UNIVERSITY OF TURKU

Developing capabilities and security for Federated Mission Networking using application of Enterprise architecture model

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Miro Kaunisto

Supervisors:

Seppo Virtanen

Petri Sainio

June 2025

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author(s): Miro Kaunisto
Title: Developing capabilities and security for Federated Mission Networking using application of Enterprise architecture
Number of pages: 77 pages
Date: June 2025

Enterprise Architecture (EA) can be seen as a discipline or structured approach to organize and align an organization's business processes, information systems, and technological infrastructure with its strategic objectives. Enterprise Architecture frameworks aim to improve understanding of complex organizational structures and enable coherent decision-making across different strategic and operational levels. By offering models and methodologies for managing change and complexity, EA supports organizations in achieving greater efficiency, agility, and resilience in dynamic environments.

While EA frameworks offer structured methodologies for organizing complex systems, they can be difficult and complex to apply, particularly within the military domain. One major reason is the inherent complexity of military environments, which often span multiple domains like land, air, sea, cyber, and space that involves numerous interconnected capabilities, stakeholders, and classified information systems.

This thesis examines Enterprise Architecture and its role in strengthening capabilities and cyber security in military context like in Federated Mission Networking (FMN). The primary purpose is to identify different military capabilities and requirements and provide a capability development model for discovering and managing them. This provides a holistic view of an organisation which enables improvement of business operations, IT and cyber security. The research takes a theoretical approach by reviewing EA and military related studies to build a knowledge base, and to propose the model as solution to respond to the identified challenges.

Key findings were challenges with complexity of EA and differences between military and business view of EA related terms and elements. Also bureaucratic structures, regulatory constraints, and security and compliance burdens in public organisations are challenging EA implementations and practices. Importance of EA in holistic cyber security management is also highlighted by improved coordination, risk management, reduced attack surfaces and unified security architectures and mechanisms. The research concludes that Enterprise Architecture can help organisations to improve their capabilities and is essential to concepts like FMN to improve interoperability and security between NATO member states and allies.

The presented capability development model aims to improve the identification of the capabilities and their attributes and to align their management and development. In wider use, it helps users identify gaps and challenges in their capabilities and enables capabilities to be coordinated and interoperated with other parties, which is crucial in FMN context. It enables shifting from minimum viable architectures to full comprehensive models that improve interoperability in strategic scale.

Key words: EA, FMN, NAF, Cyber Security

Table of contents

1 Introduction

1.1 Background and motivation of the thesis

The evolution of enterprise architecture started in the 1980s when information systems began to form into more complex entities. John A. Zachman (1987) presented an idea of architectural representations in describing and developing information systems to form an objective and universal EA framework. Zachman disclosed that information systems architecture consists from the existence of multiple architectural representations rather than a single ones. Representations coexist and can complement each other, adding complexity but also possibilities, and neglecting any one of them poses risks to the system.

Finland officially joined NATO on April 4, 2023, which made it the 31st member of the alliance. Before NATO membership, Finland has trained together with NATO and affiliates through various exercises**,** training programs and cooperation initiatives to enhance interoperability and build collective security. Membership brought new and more requirements on defence capabilities and interoperability, which creates significant pressure to change how we operate and manage our systems in the international environment. There are some capability management frameworks and military focused EA frameworks like NAF, but they can be hard to use for inexperienced user. Goal of this thesis is to provide an EA based application to approach capability identification, management and development in military context, responding to the increasing complexity of systems, and maintaining its control.

Current approaches and used frameworks in FMN context focus on the minimum viable architectures, rather than full comprehensive architecture models, which causes challenges in longer term. To address the complexity and implementation challenges of enterprise architecture frameworks, especially in the military domain, this thesis proposes a simplified capability based EA model, tailored specifically for military organisations to identify and improve their capabilities and to achieve interoperability in federated, multinational environment.

I became interested in Enterprise Architecture and its frameworks during minor studies at Turku School of Economics and noticed their benefit and necessity in working life on several occasions, especially in my work in the public sector. Viability and performance in private sector and companies is quite simple to estimate roughly through turnover and gains, but in the public organisation the same metrics are not usable or relevant, therefore an EA approach

can improve and provide metrics to measure its performance and development. This gave an idea for the thesis, where I study Enterprise Architecture and its impact on capabilities and security in the NATO and defence context. My other driving force was literature and System Thinking -lectures of Esa Saarinen.

The thesis begins with this chapter 1, which provides some background information and motivation of the thesis, scope and research method. In chapter 2 the definition of the Enterprise Architecture (EA) is presented, along with overview of most notable and used EA frameworks. Also NATO Architecture Framework (NAF) is presented, which consider military requirements from an EA aspect. Additionally, EA in the public sector is examined to understand its complexity and identify challenges. Chapter 3 introduces the concept and structure of Federated Mission Networking (FMN). In Chapter 4 the EA related studies and problems in military context is examined and capability based EA model is defined. Chapter 5 consider cyber security aspect of complex systems and how EA and presented capability development model can be used to manage it. The final chapter draws conclusions on the topic.

1.2 Selected research method and scope

This study examines the possible role of Enterprise Architecture in capability and cyber security development especially in military context. It reviews EA related studies and present most notable EA frameworks and related other frameworks and standards. Also FMN and related studies of defence field are reviewed to form an overall picture of the topic. Only publicly available sources have been used to keep the thesis public. Due a nature of complex systems, the management of the EA and evaluation of the outcomes is challenging (Brée & Lager, 2022), therefore the research questions are formulated quite broadly:

Research Question 1: What challenges are there for using Enterprise Architecture approach and practices in military context?

Research Question 2: How could Enterprise Architecture support capability development and security measures in multinational military federation?

These research questions serve as the foundation for the study and guide the focus and scope of the thesis. In conclusions the questions are answered based on findings in literature and with provided model.

1.3 Systems theory

"The central position of the concept wholeness in biology, psychology, sociology and other sciences is generally acknowledged. What is meant by this concept is indicated by expressions such as `system,´ `gestalt,´ `organism,´ `interaction, ´ the whole is more than the sum of its parts` and the like. However, these concepts have often been misused, and they are of a vague and somewhat mystical characters"
- Ludwig von Bertalanffy

Von Bertalanffy (1950) introduced the foundations of General System Theory (GST), where general system laws apply to any system of a specific type, regardless of the particular characteristics of the system or the components it contains. He defines system as a set of interrelated components that form a complex whole, where the interaction between parts leads to collective behaviour. System cannot be fully understood by analyzing its parts in isolation (reductionism) because the interaction and relationships between components are crucial. Most systems are open systems, which interact and continuously exchange matter, energy, or information with their surroundings. Closed systems (mechanical systems) are isolated and unaffected by their environment, having different characteristics and laws. Systems are naturally striving towards stability, closed systems towards equilibrium (no time component, eventually reached) and open systems towards a steady state (constantly under change, reachable under certain conditions). GST belongs to the logico-mathematical discipline proposing the use of mathematical models to describe system dynamics, allowing for the prediction of system behaviour and the identification of patterns common to different types of systems, whether in natural, technological, economic, or social sciences.

Von Bertalanffy's work laid the groundwork for systems thinking, influencing a range of disciplines by encouraging a holistic study of interrelationships, rather than isolated components, addressing the presence of a system. It helps diminishing gaps between fields, leading to the development of new fields of sciences (like cybernetics, systems biology, systems engineering, information systems sciences, and complexity theory).

1.3.1 Systems intelligence

Hämäläinen et al. (2014) wrote a book Being Better Better: Living with Systems Intelligence, which explores the concept of systems intelligence and how it can be applied to improve both

organizational performance and personal life. They state that: "We are always part of systems" and "We can act intelligently from within those systems". Systems intelligence, a term coined by the authors, refers to the ability to sense, understand and act wisely within complex systems. Recognizing how our actions are part of larger systems, we can make better decisions, foster more constructive interactions, and create positive change in both personal and professional contexts. The authors emphasize the importance of seeing the interdependencies in everyday life, where every action or decision can influence other systems and the larger system. We interact with wide range of systems during our lifetime, systems interact among themselves and since many systems are invisible for us, we tend to suffer from systems blindness. By adopting a systems perspective, people can better navigate complexity.

The book provides readers with practical tools and reflection exercises to enhance their ability to sense, understand and influence systems effectively. These tools help individuals cultivate mindfulness about the systems they operate in and make better choices within those environments enabling personal growth and improvement in human interactions. Systems intelligence can also be applied to leadership and management, influencing directly to the organization. Leaders, who recognize systemic interdependencies are better equipped to guide their organizations through change, solve problems, building synergies and foster collaboration. (Hämäläinen et al., 2014)

1.3.2 Complexity theory

Phelan (1999) examined the relationship between complexity theory and systems theory, exploring their similarities, differences, and how they complement each other in understanding complex systems and their behavior. Systemic methods were initially created and implemented in science and engineering, "hard systems", where identifying components, boundaries, and objectives are straightforward and generally acknowledged. However, applying these same principles to "soft" social systems has been more challenging, due the lack of common consensus on the definition of a system. Complexity theory recognize systems that exhibit unpredictable behaviors due to nonlinear interactions between components. It studies how systems evolve, adapt and self-organize, often focusing on open systems with dynamic and evolving patterns. Both theories aim to understand interconnected systems and examine how the behavior of individual components impacts to the overall system's behavior, but from different perspective.

Phelan argues that complexity theory focuses more on nonlinear dynamics and emergent properties in systems, while systems theory examines how systems are aiming and maintaining stability. Systems theory provides a formal structure for analyzing systems, offering models for understanding how systems function in a stable state. It provides tools for modeling and optimizing systems based on their structure. Complexity theory contributes by focusing on systems that are less predictable, emphasizing the role of self-organization, adaptation, and nonlinear change in system behavior. It helps understanding how systems evolve and adapt in changing environments. While systems theory and complexity theory differ in focus, they are closely related and provide complementary tools for analyzing complex systems. Together, they enhance our abilities to understand how systems behave, evolve, and adapt, offering valuable insights for a wide range of disciplines. (Phelan, 1999)

Marion (2008) explored how complexity theory applies to organization and leadership, focusing on understanding how organizations function as Complex Adaptive Systems (CAS) and how leadership can adapt to this dynamicity. In CAS, multiple interconnected agents (employees, teams, departments, processes, etc.) interact dynamically and these interactions create unpredictable behaviors and outcomes, which are greater than the sum of individual actions. Traditional views of leadership focus on command and control, but complexity theory suggests a different approach, where leaders influence rather than directly control outcomes, because emergence of structures and behavioral patterns within organizations results from interactions between agents, rather than from top-down control.

Marion introduces the idea of Enabling Leadership, where leaders create environment and conditions for collaboration, self-organization and innovation to emerge, rather than controlling and directing behavior. This leads to distributed leadership across various levels of an organization, encouraging collaboration, adaptability, and learning from the bottom up. Organizations are dynamic and constantly evolving, requiring leadership that is adaptable to change, and capable of managing the complexity of internal and external forces and demands. Because of this nonlinear nature of organizational behavior, leaders must focus on guiding the organization through change rather than trying to predict every outcome. Study highlights the need of change in leadership thinking, so that organizations are understood as complex systems, and leadership must evolve to manage uncertainty, foster emergence, and support adaptability (Marion, 2008).

Daoudi et al. (2021) studied how complexity impacts to enterprise architecture (EA) and emphasizes the need for adaptive approaches to manage evolving and complex systems. The EA is becoming more complex as organizations grow, integrate new technologies and adapt to changing market conditions. This complexity includes the increasing interconnectivity of systems, applications, data, processes and people and ignoring it leads to inefficiencies, communication barriers, and difficulties in decision making. Traditional EA frameworks often struggle to manage the rapid changes and complexity in modern organizations, especially in terms of scalability and flexibility, making it harder to adapt to new requirements or emerging technologies. Authors propose an adaptive EA approach that involves designing architectures that can evolve and adjust in response to both internal and external changes. This approach emphasizes modularity, scalability and flexibility, using continuous assessment, feedback loops and complexity monitoring to reduce complexity and improve efficiency and responsiveness to changes. They view EA as a system that consist of its components and relationships between them. The primary contributions of the study are to offer decision makers a set of indicators to track complexity and emphasize recognizing complexity within the EA.

2 Enterprise architecture (EA)

2.1 Definition

"***Nothing is as dangerous in architecture as dealing with separated problems."***
- Alvar Aalto

Kappelman & Zachman (2013) define that the Enterprise Architecture (EA) comprises a collection of concepts, methodologies and practices based on holistic system analysis and emphasizing the use of common terminology and principles in engineering and architecture. Numerous existing organizational functions resemble EA activities, yet carried out independently by various groups, utilizing different tools, models, and terminology. The EA aims to connect these disparate activities from strategic to operational level with the goal of improving alignment, integration, optimization, and synergy across the entire organization. Ross et al. (2006) presented that for aligning business processes and IT systems successfully, an organisation must create robust foundation for execution by excelling in three essential disciplines: Operating model, Enterprise architecture and IT engagement model.

Jonkers et al. (2006) states that EA serves as a "blueprint" for systematically defining the current state and the envisioned future state of an organization's structures. It encompasses a structured approach to develop and maintain by encapsulating the fundamental aspects of both the business and its IT operations, including their possible state in the future. EA can be seen also manifesting simultaneously as a process and a product. As a product, it acts as a guiding framework for managers to devise business processes and for system developers to build applications aligned with policies and business objectives. The impact of the architectural process extends beyond the product itself and enhances communication between different groups and stakeholders' awareness regarding business goals and information flow. Communication between stakeholders is crucial for doing EA, since architectural descriptions and knowledge must be shared and agreed (Lankhorst, 2017).

