoperability challenges [19].

Additionally, the C4ISR Architecture Framework provides a structured methodology for capturing user requirements, facilitating seamless integration of diverse systems within command and control operations [6]. The DEFII framework's application in a cyber system case study illustrates its potential in enhancing interoperability, demonstrating versatility and effectiveness in real-world scenarios [17].

The CAPD framework's deployment in scenarios like scouting platoons further exemplifies its effectiveness in ensuring secure information exchange among military assets, reinforcing command and control system interoperability [9]. Additionally, the SUE platform showcases the innovative design and capabilities that advanced frameworks bring to command and control systems, highlighting their potential to improve operational effectiveness [13]. Collectively, these frameworks underscore the DEVS/SOA framework's critical role in enhancing interoperability within command and control systems, ensuring military operations can adapt to evolving technological and operational demands.

7 Future Directions and Opportunities

7.1 Advancements in AI and Machine Learning

Advancements in artificial intelligence (AI) and machine learning (ML) present significant opportunities for enhancing interoperability in defense technologies by optimizing decision-making and operational efficiency. AI and ML automate complex processes, exemplified by the development of Autonomous Intelligent Cyber-Defense Agents (AICAs) essential for responding to cyber threats dynamically. These technologies enhance coordination among military platforms through improved distributed data analytics and intelligence augmentation, fostering robust human-machine collaboration in multi-domain operations (MDO). This is achieved via a sophisticated intelligence, surveillance, and reconnaissance (ISR) network incorporating autonomous sensors and human intelligence across multiple partners. Autonomous cyber defense mechanisms are crucial for countering intelligent malware, thereby ensuring the resilience of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems in complex environments [2, 11].

The Tactical Services Infrastructure within the TACTICS framework illustrates how AI and ML can optimize service delivery mechanisms, enhancing interoperability in resource-constrained settings. AI-driven optimization promotes reliable service delivery, ensuring seamless communication and integration across military platforms. Future research should focus on refining the GOPPRRE ontology for improved scalability and adaptability, enhancing communication frameworks [18]. Additionally, advancements in automation and dynamic mediation through refined compositional strategies for mediating connector behaviors contribute to enhanced interoperability. Integrating AI and ML into these frameworks can improve the dynamic capabilities of Idempotent Publish/Subscribe Messaging Environments, facilitating effective interoperability.

Incorporating AI and ML technologies into the C4ISR Architecture Framework can significantly enhance integration with Modeling and Simulation (MS) systems, ensuring efficient information processing and dissemination across platforms. Future research should prioritize enhancing the Digital Engineering Framework for Integration and Interoperability (DEFII) by incorporating middleware solutions for tool-specific data representation. Leveraging Semantic Web Technologies (SWT) enables

the creation of a tool-agnostic model representation, serving as an authoritative source of truth and enhancing collaboration and decision-making in complex, multi-disciplinary projects [2, 1, 3, 4, 17].

In the evolving Internet of Things (IoT) landscape, AI and ML advancements are crucial for developing robust standards and enhancing interoperability. Future work should focus on refining definitions and creating standardized protocols for implementation across domains [4]. Implementing an encryption layer for secure data communication is essential to enhance interoperability in defense technology, ensuring secure and efficient data exchange across interconnected systems.

Moreover, blockchain technology advancements are proposed to enhance interoperability in defense logistics and communications by providing secure and reliable data exchange frameworks. Future directions include refining the metadata template to accommodate additional playbook types, enhancing interoperability through advancements in knowledge management systems [1]. Additionally, enhancing the Base Object Model (BOM) to support all levels of interoperation and exploring alternative methodologies to improve composability indicate directions for future advancements in interoperability [3].

Recent research underscores AI and ML's significant role in enhancing interoperability among defense systems, crucial for cohesive and effective operations in a complex global security environment. Key developments include integrating explainable AI for improved human-machine collaboration in MDO, standardized metadata for sharing cyber threat intelligence through machine-readable course of action playbooks, and emerging autonomous cyber defense technologies designed to counter sophisticated cyber threats. These innovations facilitate rapid coalition decision-making and situational awareness, ensuring diverse defense assets can communicate and operate seamlessly in dynamic operational contexts [2, 13, 1, 11].