Greefhorst & Proper (2011) also agrees with this by defining two EA paradigms: Enterprises are deliberately designed and implemented systems, capable of being designed and configured again when necessary. The other paradigm acknowledges that enterprises primarily function as social systems, supplemented by technical systems implying that social actors are the core

component of an enterprise. Commitment between individuals and collaboration with technical artefacts is essence of functioning enterprise.

Enterprise Architecture Frameworks serves as structured approaches to do enterprise architecting and frameworks vary widely in complexity, ranging from basic models to more comprehensive ones. EA frameworks are essentially trying to address two primary challenges: how to develop enterprise architecture and how to effectively document it (Conexiam, 2024

Alex Pavlak (2006) introduced two possible approaches to do enterprise architecting: Thin framework and Fat framework. This approach focuses on stable TO-BE state and to the vision of a client using EA development waterfall. It emphasizes the importance of various artefacts to document and communicate the architecture effectively. These artefacts serve as key tools for describing the current state (AS-IS), defining the desired future state (TO-BE) and planning the transition. Creating the TO-BE architecture involves examining the connections between information systems models and business models, but the links between business processes and information systems are often unclearly defined. This approach might be clearer and understandable for organisation, however it is not well-aligned with modern agile practices and framework can be slow to adapt to emerging trends and technologies.

Kotusev & Alwadain (2024) explores the use of Business Capability Models (BCM) in EA practice. Authors focus on how BCMs are used to represent and manage the core business capabilities of an organization. In this approach, BCMs are used to map out an organization's core functions and align them with IT strategies. This helps in identifying gaps, optimizing processes, and ensuring that IT investments support business objectives (Figure 1.). BCMs provide a high-level view of an organization's capabilities, enabling better alignment between business and IT, facilitating strategic planning and improving decision-making. It assists business leaders in seeing how business strategy and its changes affect business capabilities, but it lacks details on how to achieve this and does not describe corresponding modelling approaches. Lack of expressing generated value and limited amount of academic research are probably causes why the use of BCMs is not widely adopted. Additional research on BCMs and how they are applied in practice is needed.

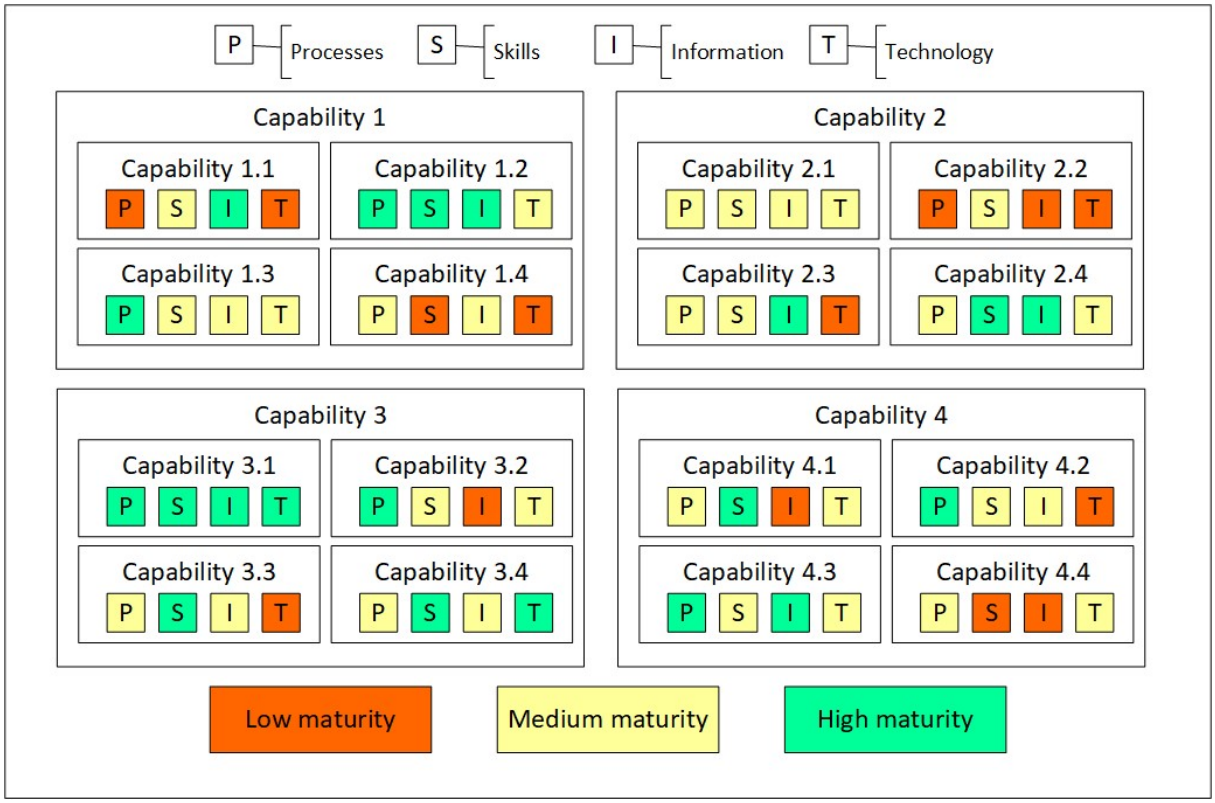

Figure 1. Color-coding of BCMs based on the current maturity of different capability components (Kotusev & Alwadain, 2024)

Current EA frameworks and can be categorized different ways: comprehensive, industry-specific, and domain-specific architecture frameworks. Comprehensive frameworks are industry and domain agnostic enabling broad usability and the two most prominent frameworks are the TOGAF® (The Open Group Architecture Framework) and the Zachman Framework. Industry-specific frameworks are tailored to optimize EA methodologies and practices within a particular industry. There are several industry frameworks like BIAN (Banking Industry Architecture Network), FEAF (The Federal Enterprise Architecture Framework), ODF (Open Digital Framework) and DODAF (Department of Defence Architecture Framework), which will be examined in more detail in this thesis. Domain-specific frameworks are designed to enhance architecture practices within a specific domain. SABSA (Sherwood Applied Business Security Architecture) for example is cyber security focused EA framework (Conexiam, 2024).

2.2 Notable EA frameworks

2.2.1 The Zachman Framework

The first framework John Zachman introduced was for information systems architecture (ISA) that provides taxonomy of concepts for real-world entities with their representations in computer and information systems. As defined earlier, In the context of information systems, the term "architecture" serves as a metaphor, comparing the development of a information system to the construction of a physical building. (Sowa & Zachman, 1992)

The ISA framework expands this metaphor by comparing perspectives between viewpoints used to describe an information system and perspectives of a construction architect. It consist of five row and three column matrix, where columns consist from the Data, Function and Network which represent various abstractions or alternative descriptions of the real world. Rows consists of Scope, Enterprise or business model, System model, Technology model and Components(out-of-context model) which represents different roles and perspectives along with set of constraints, resulting in differing model structures. (Sowa & Zachman, 1992)

The Zachman's Framework for EA (ZEF) have been evolving during years and serves as a cognitive tool to process and communicate information about organizations, encompassing all their concepts and assets. It's not a method, a methodology, or a process model but an ontology, a data model, a blueprint for organizing all enterprise-related information. It is agnostic to processes or methods', implying it is not biased towards the tools or procedures for gathering information and does not dictate which models to employ or how to utilize them, instead proposing a meta-model for each aspect it covers. (Kappelman & Zachman, 2013)

The current ZEF version 3.0 is represented as a two-dimensional matrix (Figure 2) that provides a holistic view of an organization. It includes rows and columns, each representing different aspects of enterprise architecture. The columns of the matrix correspond to six fundamental questions (interrogatives) that must be addressed to fully describe an enterprise. What (Data) describes the data or information involved. How (Function) defines the processes and functions. Where (Network) specifies the locations and distribution networks. Who (People) identifies the roles and responsibilities. When (Time) establishes the timing, schedules and events. Why (Motivation) explains the motivations, goals, and objectives. (LeanIX, 2024)

The rows represent different perspectives, which correspond to different stakeholders or views within the organization. Scope (Planner's View) provides a high-level overview of the enterprise, focusing on strategic goals and objectives. Business Model (Owner's View) represents the business perspective, detailing how the business operates. System Model (Designer's View) focuses on the system design, defining the system's architecture and functionality. Technology Model (Builder's View) considers the technology used, specifying the technology stack and configurations. Detailed Representations (Implementer's View) involves detailed specifications and the actual implementation of systems. Functioning System (User's View) describes the operational system in use, focusing on user experience and system performance. (LeanIX, 2024)

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
Objective/Scope (contextual) *Role: Planner*	List of things important in the business	List of Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goal & Strategies
Enterprise Model (conceptual) *Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (logical) *Role:Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (physical) *Role:Builder*	Physical Data/Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Reprentation (out of context) *Role: Programmer*	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
Functioning Enterprise *Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

Figure 2. Zachman Framework Detailed. Adapted from Dekker and Phogg2 (2008), Wikimedia Commons. Licensed under CC BY-SA 3.0.

Even though frameworks like ZEF are well-known and widely used, there is not a commonly accepted and standardized language for describing the architectural representations within the various cells of these frameworks (Jonkers et al., 2006). Kotusev (2018) stated that various well-known EA frameworks are too theoretical and have little value in practice while more promising tools like the Business Capability Model (BCM) receive minimal attention in mainstream EA literature and lack systematic descriptions. He criticized that ZEF is heavily

focused on documenting a wide array of architectural artefacts and this approach is promoting excessive documentation, also adding more confusion than clarity for EA practitioners. Also not being developed sufficiently to align with modern enterprise architecture practices and not adequately emphasizing the importance of delivering business value or achieving specific outcomes is problematic.

2.2.2 The Open Group Architecture Framework

The Open Group Architecture Framework (TOGAF) is one of the most widely used frameworks for enterprise architecture. It provides a comprehensive approach for designing, planning, implementing, and governing an enterprise's architecture. TOGAF helps organizations develop IT infrastructure that aligns with their business goals, ensuring that both are working seamlessly to achieve strategic objectives. The TOGAF documentation is divided into seven parts (Figure 3), each focusing on a different aspect of enterprise architecture: Introduction, Architecture Development Method (ADM), ADM Guidelines and Techniques, ADM Guidelines and Techniques, Enterprise Continuum and Tools, TOGAF Reference Models and Architecture Capability Framework (TOGAF Version 9.1, 2011).

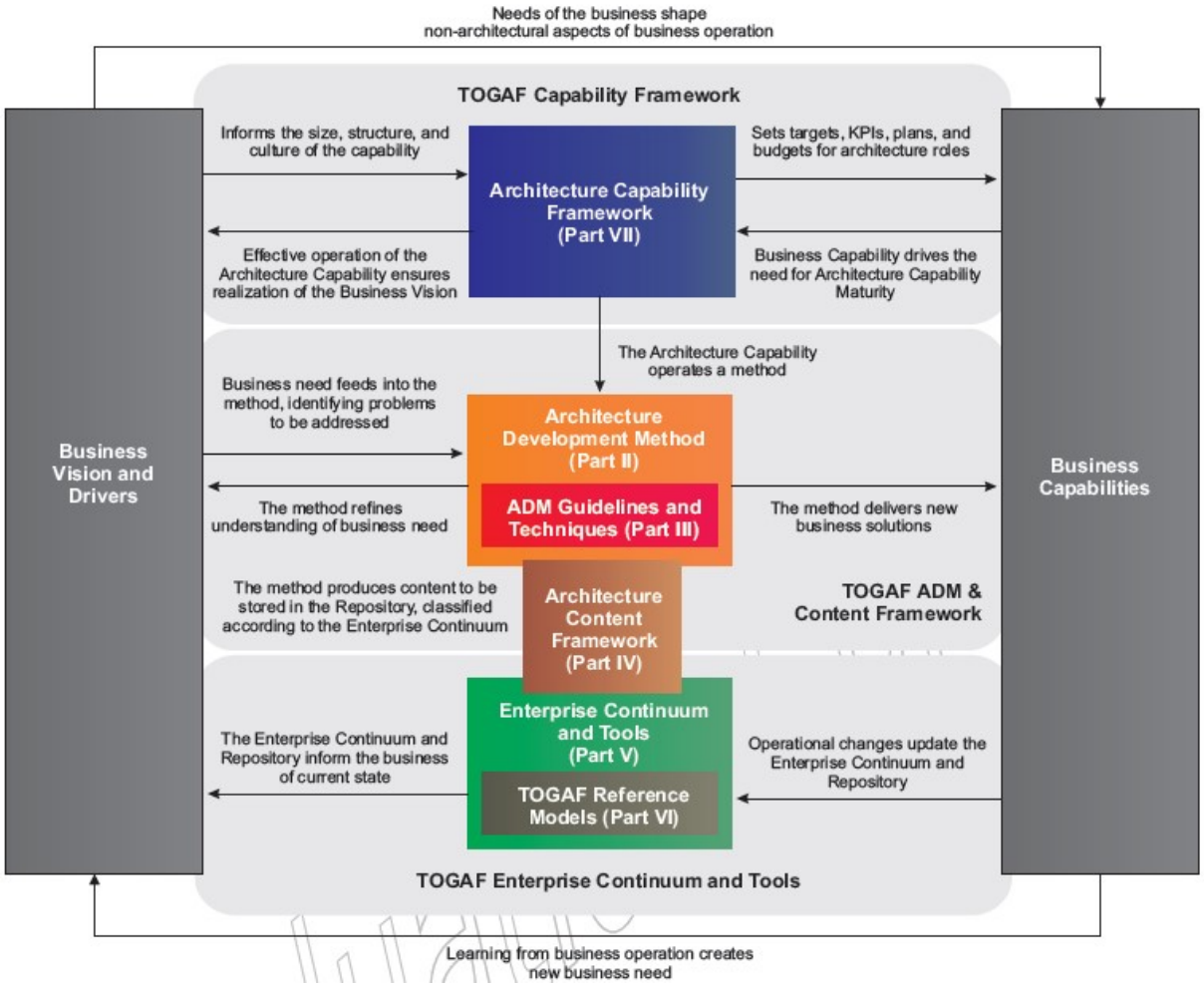

Figure 3. TOGAF. Retrieved from Fenng(dbanotes) (2009), Flikr. Licensed under CC BY-NC-SA 2.0.

Introduction provides an overview of TOGAF, explaining its objectives, structure and intended audience. It introduces the key concepts of enterprise architecture and the framework's role in supporting business and IT alignment. Architecture Development Method (ADM), the core of TOGAF, is a step-by-step approach guiding architects through the process of creating architectures at different levels: business, information systems, and technology. ADM includes (Figure 4) phases such as Preliminary Phase, Architecture Vision, Business Architecture, Information Systems Architectures (Data and Application), Technology Architecture, Opportunities and Solutions, Migration Planning, Implementation Governance, and Architecture Change Management, which will be explained shortly (TOGAF Version 9.1, 2011).

Figure 4. Architecture Development Method. Retrieved from Mirko Wolff (2019), Wikimedia Commons. Licensed under CC-BY-SA-4.0

The Preliminary Phase focuses on setting up the enterprise architecture functions to build an Architecture Capability, which includes tailoring TOGAF to the organization's needs and defining the Architecture Principles. Architecture Vision involves creating an initial architecture vision, defining the scope, identifying stakeholders, gaining approval for a development process and defining the foundation for the change to ensure alignment with business goals. Business Architecture is for developing a business architecture that supports the organization's goals, focusing on understanding the current business environment and defining the target business processes, organizational structures and capabilities to align with the agreed Architecture Vision. (TOGAF Version 9.1, 2011)

Information Systems Architectures details the development of the information systems to support the agreed Architecture Vision and is divided into Data Architecture and Application Architecture. Data Architecture defines the structure of an organization's data assets and Application Architecture defines the blueprint of different application systems and their interactions. Technology Architecture focuses on creating and building the technology infrastructure needed to support the business and information system architectures defining the technical requirements, standards and guidelines for the architecture. (TOGAF Version 9.1, 2011)

Opportunities & Solutions initiates the implementation planning, identifies the possible implementation strategies and selects the most appropriate solution to deliver the architecture defined in the previous stages. Migration Planning develops a detailed plan for migrating from the current architecture to the target architecture and prioritizes implementation projects and resources, addressing potential risks and dependencies during implementation and migration. Implementation Governance provides oversight during the implementation process to ensure that the architecture is followed. (TOGAF Version 9.1, 2011)

Architecture Change Management establishes a process for managing changes to the architecture and ensures that the architecture remains relevant and continues to meet the organization's needs as changes occur. Requirements Management runs concurrently with all other phases and involves gathering, managing, and validating requirements throughout the entire ADM, ensuring that changes in requirements are addressed and integrated into the architecture. (TOGAF Version 9.1, 2011)

ADM provides a comprehensive and structured approach to enterprise architecture development. IT ensures alignment between IT and business strategies and helps managing the complexity of enterprise transformation by breaking it down into manageable phases. ADM is not a linear process; it is designed to be iterative, meaning that architects may revisit and refine previous phases as new information becomes available or changes are required. Being cyclic, after the architecture is implemented and operational, the ADM process can be started again to address new challenges or opportunities. ADM phases can be applied in various orders, the steps can be modified or incorporate other frameworks or methodologies as needed. (TOGAF Version 9.1, 2011)

Following part, ADM Guidelines and Techniques, offers detailed guidelines and techniques to support the ADM phases. It includes methods for adapting the ADM to different contexts,

such as specific industry requirements or organizational needs, and provides best practices for applying the ADM effectively. Architecture Content Framework defines the types of work products that are created during the ADM process, including artefacts, deliverables and building blocks. It offers a standardized structure for organizing these outputs, helping ensure consistency and completeness in architectural work. Enterprise Continuum and Tools provides a classification framework for organizing architecture artefacts at different levels of abstraction. It helps practitioners understand how architectures evolve over time and how different architectures relate to each other. This section also presents tools and resources that can support the use of the TOGAF framework (TOGAF Version 9.1, 2011).

TOGAF Reference Models offers templates and guidelines for developing architecture. The most notable are the Technical Reference Model (TRM) and the Integrated Information Infrastructure Reference Model (III-RM), which provide a starting point for developing specific architectures. Architecture Capability Framework addresses the organization, processes, skills, roles, and responsibilities required to establish and maintain an effective architecture practice within an enterprise. It provides guidance on how to build the necessary architecture capability to support the successful use of the TOGAF framework (TOGAF Version 9.1, 2011).

Kotusev (2019) argues that TOGAF is excessively complex and bureaucratic. It prescribes a detailed and rigid step-by-step process (ADM) that can be difficult to follow in practice and this kind of approach is historically proven to failure. This complexity often leads to a focus on process compliance rather than delivering practical value. The author present three core EA processes: Strategic Planning, Initiative Delivery and Technology Optimization that provide summary of key activities within EA practices. Kotusev (2017) also states that many working EA principles are not TOGAF-specific and many TOGAF features (like ADM, Architecture Content Framework or Enterprise Continuum) are not used in companies ‘using’ TOGAF. He points out that TOGAF has become more focused on certification and standardization leading to a situation where organizations might adopt TOGAF simply to demonstrate compliance or gain certifications, rather than to derive genuine business value from enterprise architecture.

Kotusev (2016) examined the research landscape of EA over the years, analyzing the academic studies and practical contributions made to the field. There has been substantial academic interest in EA, the field is marked by a lack of consensus on key concepts and

practices. This fragmentation has led to challenges in applying EA principles effectively within organizations. Kotusev (2021) concludes that while many frameworks offer valuable perspectives on EA, none of them is a perfect solution and can be costly. The choice of EA practices should be based on the specific needs and context of the organization.

TOGAF v10 was published in 2022, bringing several improvements over earlier versions like addressing modern enterprise architecture needs with enhanced flexibility, guidance and tooling. It introduces a modular structure, making it more adaptable to different business contexts allowing users to adopt the components relevant to their needs without strictly following the entire framework. It provides more practical guides and reference materials, specific content supporting Agile and Lean principles and improved guidance for enterprises to engage digital transformation in the IT landscapes of cloud computing, micro services, digital ecosystems and emerging innovations. It has stronger focus on the interoperability of systems and development of architecture capabilities within organizations including people-centric perspectives. (TOGAF Version 10, 2022)

2.2.3 The Department of Defense Architecture Framework

The Department of Defense Architecture Framework (DoDAF), Version 2.0 serves as a comprehensive framework and conceptual model for creating architectures within the US Department of Defense (DoD). It provides a structured approach for managing and documenting the architecture of complex systems. It supports decision-making by offering a clear, consistent way to view, analyze, and share information about the architecture between various entities such as the departments, Joint Capability Areas (JCAs), missions, components, and programs. DoDAF is a key component supporting the Chief Information Officer (CIO) in fulfilling his responsibilities by establishing a method for illustrating enterprise architecture that enables stakeholders to concentrate on particular areas of interest while retaining sight of the big picture. (DoD-Architecture-Framework v2.02, 2010)

Within DoD process owners specify their architectural requirements and govern development within their respective domains. Components (products and solutions) are expected to align with DoDAF guidelines to ensure consistency, promote information reuse and enforce shared understanding. DoDAF enables the creation of "Fit-for-Purpose" architectural descriptions aligned with specific project or mission objectives. These descriptions vary in content, structure and level of detail based on the intended use, stakeholders and users. (DoD-Architecture-Framework v2.02, 2010)

Architectural data visualization is achieved through models, which can take various forms such as documents, spreadsheets, dashboards or graphical representations. When data are presented within a model, it forms a "view". Collections of views, representing various aspects like processes, systems, or standards, are termed viewpoints and collectively form the Architectural Description. Viewpoints (architecture views) in DoDAF are capability (CV), data and information (DIV), operational (OV), project (PV), services (SvcV), standards (StdV) and system (SV) viewpoints. The aim is to guarantee that a solution meets a defined set of operational or capability needs. The Viewpoints encapsulate the principles, guidelines, and best practices from various domains such as doctrine, operations, business, technology and industry. These serve as the foundation for engineering specifications, establish common elements and guide the development of solutions. (DoD-Architecture-Framework v2.02, 2010)

The Department of Defense Architecture Framework (DoDAF) supports six core processes within the DoD, aiding in decision-making and coordination across various operational areas: Joint Capability Integration and Development System (JCIDS), Defense Acquisition System (DAS), Systems Engineering (SE), Planning, Programming, Budgeting, and Execution (PPBE), Portfolio Management (PfM) and Operations. Joint Capability Integration and Development System is process for identifying, developing, and validating new military capabilities to address operational requirements and gaps, and proposing material and non-material solutions (Figure 24). It ensures that the acquired systems and technologies effectively support joint operations and missions. (DoD-Architecture-Framework v2.02, 2010)

Defense Acquisition System manages investments in technologies and programs to support national security objectives and the Armed Forces. DoDAF supports translating mission needs into well-managed acquisition plans. Systems Engineering ensures that programs commit to robust technical approaches to balance performance and cost. DoDAF supports SE by documenting requirements and design decisions. Planning, Programming, Budgeting, and Execution allocates resources, guides strategy development, and informs decision-making processes. DoDAF supports PPBE by identifying crucial data and facilitating informed decision-making. (DoD-Architecture-Framework v2.02, 2010)

Portfolio Management ensures that IT investments are managed as portfolios to maximize return on investment and support the department's goals. DoDAF assists in analyzing

investment decisions, evaluating risk, and identifying capability gaps. Routine or repeatable business and mission operations are evaluated and captured to enhance architecture repositories with templates and improved artefacts. It contributes to a knowledge-based approach ensuring informed decision-making throughout the acquisition process. Overall DoDAF serves as a tool in aligning operations, guiding investment decisions, and enhancing coordination across various processes within the organization. (DoD-Architecture-Framework v2.02, 2010)

DoDAF have been criticized being ineffective consuming hundreds of millions of money, producing extensive documentation unsuitable for decision-making purposes and with little practical applications. DoD's ability to use the architecture to guide investments have remained limited (Kotusev, 2021). Michael Vinarcik (2019) presented problems with DoDAF like unclearly defined artifacts between entities (projects, missions etc.), artifacts being static hindering agile based development, limited number of viewpoints, siloed and disconnected views without consistency between them.

2.2.4 The Scaled Agile Framework

The Scaled Agile Framework (SAFe) is a framework used for scaling Agile principles and practices across different sized organizations. It provides a structured approach for implementing Agile methodologies especially in complex environments involving multiple teams working on interrelated projects. It provides mindset and agile leadership guidelines enabling growth and holistic views through system thinking. SAFe aims to enhance productivity, quality, and time-to-market by enabling organizations to align and synchronize their teams around common goals. SAFe introduces seven core competencies needed for business agility: Enterprise solution delivery, Agile product delivery, Team and technical agility, Lean–Agile leadership, Lean portfolio management, Organizational agility and Continuous learning culture. Each competency contains three dimensions, which are a set of interrelated knowledge, skills, and behaviours. (SAFE 5.0, 2019)

Key values of SAFe are Alignment, Built-In Quality, Transparency and Program Execution. Alignment is ensuring all levels of the organization are aligned with the business objectives and strategies. Built-in quality emphasizes quality throughout the development process ensuring that every element meets high standards. Transparency encourages openness and visibility into processes, work items and decision-making. Program execution focuses on delivering value and achieving outcomes through effective execution. SAFe is designed to be

flexible and can be tailored to an organization's size, needs and complexity. It can be used at different maturity levels, configurations, which are Essential, Large solution, Portfolio and Full SAFE (Figure 5). SAFe also defines several specific roles and responsibilities to ensure efficient implementation of the framework and practices to align teams with the organization's goals and ensure continuous integration and deployment promoting faster delivery and feedback loops. (SAFE 5.0, 2019)