7.2 Integration of IoT and Cybersecurity

Integrating Internet of Things (IoT) technologies with cybersecurity measures is crucial for enhancing interoperability in defense systems, addressing the complexities and connectivity challenges of modern military operations. IoT technologies enable seamless data exchange across platforms, improving situational awareness and operational efficiency. However, the fragmented nature of IoT technologies poses significant barriers to achieving interoperability, necessitating robust cybersecurity strategies to secure data exchange across heterogeneous systems [24].

Cybersecurity is essential for mitigating risks associated with IoT integration, as IoT devices are often vulnerable to cyber threats that can compromise defense systems' integrity and functionality. The proposed context-aware, policy-driven framework (CAPD) aims to secure information exchange within Internet of Battlefield Things (IoBT) systems, mitigating cyberattack risks and ensuring operational integrity [9]. This framework utilizes ontology-based approaches for knowledge sharing and reasoning, enhancing IoT systems' interoperability by providing a dynamic and adaptable framework for secure data exchange.

Moreover, integrating blockchain technology within military logistics exemplifies innovative approaches to enhancing interoperability by providing secure and reliable data exchange frameworks [16]. Blockchain offers a decentralized, tamper-proof method for securing data transactions, ensuring that information shared across IoT devices remains authentic and unaltered. This integration not only enhances IoT systems' security but also facilitates efficient and trustworthy communication across diverse defense platforms.

The incorporation of Software-Defined Networking (SDN) in tactical environments further illustrates efforts to refine defense technology towards greater interoperability. SDN provides a robust infrastructure for managing network resources and ensuring secure communication across IoT devices, enhancing overall interoperability [15]. By integrating IoT technologies with advanced cybersecurity measures, defense systems can achieve a higher degree of interoperability, adapting to modern warfare demands while maintaining the security and integrity of interconnected systems.

7.3 Strategic Collaboration and Policy Development

Strategic collaboration and policy development are essential for addressing interoperability challenges in defense technology, particularly regarding autonomous systems. The ethical, societal, and legal implications of deploying autonomous systems in military contexts necessitate comprehensive

policy frameworks and international cooperation to ensure responsible operation [11]. Collaborative efforts among nations establish common standards and protocols, crucial for achieving seamless interoperability across diverse defense platforms.

Developing comprehensive and adaptable policy frameworks is vital for guiding the integration of advanced technologies, such as AI and ML, into defense systems. These frameworks must ensure robust human-machine collaboration, facilitate secure information sharing among autonomous assets, and enhance situational awareness in multi-domain operations. They should also address emerging challenges, including cybersecurity threats from autonomous intelligent malware, by incorporating context-aware mechanisms that promote resilience and interoperability across systems and partners [2, 11, 1, 9]. Policies must consider the potential risks and ethical implications of autonomous systems, ensuring alignment with international norms and regulations. Strategic collaboration among allied nations fosters knowledge exchange and best practices, enhancing the development of interoperable systems that improve collective security and operational effectiveness.

Effective policy development is also crucial for establishing standardized interoperability frameworks, vital for seamlessly integrating emerging technologies into existing military infrastructures. This standardization addresses inconsistencies in interoperability definitions across domains and enhances global collaboration and innovation. Implementing formal standards for interoperability, particularly in modeling and simulation for command and control systems, can lead to improved coordination and efficiency in joint and coalition warfare, ultimately enhancing command and control capabilities [5, 4]. By establishing clear guidelines and standards, policymakers can ensure cohesive operation among defense systems from different nations, thereby enhancing overall military interoperability.