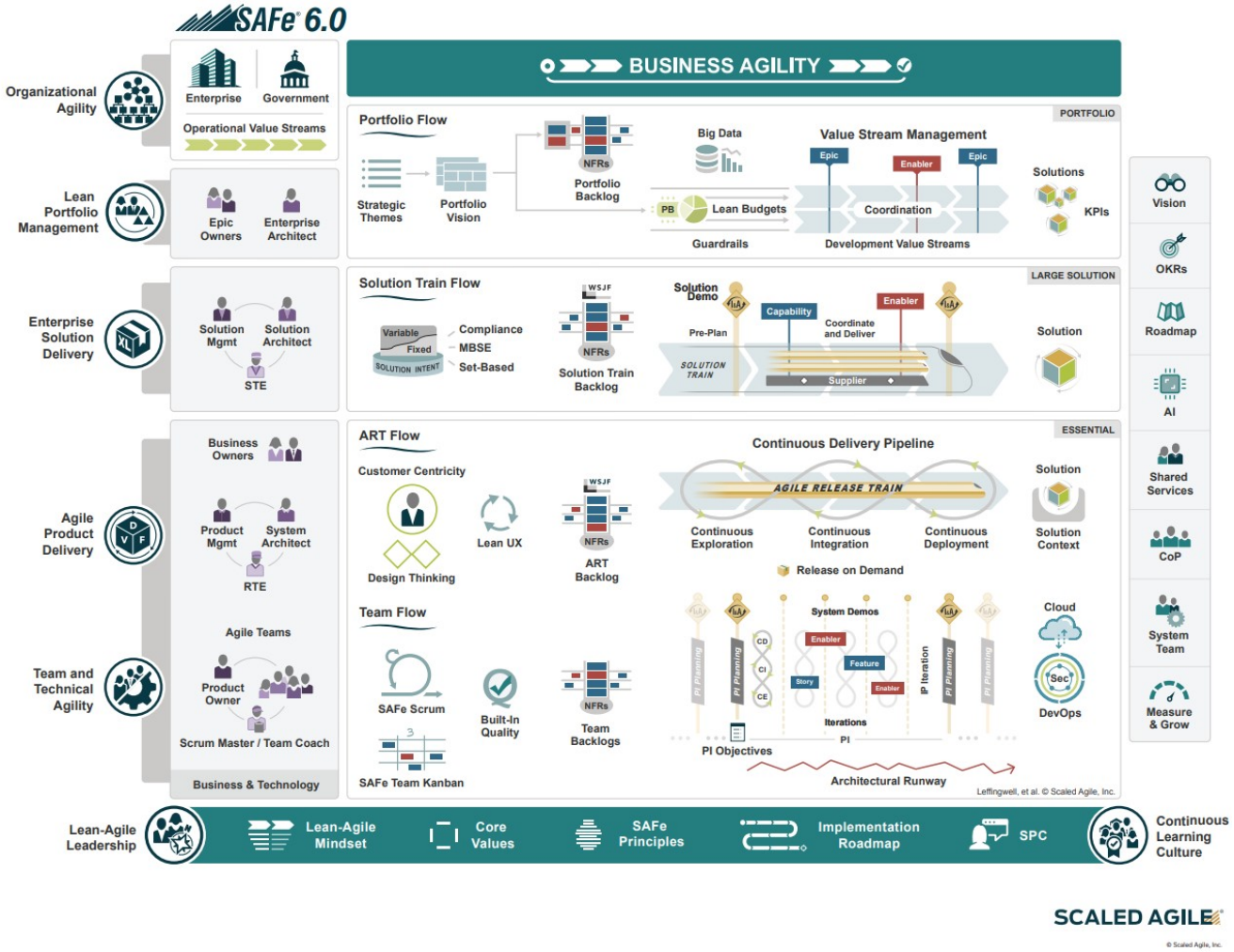

Figure 5. Full SAFe configuration. Retrieved from Scaled Agile, Inc. (2025). Used with permission.

There have been concerns that SAFe can maintain traditional waterfall practices under the guise of Agile, particularly if organisation focuses more on following the framework's processes than embracing agile values. Long-term planning practices (months instead of weeks), controlling processes and bureaucratic and inefficient hierarchical structure are present in SAFe. It is also criticized for its complexity and rigid structure, limiting its flexibility and being too certification centric leading on obtaining certifications instead of

understanding and implementing of Agile principles (Altexsoft, 2023). Safedelusion.com is gathering information from SAFe implementations to improve transparency in agile framework markets since there are very few studies (not gray literature) about SAFe implementations. (Putta et al., 2018)

SAFE 5.0 recognise some of these problems by defining two different systems, where the first system is predominantly hierarchical, typical of most organizations ensuring the efficiency, stability and scalability required to fulfil the current mission and business processes. The second system is a customer-focused network, essential for rapidly delivering innovative solutions in a quickly changing market environment. When recognising these two systems coexist, it's possible to successfully implement EA with SAFe depending how these systems can be reconciled and how holistic the view is. However in a hierarchical public organization, cultural challenges can cause the focus to shift toward the first system without proper governance. (SAFE 5.0, 2019)

2.2.5 Sherwood Applied Business Security Architecture

Sherwood Applied Business Security Architecture (SABSA) is enterprise architecture framework emphasizing security by developing risk-based and business-driven solutions, ensuring that security strategies are aligned with an organization's objectives, risks, and operational needs. It is highly scalable depending on business need and can be integrated with other frameworks and standards, focusing on filling the gaps in security architecture and management. It also helps achieving compliance with multiple regulations like GDPR, ISO 27001 and NIST, by mapping security controls to requirements and improving audition readiness. SABSA introduces business attributes that links business needs to technical solutions, risk management to evaluate balance between opportunities and threats, and also tools to maintain its lifecycle and development. (SABSA, 2009)

SABSA Model divides Security architecture into 6 layers: Contextual Security Architecture, Conceptual Security Architecture, Logical Security Architecture, Physical Security Architecture, Component Security Architecture, and Security Service Management Architecture governing the other layers. These layers maps into the views of different roles (Business, Architect’s, Designer’s, Builder’s, Tradesman’s and Service Manager’s View). From these six horizontal layers and six vertical architectural elements (representing questions: What, why, how, who, where and when), a 6x6 Matrix (Table 1) that represents as model of enterprise security architecture. This model can be aligned with other frameworks

and is actually recommended since focusing security aspects can narrow the view on overall picture. (SABSA, 2009)

Table 1. SABSA Matrix (SABSA, 2009)

Architecture Layer	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
Contextual	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets and Goals	Opportunities & Threats Inventory	Business Value Chain, Capabilities	Org. Structure & the Extended Enterprise	Inventory of Sites, Jurisdictions	Time dependencies of objectives
Conceptual	Business Knowledge & Risk Strategy	Risk Mgmt. Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives	Process Mapping ICT Strategies	Owners, Custodians and Users	Security Domain Concepts	Through-Life Risk Management
Logical	Information Assets	Risk Mgmt. Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps Inter-domain Interactions	Calendar & Timetable
	Inventory	Domain Policies	Information Flows, Services	Trust Models; Privilege Profiles	Domain Definitions, interactions	Deadlines, Start Times, Life Times
Physical	Data Assets	Risk Mgmt. Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary, Storage Devices	Rules, Procedures	Middleware, Systems, Security mechanims	Identity & Access Control	Devices, Networks Layout	Timing & Sequencing of Processes and sessions
Component	ICT ComponentsAssets	Risk Components & Standards	Process Tools & Standards	Personnel Managment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products Data Repositories and Processors	Risk Registers, Analysis Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions;	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers
Management	Service Delivery Management	Operational Risk Management	Process Delivery Management	Governance & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment, Monitoring, Reporting and Treatment	Support of Systems & Services, Activations	Account Provisioning; User Support Management	Buildings, Platforms, Sites, Networks	Calendar, Timetable Management

2.3 NATO Architecture Framework

The NATO Architecture Framework (NAF) is a structured framework used by NATO (North Atlantic Treaty Organization) for the development and management of enterprise architectures within the alliance. The goal of the NAF is to establish a universal standard for developing and describing architectures in complex military systems and it addresses both strategic and tactical aspects of defence planning and operations. It's ensuring that architectures developed within framework are comprehensible, comparable, justifiable and relatable, and provides a common approach for NATO members and partner nations to ensure interoperability, standardization and alignment of military and defence-related capabilities across different nations. The NAF methodology outlines the approach and the context within which architecture-related tasks are conducted and it maintain alignment with other international standards. (NATO Architecture Framework Version 4, 2018)

NAF Version 4 (NAFv4) was released in 2018. Preceding Version 3 (NAFv3) was released in 2007 to enhance alliance interoperability by ensuring consistent use of architectures and enabling the reuse of architecture artifacts and products for system and application descriptions. It had some major flaws like failing to establish a unified architecture approach and projects did not adopt it consistently. The NATO Architecture Body of Knowledge (NABoK) is a comprehensive collection of guidelines, best practices, methodologies, and reference materials designed to assist NATO and its member nations in developing and implementing architecture frameworks. It provides guidance on several key areas, such as: Offering practical examples to illustrate architecture development in line with NATO's goals, **e**xplaining how NAFv4 can be applied within NATO to accomplish specific tasks like Capability Planning or developing Mission Threads (set of steps for ensuring interoperability between systems in mission environments), presenting guidelines on how to use commercial meta-models to create NAFv4 viewpoints and artifacts and providing best practices in transitioning from NAFv3 to NAFv4 ensuring backward compatibility (NATO Architecture Framework Version 4, 2018).

NAFv4 defines architecting principles being derived from broader enterprise principles and can be tailored to guide specific projects based on architecture motivation data. Architecture principles are identified once the organizational context is fully understood and architecture activities have been aligned with motivation data for ensuring that enterprise and project-level principles, goals, and drivers are clear and up-to-date. Architecture descriptions and

architecting stages can be observed from different (architecture) Viewpoints (Operational views, System views, Technical views etc.) based on stakeholder needs. (NATO Architecture Framework Version 4, 2018)

NAFv4 defines that architecture descriptions contains one or more (architecture) Views, addressing specific concerns of stakeholders related to the system of interest. A Viewpoint focuses on particular concerns and multiple Viewpoints may address the same concern. It sets the guidelines for creating and assessing Views that address the concerns framed by it improving focus on different aspects of stakeholders needs. While NAF offers a set of standardized Viewpoints for NAF-compliant architecture initiatives, every Viewpoint is not mandatory and can also be tailored to specific needs. The Viewpoints are structured into a grid representation (Figure 9) to systematically organize subjects (rows) and related aspects (columns). This layout ensures a logical and consistent approach making it easier navigate and understand the relationships between different architectural components. (NATO Architecture Framework Version 4, 2018)

The Viewpoints in the Concepts row assist in aligning capabilities with the organization's strategic goals by analyzing and optimizing their delivery. The Service Specifications row focuses on solely defining the services regardless of their implementation or usage. Services are viewed as units of work that deliver value from a provider to a consumer aiming to create a library of standardized services and supporting service-oriented architectures. The Logical Specifications row focuses on describing solution-independent logical components (capability elements), related activities and resource and information exchanges necessary for executing missions, whether combat or business-related. The Physical Resource Specifications row describes the structure, connectivity, and behavior of Resources. Resources include people, organizations, artifacts, software, hardware and their combinations. Viewpoints of this row focus on how resources are configured and connected to deliver services and enabling capabilities. The Architecture Foundation row supports administrative elements of the architecture, like standards, governance, version control and documentation. (NATO Architecture Framework Version 4, 2018)

Table 2. NAFv4 Viewpoints (Grid Representation) (NATO Architecture Framework Version 4, 2018)

Category	Taxonomy	Structure	Connectivity	Processes	States	Sequences	Information	Constraints	Roadmap
Concepts	C1 Capability Taxonomy *(NAV-2, NCV-2)*	C2 Enterprise Vision *(NCV-1)*	C3 Capability Dependencies *(NCV-4)*	C4 Standard Processes *(NCV-6)*	C5 Effects	–	C7 Performance Parameters *(NCV-1)*	C8 Planning Assumptions *(NCV-4)*	Cr Capability Roadmap *(NCV-3)*
Service Specifications	S1 Service Taxonomy *(NAV-2, NSOV-1)*	S2 Service Structure *(NSOV-2, 6, NSV-12)*	S3 Service Interfaces *(NSOV-2)*	S4 Service Functions *(NSOV-3)*	S5 Service States *(NSOV-4b)*	S6 Service Interactions *(NSOV-4c)*	S7 Service I/F Parameters *(NSOV-2)*	S8 Service Policy *(NSOV-4a)*	Sr Service Roadmap
Logical Specifications	L1 Node Types *(NOV-2)*	L2 Logical Scenario *(NOV-2)*	L3 Node Interactions *(NOV-2, NOV-3)*	L4 Logical Activities *(NOV-5)*	L5 Logical States *(NOV-6b)*	L6 Logical Sequence *(NOV-6c)*	L7 Information Model *(NOV-7)*	L8 Logical Constraints *(NOV-6a)*	Lr Lines of Development *(NPV-2)*
Physical Resource Specifications	P1 Resource Types *(NAV-2, NCV-3, NSV-2a, 7, 9, 12)*	P2 Resource Structure *(NSOV-4, NSV-1)*	P3 Resource Connectivity *(NSV-6)*	P4 Resource Functions *(NSV-4)*	P5 Resource States *(NSV-10b)*	P6 Resource Sequence *(NSV-10c)*	P7 Data Model *(NSV-11a, b)*	P8 Resource Constraints *(NSV-8)*	Pr Configuration Management
Architecture Foundation	A1 Meta-Data Definitions *(NAV-2)*	A2 Architecture Products *(NAV-1)*	A3 Architecture Correspondence *(ISO42010)*	A4 Methodology Used *(NAF Ch2)*	A5 Architecture Status	A6 Architecture Versions *(NAV-1)*	A7 Architecture Compliance *(NAV-3a)*	A8 Standards *(NTV-1/2)*	Ar Architecture Roadmap

NAFv4 defines eight architecting activities (Figure 6) used within different organization levels. Architecture Landscape (AL) Outlines the overall context and specifies the necessary abilities and resources required for architectural development. Architecture Vision (AV) defines the architectural vision by considering the environment, key stakeholders, time

constraints and the urgency for (market) delivery. Architecture Description (AD) presents the architecture from the perspectives of stakeholders, considering the environment and identifying a range of architectural alternatives for assessment. Architecture Evaluation (AE) revises the criteria used for architecture evaluation based on motivational data, assessing each alternative to identify the most suitable ones and forms change requests to achieve optimal trade-offs from the approved best alternatives. Migration Plan (MP) manages and updates the architecture migration plan and defines justification for chosen implementation. Architectures Governance (AG) verifies the implementation of the optimal architecture according to the migration plan and offers guidance to resolve any dependency conflicts. Architecture Changes (AC) evaluate, elaborate and get approval for requests regarding changes in architecture. Motivation Data & Dashboard (MD) manages overall architectural context, constraints and drivers and provide views on architecture progress status and dependencies to other architectures and building blocks. This is done through a dashboard that aligns products with the overall landscape, including reference libraries and repositories. (NATO Architecture Framework Version 4, 2018)