8 Conclusion

The investigation into defense technology interoperability underscores its pivotal role in enhancing military operational effectiveness and adaptability. Integrating advanced technologies, such as Autonomous Intelligent Cyber-Defense Agents, is crucial for future cyber defense capabilities, requiring extensive research to address existing technological hurdles. Scalable and secure protocol enforcement, as demonstrated by mechanisms like Cop, enhances the reliability and security of multi-agent systems, highlighting the necessity of robust interoperability frameworks.

A structured framework for interaction semantics serves as a guide for overcoming interoperability challenges and advancing industry standardization. The Situational Understanding Explorer (SUE) illustrates the potential of sophisticated frameworks to improve coalition situational awareness, suggesting avenues for future research on its application in coalition tasks.

Standardization and adaptable architectures are essential to facilitate seamless IoT integration, addressing fragmentation threats to the Internet of Things' success. The Idempotent Publish/Subscribe Messaging Environment (IPSME) presents a feasible solution for integrating diverse systems, promoting scalability and enabling dynamic protocol adaptations.

Integrating High Level Architecture with Model-Driven Architecture is critical for enhancing simulation interoperability and maintaining relevance amid technological progress. The application of blockchain technology is vital in bolstering the integrity and security of military logistics, crucial for advancing defense capabilities.

Despite progress in Software-Defined Networking for tactical networks, significant research gaps remain in interoperability, security, and adaptive traffic management. The LCIM framework emphasizes the importance of aligning conceptual models with technical implementations to achieve meaningful interoperability, positioning the Base Object Model as a key milestone.

These findings highlight the necessity for continuous innovation and strategic collaboration in policy development to address the complex challenges of interoperability in defense technology. Interdisciplinary collaboration, akin to that in healthcare delivery, is equally crucial in defense technology, where AI and advanced technologies can significantly enhance capabilities. Achieving interoperability may not always require rigid standardization; instead, future research should explore flexible design approaches. The ontology developed using the GOPPRRE approach supports model-based systems engineering formalisms and holds the potential to evolve into a standardized ontology for the MBSE community, further advancing data interoperability. These insights are vital for

ensuring military systems operate cohesively and effectively within an increasingly complex and interconnected global security landscape.

References

[1] Vasileios Mavroeidis, Pavel Eis, Martin Zadnik, Marco Caselli, and Bret Jordan. On the integration of course of action playbooks into shareable cyber threat intelligence, 2021.

[2] Alun Preece, Dave Braines, Federico Cerutti, and Tien Pham. Explainable ai for intelligence augmentation in multi-domain operations, 2019.

[3] Wenguang WANG, Andreas TOLK, and Weiping WANG. The levels of conceptual interoperability model: Applying systems engineering principles to ms, 2009.

[4] Giada Lalli. Defining interoperability: a universal standard, 2024.

[5] Saurabh Mittal, Bernard P. Zeigler, and José L. Risco-Martín. Implementation of formal standard for interoperability in ms/system of systems integration with devs/soa, 2024.

[6] Andreas Tolk. Using the c4isr architecture framework as a tool to facilitate vva for simulation systems within the military application domain, 2010.

[7] Alessandro Aloisio, Marco Autili, Alfredo D'Angelo, Antti Viidanoja, Jérémie Leguay, Tobias Ginzler, Thorsten Lampe, Luca Spagnolo, Stephen Wolthusen, Adam Flizikowski, and Joanna Sliwa. Tactics: Tactical service oriented architecture, 2015.

[8] Youssef Bassil. Service-oriented architecture for weaponry and battle command and control systems in warfighting, 2012.

[9] Sai Sree Laya Chukkapalli, Anupam Joshi, Tim Finin, and Robert F. Erbacher. Capd: A context-aware, policy-driven framework for secure and resilient iobt operations, 2022.

[10] Shervin Ostadzadeh and Fereidoon Shams. Towards a software architecture maturity model for improving ultra-large-scale systems interoperability, 2014.

[11] Paul Théron and Alexander Kott. When autonomous intelligent goodware will fight autonomous intelligent malware: A possible future of cyber defense, 2019.

[12] Shaun Kai Ern Ee. Us-singapore cooperation on tech and security: defense, cyber, and biotech, 2024.

[13] Katie Barrett-Powell, Jack Furby, Liam Hiley, Marc Roig Vilamala, Harrison Taylor, Federico Cerutti, Alun Preece, Tianwei Xing, Luis Garcia, Mani Srivastava, and Dave Braines. An experimentation platform for explainable coalition situational understanding, 2020.

[14] Naftaly Minsky and Chen Cong. Scalable, secure and broad-spectrum enforcement of contracts, without blockchains, 2019.

[15] Redowan Mahmud, Adel N. Toosi, Maria Alejandra Rodriguez, Sharat Chandra Madanapalli, Vijay Sivaraman, Len Sciacca, Christos Sioutis, and Rajkumar Buyya. Software-defined multi-domain tactical networks: Foundations and future directions, 2020.

[16] K Hyu Lee and H Sook Park. Study on trends and strategies for defense blockchain and ict technologies. *Electronics and Telecommunications Trends*, 35(1):12–24, 2020.

[17] Daniel Dunbar, Thomas Hagedorn, Mark Blackburn, John Dzielski, Steven Hespelt, Benjamin Kruse, Dinesh Verma, and Zhongyuan Yu. Driving digital engineering integration and interoperability through semantic integration of models with ontologies, 2022.

[18] Lu Jinzhi, Ma Junda, Xiaochen Zheng, Guoxin Wang, and Dimitris Kiritsis. Design ontology supporting model-based systems-engineering formalisms, 2020.

[19] Romina Spalazzese and Paola Inverardi. Components interoperability through mediating connector patterns, 2010.

[20] Pierre de Leusse, Bartosz Kwolek, and Krzysztof Zielinski. A common interface for multi-rule-engine distributed systems, 2012.

[21] Kim Nevelsteen and Martin Wehlou. Ipsme- idempotent publish/subscribe messaging environment, 2021.

[22] Andreas Tolk. Avoiding another green elephant - a proposal for the next generation hla based on the model driven architecture, 2010.

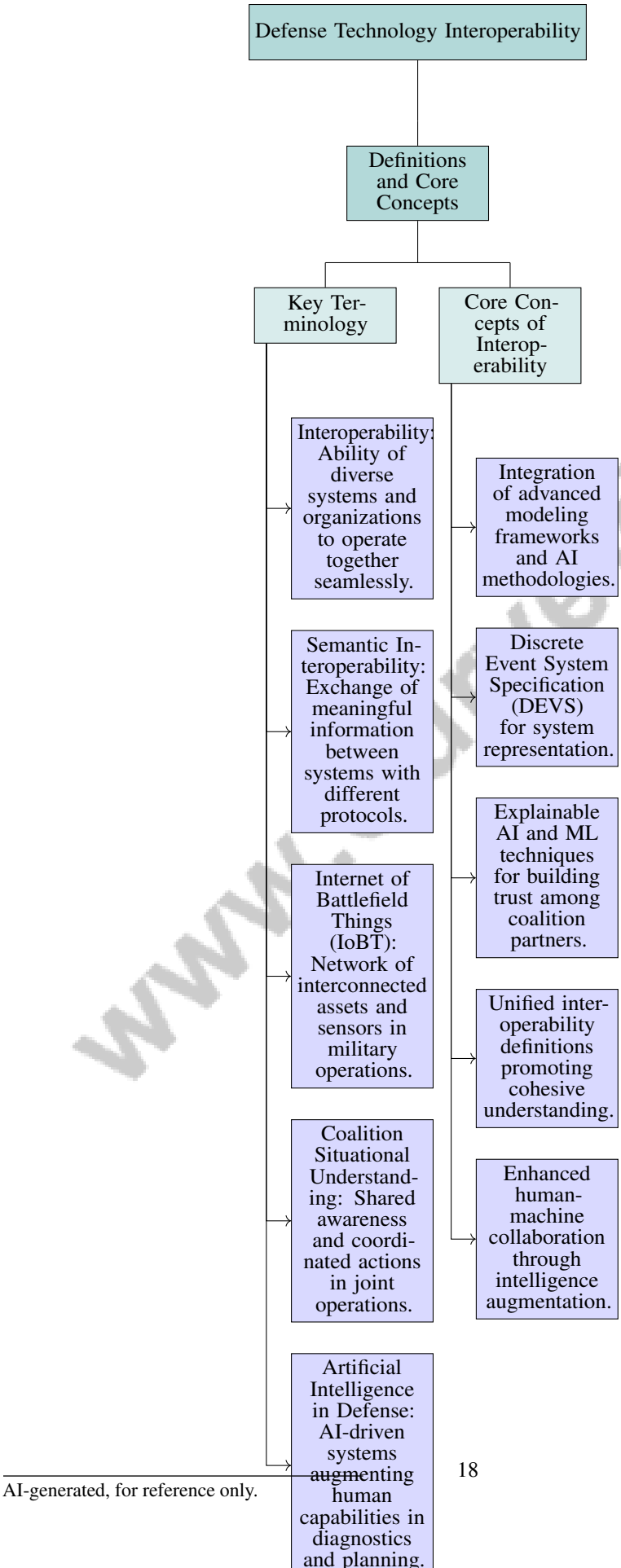
[23] Johannes Reich and Tizian Schröder. A reference model for interaction semantics, 2019.