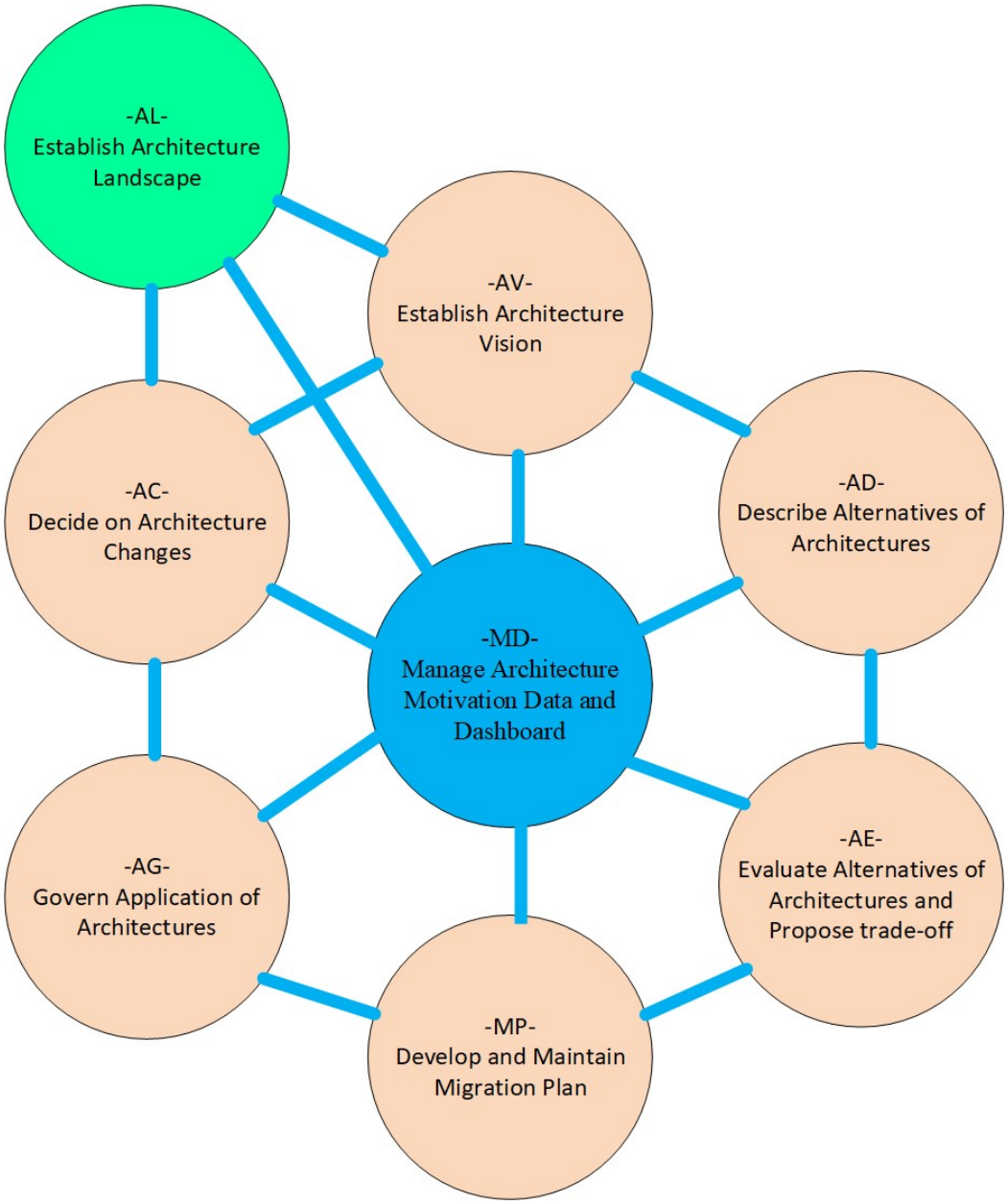

Figure 6. Architecting stages (conducted from TOGAF/ ADM) (NATO Architecture Framework Version 4, 2018)

This approach enables the use of multiple Viewpoints and Views (NAFv3) at various stages of architecture development, aiming to gather and manage architecture motivation data, elements that guide the architecture process from vision to the last step of iteration cycle. It expands the traditional requirement baseline to include broader factors like goals, expectations, constraints, drivers, risks, costs, value, and opportunities. NAFv4 architecting method draws inspiration from the architecture description method (ADM) of the TOGAF with couple differences: to comply with EA standards ISO/IEC/IEEE 42010, 42020 and

42030, simplifying its implementation across various environments beyond just information technology and to enable flexible progression through different stages of the architecture process. NAFv4 architecting method enhances the requirements management phase by adding traceability to architecture products by maintaining an architecture dashboard. It emphasizes decisions to adjust architecture in response to evolving motivation data and also offers guidance on evaluating the architecture and analyzing trade-offs when identifying and comparing different alternatives (NATO Architecture Framework Version 4, 2018).

The NATO Architecture Framework is a vital tool for NATO, its member states and partners providing a standardized approach to enterprise architecture that ensures interoperability, enhances operational effectiveness and supports the development of future capabilities. Through its structured methodology and alignment with international standards, NAF supports NATO to achieve its strategic goals and maintain its position as a leading global defence alliance.

NAF v4 is also compatible with ArchiMate modelling language with small changes to support NAF Viewpoints. EA elements are tailored to correspond with NAF structures to improve compliance, usability and clarity. Viewpoint layer colours are used on related EA elements in ArchiMate models of Viewpoints to improve clarity. (Archimate Modeling Guide NAF v4, 2025)

However, NAF v4 have some flaws like trying to consider too many possible aspects of Viewpoints, leading to complex mess of concerns, usage possibilities, representations and their examples. It is also shifting focus from the capabilities into views of stakeholders, which may lead to a distorted perception of the relationships between capabilities. Focus in NAF is also mainly in NATO operations, while the true value of Enterprise architecture comes at a strategic level. Also tailoring, local extensions, and freedom through flexibility can cause divergence and incompatibility if not tightly governed.

2.4 Other standards and frameworks

2.4.1 ISO/IEC 27001

ISO/IEC 27001:2022 is the latest version of the ISO/IEC 27001 standard which provides a framework for an information security management system (ISMS). Original version was

published in 2005, revised in 2013 before latest version. It defines the requirements to establish, implement, maintain and continuously improve an information security management system in any organization and provides an overview and terminology based on the ISO/IEC 27000 family to ensure common understanding and clear key elements in systematic information security management. The changes to 2022 version were reduced number of controls though consolidating and reorganizing them into four groups: Organizational, People, Physical and Technological controls. Also new controls were introduced: Threat intelligence, cloud security, ICT readiness and business continuity, Data masking and leakage prevention, monitoring activities, web filtering and security coding. (ISO/IEC 27001:2022)

Key elements of the ISO/IEC 27001 are common terminology, organization intelligence, leadership, planning, support, operation, evaluation and continual improvement. Organization intelligence means understanding the organization and its context, identifying requirements of the stakeholders and determining the scope of the ISMS and establishing it. Leadership means commitment and governance from top management and assigning roles and responsibilities. Planning contain evaluating risks and opportunities, assessing and treating information security risks and defining security objectives. Support means adequacy of resources, competence and training, communication and documentation management. Operation consist of planning and controlling operations, risk management and security control implementations, monitoring and reviewing the ISMS. Evaluation refers to monitoring, measuring and analysing the performance, doing internal audits and management reviews. Continual improvement means handling and analysing nonconformities for identifying correct measures to improve ISMS. (ISO/IEC 27001:2022)

Benefits of using ISO/IEC 27001 are up-to-date security practices that enable addressing current and emerging threats. Improved efficiency from easier implementation and maintenance enabled by streamlined controls and documentation requirements. Improved risk management with enhanced focus that helps identifying and mitigating security risks. Increased resilience improves ability to respond and recover from security incidents. Implementing security mechanisms defined in ISO/IEC 27001:2022 can help organizations enhance their information security level, comply with regulatory requirements, and build trust with stakeholders by demonstrating a commitment in protecting sensitive information. (ISO/IEC 27001:2022)

2.4.2 KATAKRI

Katakri is a tool and collection of security measures for information security auditing, that stands for kansallinen turvallisuusauditointikriteeristö (national security auditing criteria) and its first version was presented in 2009. Currently version Katakri 2020 is governed and improved by Finnish NSA (National Security Authority) and its stakeholders. Katakri can be used for evaluating the maturity of security implementations of the company, community or authority. It consist of three different areas: Safety management, Physical security and Technical information security. (Katakri 2020)

The safety management aims to ensure sufficient security procedures and information security management systems for protecting classified information. The Physical Security focuses on requirements for the environment where classified information is used or managed. The technical information security defines security requirements for the technical solutions which are divided into three sub-areas: Communications security, information systems security and operations security. (Katakri 2020)

Communications security includes network architectures, topologies, monitoring, segmenting and filtering, wireless and wired data transfer and service systems, boundary protection services and other information processing environments. Systems security consist of access management, access verification, system hardening, incident detection, traceability and recovery, crypto solutions, security software's, electric and electromagnetic protection (Tempest) and life cycle management of all above. Operations security focus on maintaining the life cycle of information processing environments, the exchange and handling of classified information, remote use and its management, change management, disposal of classified information, management of software vulnerabilities and countermeasures. (Katakri 2020)

Requirements of Katakri allow different options for implementation. This supports interoperability between solutions and life cycle management yet still achieving minimum protection requirements. However, requirements of Katakri cannot be used alone, but sufficient protection must be considered on a case-by-case basis in each case. (Katakri 2020)

2.4.3 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) 2.0 is an updated version of the original NIST Cybersecurity Framework, which is a tool to improve and organise cybersecurity measures

and maturity by providing guidelines and best practices for organizations to manage and reduce cybersecurity risks. Developed by the National Institute of Standards and Technology (NIST), the CSF is widely used across industries to enhance the security and resilience of critical infrastructure and sensitive information. Primary audience for the CSF are individuals and groups responsible for developing and leading cybersecurity programs of the organizations but CSF can be also used for cybersecurity risk management. (The NIST Cybersecurity Framework (CSF) 2.0, 2024)

The core components of the framework are divided into six functions: Govern, Identify, Protect, Detect, Respond, and Recover. These functions provide a set of desired cybersecurity activities and outcomes using common, comprehensible language and enables strategic view of the lifecycle of an organization's cybersecurity risk management. The Functions should be addressed simultaneously. Actions supporting Govern, Identify, Protect and Detect should occur continuously, while actions supporting Respond and Recover should be prepared at all times and activated when cybersecurity incidents happen. Each function plays a crucial role in managing cybersecurity incidents. Govern, Identify and Protect help in preventing and preparing for incidents, while Detect, Respond, and Recover are essential for discovering and managing incidents. (The NIST Cybersecurity Framework (CSF) 2.0, 2024)

CSF implementation level (Tiers) indicates maturity of an organization's cybersecurity risk management practices. Tier 1 (Partial) indicates lack of cybersecurity risk management processes and practices are reactive. Tier 2 (Risk informed) means that risk management processes and practices are in use but not established organization-wide. In Tier 3 (Repeatable) risk management practices have been formally approved and have their own policies. Tier 4 (Adaptive) means that risk management practices are part of the organization's culture and are constantly evolving. CSF also provides different profiles that align cybersecurity activities with business requirements based on selected outcomes. CSF 2.0 also includes Supply Chain Risk Management for recognizing the growing importance of securing interconnected systems and third-party relationships

2.4.4 Information Technology Infrastructure Library

Information Technology Infrastructure Library (ITIL) is a framework for IT service management (ITSM). It provides best practices and guidelines to help organizations effectively manage and improve their IT services and align them with business needs providing organizational agility and resilience. Its purpose is to ensure a flexible, coordinated

and integrated system for the efficient implementation and governance of IT-enabled services and continuous service delivery. (ITIL 4 foundation book, 2020)

First version of ITIL was developed during the 1980s by British government's Central Computer and Telecommunications Agency (CCTA) and it consisted of over 30 books. These books were developed and released over time and contain of best practices in IT compiled from various public and private sector sources globally. The objective of ITIL was to gather and compile best practices that could address lack of standardization, frequent errors and rising costs of information technology within the organization rather than to create a commercial product. Over time, ITIL's utility and credibility were recognized and in 2005 ITIL version 2 and its practices contributed to the ISO/IEC 20000 Service Management standard and were aligned with it. After that ITIL was revised in 2007 as version 3 (reorganised in 2011) and in 2018 version 4 was published with major changes. (White & Greiner, 2022)

ITIL v3 focused on a lifecycle approach to service management consisting of five core stages and their practices: Service strategy, Service design, Service transition, Service operation, and Continual improvement. ITIL v4 align with these elements and provides more holistic, flexible, and agile approach to ITSM, aligning with modern practices like DevOps, Agile, and Lean. It focuses on the value co-creation with customers and other stakeholders using Service value system (SVS) consisting of five components (Figure 7.): Guiding principles, Governance, Service value chain, Practices and Continual improvement. For ensuring a holistic approach, ITIL v4 defines four dimensions that should be taken into account for every component of the Service Value System (SVS). These four dimensions are: organizations and people, information and technology, partners and suppliers, value streams and processes seen in Figure 8. (ITIL 4 foundation book, 2020)