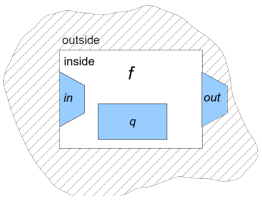
[24] Mohab Aly, Foutse Khomh, Yann-Gaël Guéhéneuc, Hironori Washizaki, and Soumaya Yacout. Is fragmentation a threat to the success of the internet of things?, 2018.

[25] Enrico Coiera. The standard problem, 2023.

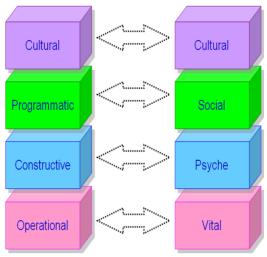
Disclaimer:

SurveyX is an AI-powered system designed to automate the generation of surveys. While it aims to produce high-quality, coherent, and comprehensive surveys with accurate citations, the final output is derived from the AI's synthesis of pre-processed materials, which may contain limitations or inaccuracies. As such, the generated content should not be used for academic publication or formal submissions and must be independently reviewed and verified. The developers of SurveyX do not assume responsibility for any errors or consequences arising from the use of the generated surveys.

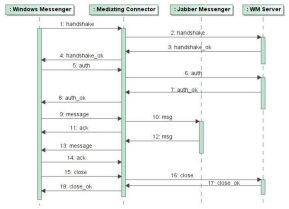

Defense Technology Interoperability
Definitions and Core Concepts
Key Terminology
Core Concepts of Interoperability
Interoperability: Ability of diverse systems and organizations to operate together seamlessly.
Semantic Interoperability: Exchange of meaningful information between systems with different protocols.
Internet of Battlefield Things (IoBT): Network of interconnected assets and sensors in military operations.
Coalition Situational Understanding: Shared awareness and coordinated actions in joint operations.
Artificial Intelligence in Defense: AI-driven systems augmenting human capabilities in diagnostics and planning.
Integration of advanced modeling frameworks and AI methodologies.
Discrete Event System Specification (DEVS) for system representation.
Explainable AI and ML techniques for building trust among coalition partners.
Unified interoperability definitions promoting cohesive understanding.
Enhanced human-machine collaboration through intelligence augmentation.



(a) The image depicts a geometric figure with a shaded area, labeled "outside," "inside," "in," "out," and "q."[23]



(b) The image represents a diagram illustrating the interconnections between different aspects of cultural, programmatic, social, constructive, operational, and vital elements.[10]



(c) The sequence diagram depicts the communication between a Windows Messenger client and a Jabber Messenger server through a Mediating Connector.[19]

Figure 3: Examples of Interoperability Models and Frameworks