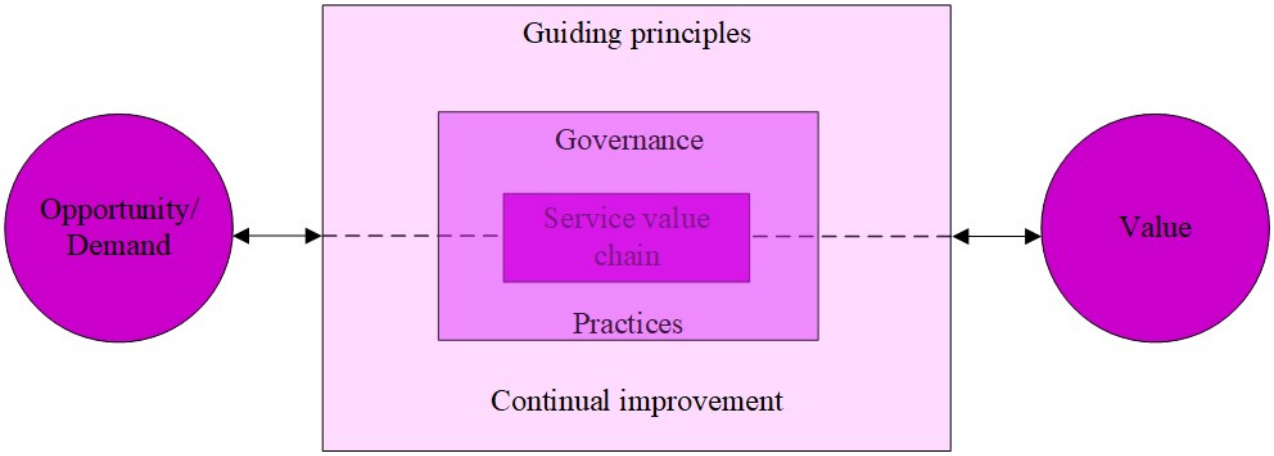

Figure 7. The ITIL service value system (ITIL 4 foundation book, 2020)

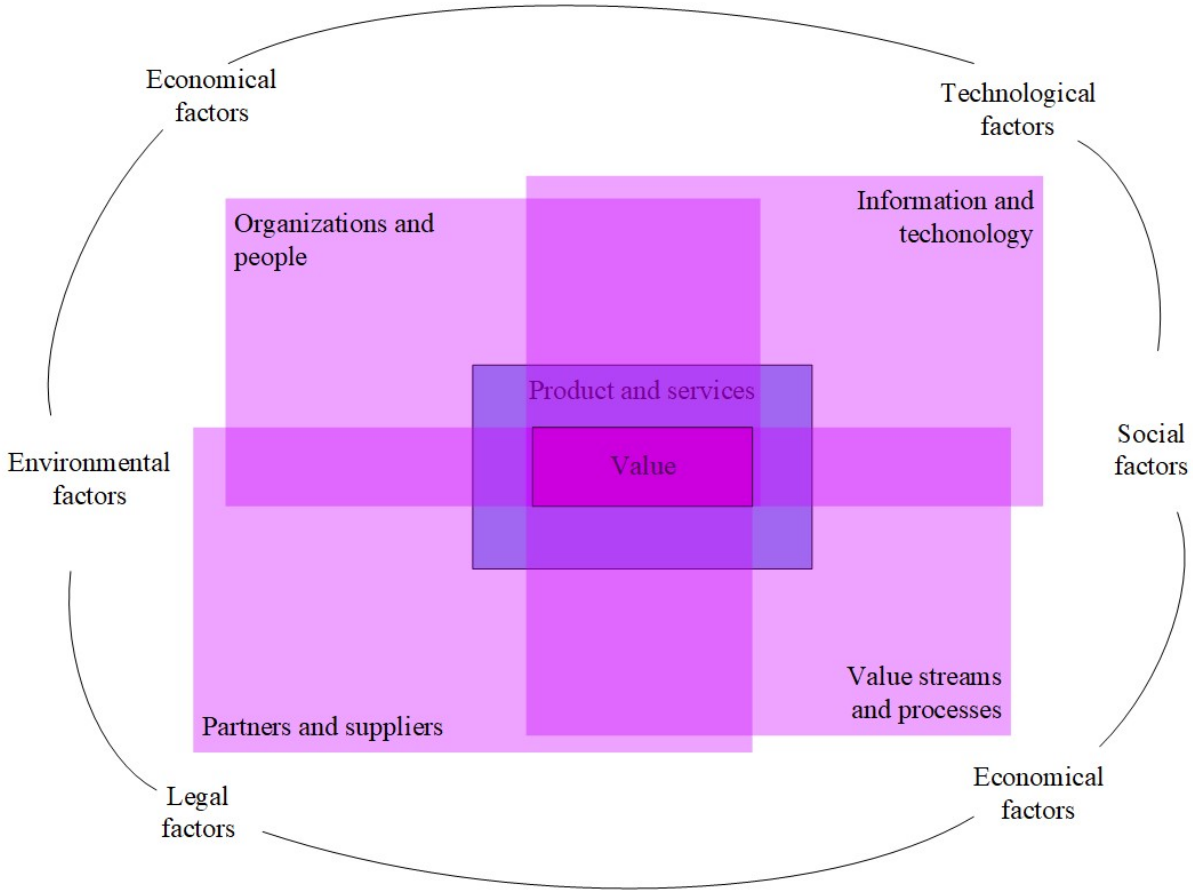

Figure 8. The four dimensions of service management (ITIL 4 foundation book, 2020)

2.4.5 Network and Information Systems Directive 2

Network and Information Systems Directive 2 (NIS2) is an updated version of the original NIS Directive from 2016, which is a part of EU legislation for improving the cybersecurity and resilience of critical infrastructure within the European Union. The directive seeks to improve the overall security and interoperability of network and information systems across EU members, particularly those systems critical to the economy and society. NIS2 expands the scope to include more sectors and services beyond those covered in the original NIS Directive such as energy, transport, banking, financial market infrastructures, health, water supply, digital infrastructure and medium-sized and large businesses in these key sectors. NIS2 represents a significant step towards strengthening the EU's cybersecurity framework, responding to the evolving threat landscape, and ensuring that critical sectors are well-prepared to manage and mitigate cybersecurity risks. Public organisations that practice activities mainly for national security, public safety, defence or law enforcement are excluded from NIS2 directive therefore its impact to this thesis is minor (NIS2 Directive, 2022).

2.5 Enterprise Architecture in public organizations

Dang & Pekkola (2016) studied root causes of problems with EA and its implementation in public organizations: In many public organizations, departments operate in silos with little or without communication between them. EA aims to integrate these departments, but the siloed mentality often limits cooperation leading to incomplete or ineffective implementations. Public sector organizations tend to have complex organizational structures and multiple layers of management making EA implementation a bureaucratic and slow process. This complexity often causes delays in decision-making and execution. EA implementation also often faces cultural challenges and resistance from employees accustomed to existing processes. Change management becomes difficult as individuals revert to old ways of doing things, failing to realize the full benefits of EA, as essential changes in process or mindset are ignored. There should be common consensus and understanding of EA.

Public organizations usually have budget constraints and have to strictly follow policies and legislation, which can limit their ability to fully implement EA. This includes the cost of necessary software tools, hiring skilled personnel, and maintaining systems. In public organizations the amount of stakeholders is vast and getting all parties on board can be

difficult, which limits the effectiveness of EA efforts. Public sector projects often prioritize immediate results (due political pressure), which can conflict with the long-term nature of EA. The pressure to show quick wins can lead to shortcuts or misalignment between strategic goals and EA objectives. EA implementations can also be too technology focused if IT departments are responsible of EA teams and programs, instead of business units.

Ylinen & Pekkola (2018) studied difficulties of organizational transformations in public sector and why EA is hard to successfully implement. Before adopting EA, approach of the organization under study was fragmented with siloed IT development focusing on single departments. Other challenges were key person dependency and an excessive focus on technology rather than holistic management. With the organization's growing investments in digitalization, the IT department was under pressure to shift toward comprehensive IT management and EA was introduced to achieve it. However, lack of communication and collaboration between the EA team and IT project managers, insufficient EA tools and standardization, slow and hesitant decision-making, and lack of mutual understanding of EA resulted in short-term solutions rather than achieving the broader objective of comprehensive IT management. Transformation required not only a shift in strategy and services but also change in relationship between customers and IT department which caused tension and disagreement. Change initiatives in the public sector often create tension between maintaining the stability and the need for transformation. Exploring and identifying organizational tensions is crucial for resolving these challenges and EA does not cause them, but make them visible. Seppänen et al. (2018) recommend that any EA implementation project should prioritize the three key areas: Resistance towards EA, relevant and clear EA goals, and EA tools and practices.

Lemmetti & Pekkola (2012) investigated the perceptions and understanding of enterprise architecture among Finnish public sector organizations and found out that there is significant variation in how different organizations understand and apply EA. Some organizations have started to recognize EA as a strategic tool for coordinating different sectors and improving decision-making processes, some see it focusing mainly on IT systems, only consuming resources and being too complex and difficult to implement, especially in a context of the public sector’s unique needs and constraints. In the survey of qualitative research almost any responder did not see themselves as developers of EA activities, except Defence Forces and health sector. The development of the to-be architecture is also rare in many organizations;

Defence Forces have been doing it since 2004, making it probably having longest history with EA in the Finnish public sector.

Banker et al. (2011) studied role of Chief information officer (CIO) and how reporting structure (to CEO or CFO) and strategic positioning of the CIO affects on organization's ability to lead IT transformation to support business strategy and the alignment of IT with organizational goals. They found out that involvement of CIO in strategic decision-making and participate in high-level business discussions have a strong positive impact on performance of the organization by better integration of technology with business strategies, enhancing organizational efficiency and innovation. Organisations recognizing the importance of IT by giving the CIO direct access to the CEO are more likely to notice positive impact on performance and competitive advantage. Hussain et al. (2016) studied difficulties in identifying the CIO's role in public sector and how limited awareness among decision makers regarding the importance and strategic value of the CIO affect the overall implementation of ICT in public organizations. Institutional and cultural barriers, resource and capacity limitations, lack of strategic IT vision and political support are problems with many public organisations and can be answered and mitigated with creation of the CIO role for aligning IT resources more effectively and leading digital transformation.

In Finland, Enterprise Architecture is actively used within public organizations through the Public Sector ICT (JulkICT) initiative, guided by the Public Administration ICT Steering Group (JUHTA). JUHTA oversees and guides the digital transformation of public services, setting the requirements how EA should be adopted across various governmental sectors. Finland’s approach to EA in public administration emphasizes efficiency, transparency and interoperability across different organizations, reducing overlapping work, and ensuring smooth coordination between municipalities, government agencies, and service providers (VM, 2024).

Before the Act on Information Management in Public Administration (906/2019) came into force on 2020, Public Administration ICT Steering Group managed JHS (Julkisen hallinnon suositukset)-system that provided JHS-recommendations. These recommendations were guidelines specifically created for public administration in Finland for adopting information management practices to improve interoperability, support digitalization of public services, and support the development and management of their information systems (DVV, 2024). JHS 179 (Design and development of the enterprise architecture) and JHS 198 (Descriptions

of the enterprise architecture) were major recommendations related to EA and were based on TOGAF v. 9.1 (DVV, 2024).

Act on Information Management in Public Administration (906/2019) includes all statues and regulations how public administration have to preserve corporate governance in information and data management by maintaining interoperability of information systems and resources, implementing of those systems, technical solutions and information security, and describing and documenting those systems, resources and solutions. (VM, 2024) This helps public sector organizations to better manage their information assets, improve service delivery, and comply with both national and EU-level regulations.

The national level use of EA in Finland activated and got attention when the new ICT strategy was presented by Minister of Public Administration and Local Government in 2012. After that, many projects, working groups and advisory boards have been initiated by Ministry of Finance to improve the use of ICT (EA) in public administration (VM, 2012): Advisory Board on Information Management in Public administration (Julkisen hallinnon tietohallinnon neuvottelukunta, active 1.1.2010 – 31.12.2012) (VM, 2010), Advisory Board on Enterprise Architecture (Kokonaisarkkitehtuurijaosto (JHKA-jaosto), active 1.5.2013 – 29.2.2016) (VM, 2013), Advisory Board on Enterprise Architecture in Public administration (Julkisen hallinnon yhteisen kokonaisarkkitehtuurin (JHKA) työryhmä, active 23.6.2016 – 28.2.2019) (VM, 2015), Advisory Board on Enterprise Architecture in Public Administration (Julkisen hallinnon kokonaisarkkitehtuurijaosto, JHKA-jaosto, active 27.5.2019 – 31.12.2019) (VM, 2019), Advisory Board on Interoperable Services Architecture in Public Administration (Julkisen hallinnon toiminnan kehittämisen arkkitehtuuriyhteistyöryhmä, active 1.10.2020 – 31.12.2023) (VM, 2020).

Current initiatives to improve EA in Finnish public administration are: Advisory Boards on Information Management (Tiedonhallinnan yhteistyöryhmät): Expert Group on Information Management in Public Administration (Julkisen hallinnon tiedonhallinnan asiantuntijaryhmä VM099:00/2024, active 01.05.2024 – 31.12.2027) (VM, 2024), Advisory boards of Coordination Group for Digitalisation (Digitoimiston yhteistyöryhmät): Strategic Advisory Board on Digitalisation and the Data Economy (Digitalisaation ja datatalouden strateginen yhteistyöryhmä, active 2.4.2024 – 31.12.2027) Advisory Board on Information Management in Central Government (Valtionhallinnon tiedonhallinnan yhteistyöryhmä (VALTI), Strategic Advisory Board on Cyber Security in Public Administration (Julkisen hallinnon

kyberturvallisuuden strateginen yhteistyöryhmä, active 12.6.2024 - 31.12.2027) (VM, 2024). Coordination Group for Digitalisation (Digitoimisto) is a group of experts and representatives from each ministry and its role is to coordinate cooperation between ministries and oversee efforts to advance digitalisation and the data economy within central government (VM, 2024).

Even though responsibility of EA is heavily on Ministry of Finance, some other ministries and agencies are also giving contribution. Digital Office - Coordination Group (Digitalisaation ja datatalouden vastuualueen yhteistyöryhmä (Digitoimisto) 14.10.2021 –) is a permanent cooperation group, initiated by Ministry of Transport and Communications, that functions as the secretariat for the ministerial working group responsible for societal reform concerning the data economy and digitalization (VN, 2021). The Digital and Population Data Services Agency supports EA activities in public administration through Architecture Guild (Arkkitehtuurikilta), which is a network of public administration trying to improve the expertise of architects at national level and share experience and practices between different industries and actors (DVV, 2024).

3 Federated Mission Networking (FMN)

”Eripura omissa joukoissa iskee pahemmin kuin vihollisen miekka."
-Carl Gustaf Emil Mannerheim
("Dissension in own troops strikes worse than the sword of an enemy")

Not only dissension in morale but also in the strategy, capabilities, systems and operating methods.

3.1 Definition and Objective

In November 2012, development of the Federated Mission Network (FMN) was initiated under the guidance of the Military Committee. The FMN aims to facilitate efficient information sharing between NATO, NATO member nations, and non-NATO entities (NATO friendly nations and organisations, collectively referred to as Affiliates) (NATO C2COE, 2020). Federated Mission Networking (FMN) framework is a structured conceptual framework that includes the people, procedures and technology needed to initiate, organize, develop, utilize, and enable capabilities for (Federated) Mission Networks. FMN principles are based on the experiences gained from the deployment of the Afghanistan Mission Network (AMN) and the NATO Network Enabling Capability (NNEC) Programme (NATO COI, 2024).

The FMN framework offers comprehensive resources such as processes, plans, templates, enterprise architectures, capability components, and tools necessary for strategizing, organizing, constructing, developing, managing, implementing and concluding Mission Networks to support Alliance in decision-making, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), and multinational operations within dynamic environments. The FMN Framework serves as a continuous, structured basis to guarantee the effective establishment and management of mission networks, whether for operational activities, exercises, training initiatives or interoperability assessments. (NATO COI, 2024)

The root of FMN is trust, willingness, and commitment. FMN Participants are participating in joint exercises and missions, each maintaining authority over their own capabilities and operations while following agreed requirements. FMN Affiliates are actively involved in continuous efforts to improve and maintain the necessary capabilities for establishing and managing mission networks. They regularly participate in NATO’s collective testing-,

verification- and validation exercises to develop and maintain full interoperability of their forces and assets. Once they meet the compliance with standards necessary for Federating Mission Networks, they can become Mission Network Participants (NATO COI, 2024). FMN capabilities are a crucial part of the Connected Forces Initiative (CFI), which strengthens communication, training, and cooperation between NATO and partner forces (NATO C2COE, 2020).

Operational Coordination Working Group (OCWG) represents FMN operators and is responsible for gathering, defining, and managing operational requirements. The NATO Command and Control Centre of Excellence (NATO C2COE) focus on information management and human factors and supports FMN capabilities by contributing valuable information that influence to the development of command and control concepts for FMN (NATO C2COE, 2020).

3.2 Development and interoperability

The success of FMN relies on NATO and national affiliates working together in developing and testing defined specifications and their implementations based on existing NATO and commercial standards, for achieving full interoperability. Pullen et al. (2022) evaluated in their study how well different modelling and simulation (M&S) standards can interoperate within a complex, multinational military exercise environment, in Coalition Warrior Interoperability Exploration, Experimentation, Examination and Exercise (CWIX). The development of FMN and its specifications is progressing through overlapping sequences of Spirals (Figure 9), where each stage is divided into four milestones: Draft, Candidate, Proposed, and Final. These "evolutionary cycles" are designed to progressively improve the maturity level of federated mission networking capabilities over time (C3B Interoperability Profiles Capability Team, 2023).

One of the key challenges addressed in the study is ensuring that different M&S systems can effectively communicate and integrate, despite being based on different technical solutions or architectures. Series of tests were conducted during the CWIX event to validate the interoperability and evaluate the performance, data exchange, and integration capabilities of various systems. While significant progress in M&S has been made towards interoperability, there are still gaps and challenges that need to be addressed. Future tests will be evaluated with FMN Coalition Interoperability Assurance and Validation (CIAV) Working Group to

test how current M&S and Service Instructions (SI) are aligning with requirements of FMN implementations. (Pullen et al., 2022)

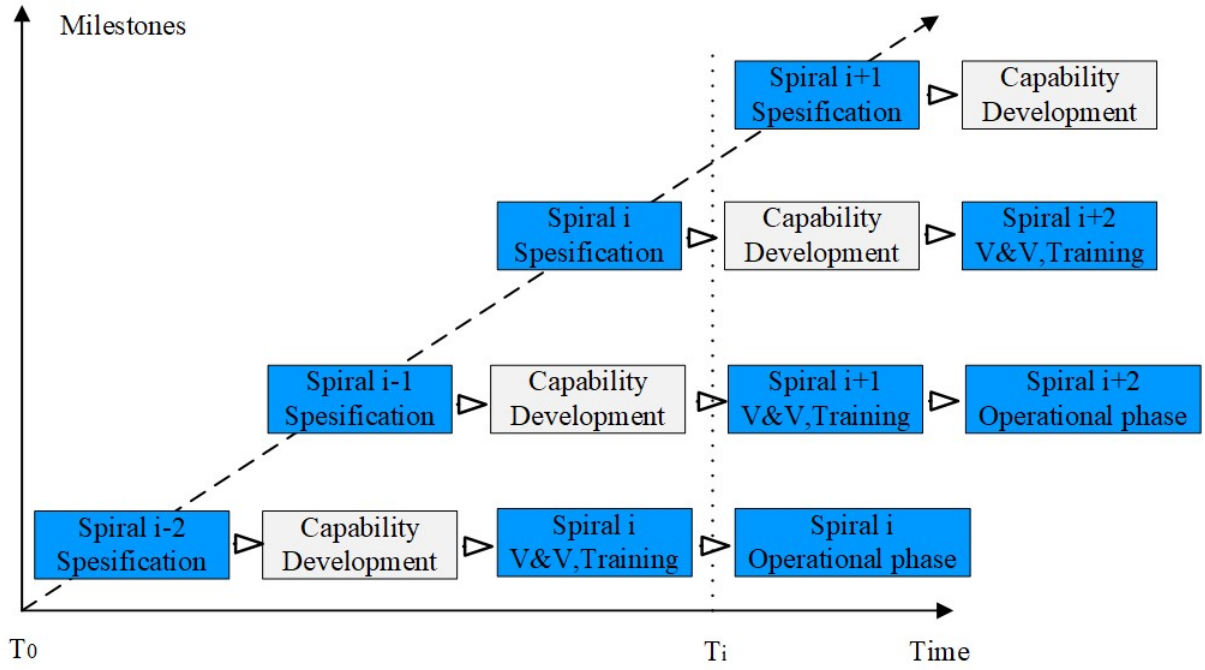

Figure 9. The FMN Spiral Development Process (Pullen et al. 2022)

NATO Interoperability Standards and Profiles (NISP) is a document aiming to ensure technical interoperability between NATO forces and Nations and Communities of Interest (COI) by establishing a set of standards and profiles. These standards are designed to align with both technical and operational requirements, to improve operational efficiency in joint missions and to support defining how systems should interact, exchange data, and work together across different military domains. NISP defines some standards and profiles mandatory, which are required to be used. Candidate standards and profiles are under development and testing, but are expected to be used after a certain time. NATO Consultation, Command and Control Board (C3B) Interoperability Profiles Capability Team (IPCaT) is developing NISP for improving interoperability, and continuously adapting to new technologies, operational requirements, and emerging threats. (C3B Interoperability Profiles Capability Team, 2023).

NISP consist of commercial (non-NATO) and NATO standards, which are managed and developed by their own standardization bodies, and NISP tracks the status of the standards' life cycles. Approved and ratified commercial and NATO standards are included in NISP

database, standards with other statuses are managed in NATO Standardization Document Database (NSDD), hosted by NATO Standardization Organization (NSO). The use of standards is defined in interoperability profiles, which specify how standards are applied at a Service Interoperability Point (SIOP). SIOPs act as a reference for interfaces of the systems and services and as a central point for ensuring service interoperability between connected systems. Profiles enable identifying the key components for implementable combinations including: Capability Requirements, Architectural Views of NAF, protocols, SIOPs, and other interconnections and relationships. (C3B Interoperability Profiles Capability Team, 2023).

The NATO Defence Planning Process (NDPP) is the main tool for identifying required capabilities and ensuring their timely coordinated development and implementation. It focus on operational needs and provides various solutions and products to support development of military architectures and interoperability requirements, based on C3 Taxonomy. NISP is supporting NDPP for creating a more unified approach in developing CIS (Computer Information Systems) capabilities for the Alliance. C3 Taxonomy is model, where capabilities and their relationships are categorized into different elements; and standards and profiles used in NATO are mapped into them. This provides a common language for interoperability and synchronized operation (C3B Interoperability Profiles Capability Team, 2023).

The coordination of profiles and standards between NATO and its member nations is essential for achieving interoperability. NISP defines specific roles and responsibilities for various NATO bodies in different levels, such as the NATO Communications and Information Agency (NCIA), FMN CPWG (Federated Mission Networking Capability Planning Working Group), and different C3B CaP working groups (NATO Consultation, Command and Control Board, Capability Panels) (C3B Interoperability Profiles Capability Team, 2023).

NISP also contains FMN spiral specifications, which consist of four sections: reference architecture, instructions, profiles, and requirements (C3B Interoperability Profiles Capability Team, 2023). FMN Spirals refer to the incremental development stages of the FMN capabilities, which aim to improve information sharing and operational interoperability among NATO, NATO nations and NATO Affiliates. Spirals provide well-defined and agreed objectives in agreed scope and schedule. Each Spiral represents a progressive cycle of updates, improvements, and testing phases of FMN specified standards, technology, and protocols. The spirals ensure that capabilities of FMN are evolving and operational requirements are met and improved, allowing for better collaboration, communication**,** and

mission readiness across the federated networks. Spirals address the importance of backwards compatibility and support for legacy systems, ensuring that newer technologies can integrate with existing infrastructure, providing more options for affiliates. Several spiral specifications are active simultaneously, but since released in stages, each one can be consistently built upon the previous one. (Capability Planning Working Group, 2018)

FMN Spiral Standards Profiles specifications are generic, designed to support national implementations while maintaining essential interoperability with NATO capabilities. The framework is built on a service-oriented approach, with relevant interoperability standards identified according to the NATO C3 Taxonomy. Standards Profiles are a collection of standards designed for a specific purpose and objectives, which can be applied in various operational environments. Interoperability standards of the profiles are divided into four categories: Mandatory, conditional (must in certain circumstances), recommended (excludable with valid reason) and optional. (Capability Planning Working Group, 2018)

Currently FMN spiral 4 is at operational use, spirals are preferred to be operational in 2 years cycles (Figure 10). Johnsen & Hauge (2022) studied policy based routing in mobile networks and how information services can adapt to networks in constrained tactical environment. Earlier spirals primarily focused on defining interoperable services for Operational Communication and Information Systems (OPCIS), but in Spiral 5 also mobile solutions are being defined to support Tactical Communication and Information Systems (TACCIS) domain. Authors study explores how standardization, technical interoperability, and adaptable information systems play crucial roles in ensuring that coalition partners can work together seamlessly, even with different technological infrastructures. They propose policy-driven frameworks and flexible architecture solutions such as CLO (cross-layer optimization) which enables information of network level for application level, and which can adapt to the varying capabilities of different national forces while maintaining robust and secure information exchange (Johnsen & Hauge, 2022).

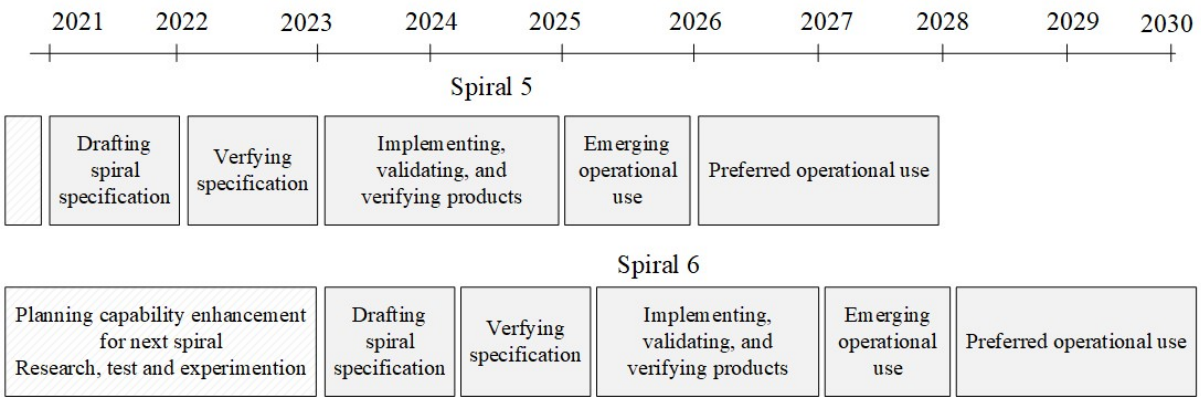

Figure 10. FMN Spirals 5 and 6 (Johnsen & Hauge, 2022)

FMN Milestone 2 (Focusing on information sharing environments in mission network for different levels of security classifications with differentiated physical infrastructures for each mission) and Milestone 3 (Focusing on information sharing environments in all mission networks utilising an unified infrastructure and supporting different levels of security classifications) should be operational in Spiral 5 (2026-2027) and Spiral 7 (2030-2031), so these requirements should be addressed by affiliates. FMN CPWG have projects of using Protected Core Networking (PCN) to respond requirements of Milestones 2 and 3 but also other Data Centric Security solutions and technologies are being considered. Some of these are commercial solutions for classified (CSfC) -solutions, virtualization solutions and mobile, dynamically reconfigurable environments. NATO Industrial Advisory Group (NIAG) acts as a link for communicating NATO objectives to industry and vice versa, which improves FMN awareness and better solutions and products to support FMN capabilities. (NIAG, 2021)

3.3 Structure

One possible implementation to achieve FMN capability is Protected Core Network (PCN) architecture. Boonstra et al. (2012) studied how to create secure architecture for The NATO Network-Enabled Capability (NNEC) program (later integrated into FMN) to share and use differently classified information in PCN environment. The authors first present an architecture that separates infrastructure, information, and security layers (PCN) to enhance flexibility and efficiency of resources, and control over differently classified information. Interconnecting typical standalone networks or System High infrastructures are not cost-effective and communication methods are usually misaligned due information security requirements and the security measures embedded within the each infrastructure is different (Figure 11).

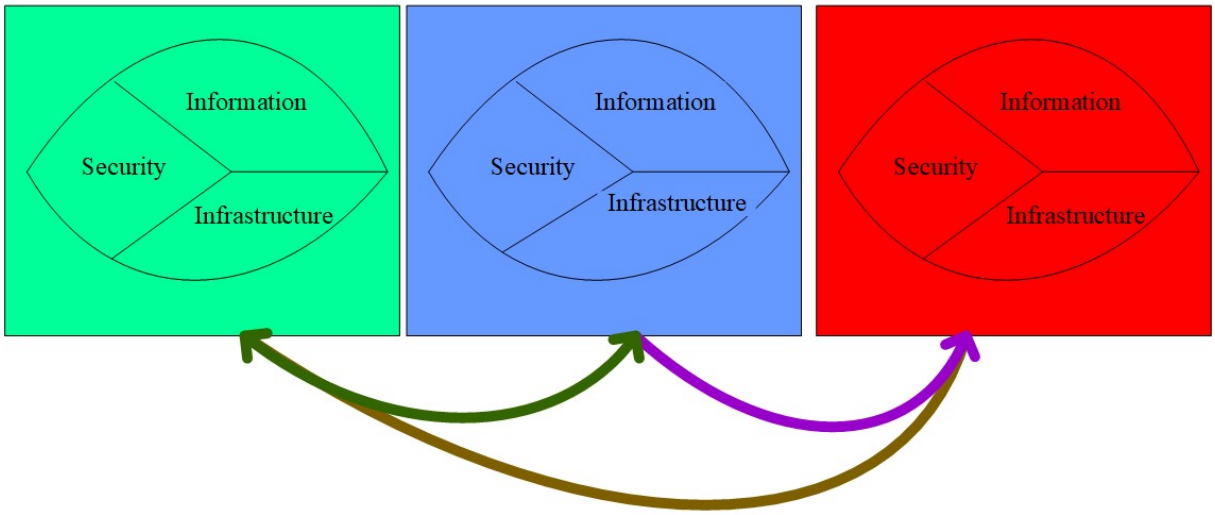

Figure 11. Interconnected System High communication infrastructures (Boonstra et al., 2012)

The need for a unified infrastructure had been recognised as early as 2005 by NATO C3 Agency. To achieve common Networking & Information Infrastructure (NII), NNEC proposed integrating core information systems and networking systems from both NATO and its member nations to establish a Federation-of-Systems (FoS) capability (NNEC FS, 2005). Disentangling information management from the infrastructure (Figure 12) enables interoperated military operations within federated systems. This type of network got name Protected Core Network (PCN) (Boonstra et al., 2012).

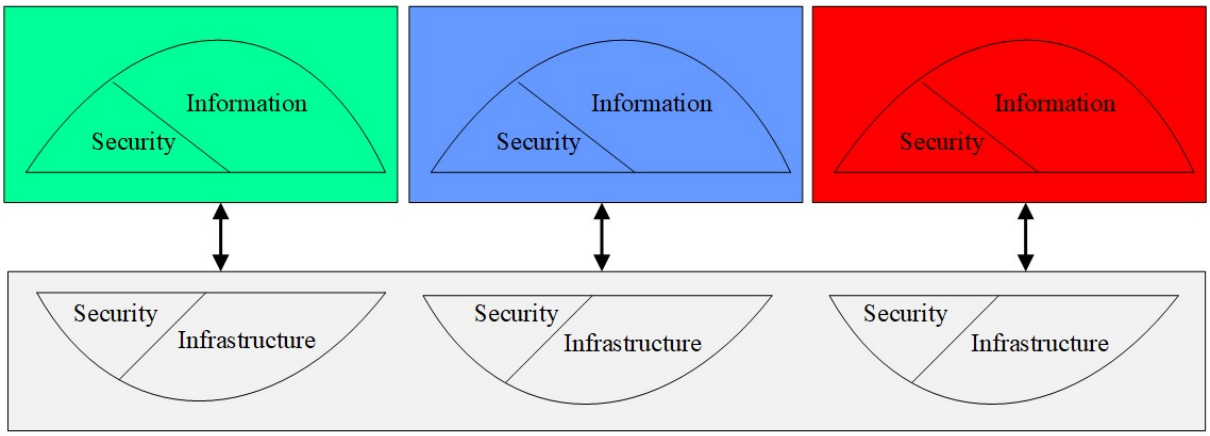

Figure 12. Disentanglement of information and infrastructure (Boonstra et al., 2012)

The main function of PCN is to provide connectivity between the various network nodes and provide only a basic level of protection. PCN is “unclassified” network, meaning it does not

provide confidentiality of any kind but confidentiality measures are executed in each connected network (Figure 13). Protected Core (PCore) is core of unclassified network, which interconnect every participant. Each participant in coalition forms dynamically managed segment in PCN, known as Protected Core Segments (PCS) (Boonstra et al., 2012).

The PCore ensures network availability and provides basic security features. A key aspect of maintaining its availability and resilience is access control, by determining which nodes can connect and under what conditions. This is where the term "protected" comes from. Therefore term “PCN” also describes the interface between different Core Segments and between Core Segments and PCore users (Boonstra et al., 2012).

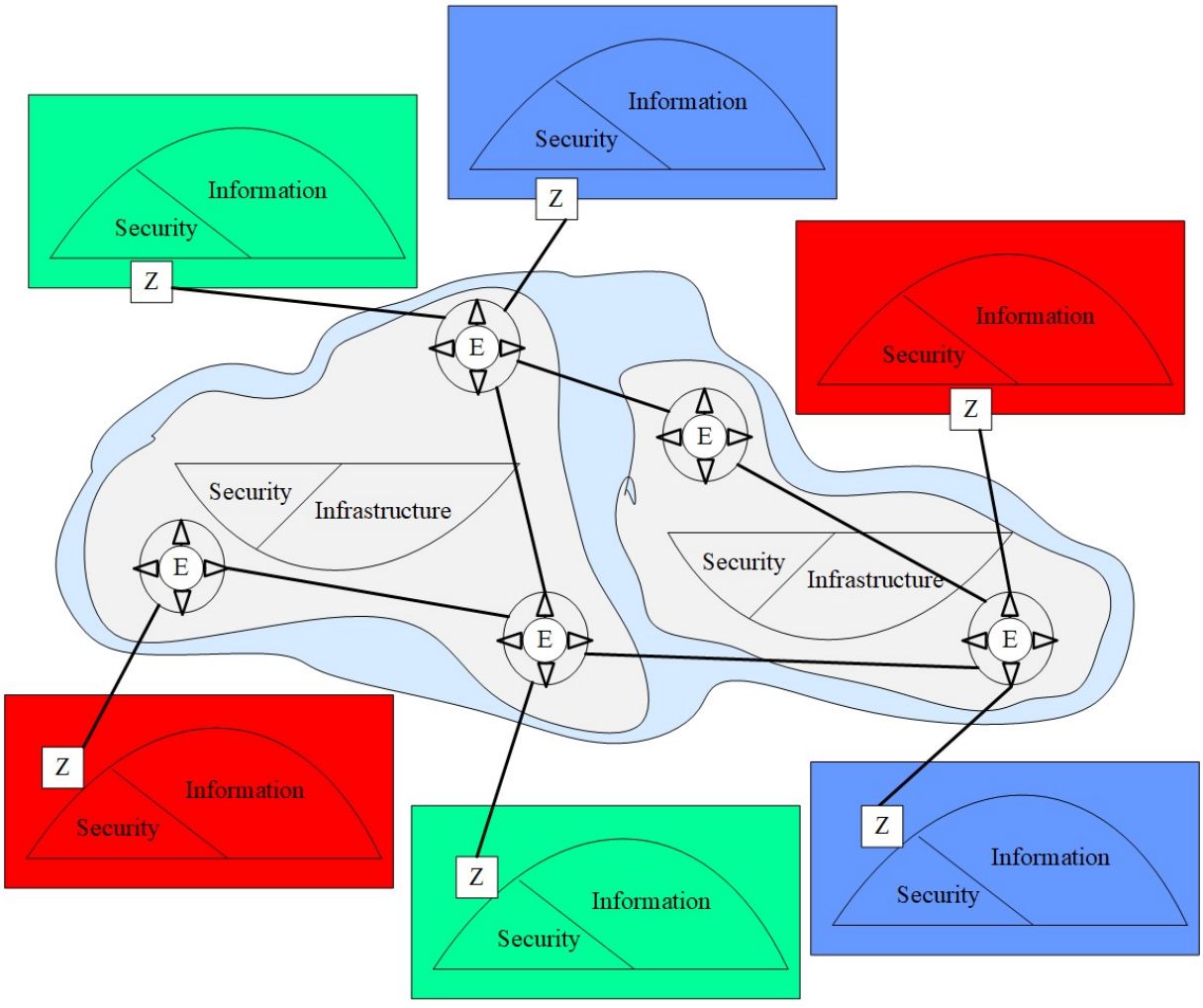

Figure 13. Protected Core connected to clouds (networks) of different security classifications (Boonstra et al., 2012)

Schutz (2010) studied the PCN concept and its challenges, and how it could work in NATO context. Information should be exchanged between NATO and static HQ's of the nations,

between static HQ's and deployed HQ's of the nation and between HQ's and lower management steps and deployed operational bases (DOB). Due the number of networking layers, the corresponding service level policies are needed. Cross-layer capacity management enables the bearer network to communicate any changes in available capacity, Cross-layer resource management ensures that "coloured clouds" (CCs, network connected to PCN) can dynamically request guaranteed resources for sessions and Service level management focuses on maintaining a consistent allocation of network resources aligned with the mission's objectives.

Author also highlights challenges in implementing PCN solution: Integrating PCN into existing network infrastructures can be very complex, requiring significant modifications to current architectures and protocols. As networks grow, scaling and maintaining a protected core that effectively secures all data transmissions becomes increasingly challenging. Balancing security and performance is essential to PCN since additional security measures and monitoring tools can increase latency, potentially affecting the overall performance of the network. PCN also does not resolve all interoperability challenges, mostly at technological architecture level from EA aspect (Schutz, 2010).

Eie (2016) studied authentication schemes in Protected Core Networking, addressing the challenges of enhancing information sharing among national and coalition partners while maintaining security. Author introduces two protocols that enable CCs to dynamically push packets with service policies into the network using identity-based signatures. The signatures are encapsulated and carried by Kerberos symmetric key and Kerberos PKINIT (Public Key Cryptography for Initial Authentication), which are verified in the symbolic model using scyther-proof tool. Experiment validates that both CCs and PCSs gain increased performance with the agreed attributes, leading to more reliable and predictable service delivery.

4 Achieving capabilities in FMN using EA approach

4.1 Previous systemic and EA related studies in the military context in Finland

Systemic or EA related development approaches in military in Finland are not a new thing. Anteroinen (2013) explored the systemic approaches to improve military capability development. The research focuses on integrating concept development and experimentation (CD&E), as well as national defence materiel collaboration. Two holistic capability models were examined, Comprehensive Capability Meta-Model (CCMM) and Holistic Capability Life Cycle Model (HCLCM) for better understanding of military capabilities. Study also introduced a systemic approach to improve the collaboration between defence forces, industry and academia, enhancing efficiency in capability planning, development, and procurement.

Maltusch (2020) explored how EA can be used to aid strategic planning and operational development at the National Defence University (Maanpuolustuskorkeakoulu) in Finland. The focus is on utilizing EA to visually model and monitor the implementation of the institution's 2020-2025 strategy, helping streamline operations and ensure alignment with organizational goals. EA could improve strategic decision-making and supports continuous monitoring of key objectives and their interrelationships, and enhances ability to manage strategy execution, aligning technological resources with operational needs. This however, is challenging if usefulness of EA and its role to support the whole organisation is not understood.

Blomvall & Hirvi (2024) studied the challenges faced by military headquarters in modern warfare, where increased complexity and rapid technological advancements can hinder decision-making agility and reduce survivability through excessive centralization. They propose Dynamic Headquarters Structure (DHS) instead of adhering to classical static and generic headquarter structure. This approach involves tailoring structures dynamically based on the specific situation and context. By adjusting networking, information flows and delegation of decision-making, DHS enables military headquarters to operate more effectively across diverse environments.

Ikonen & Pitkäkoski (2025) examined different project management methods, tools, and techniques and how they are employed in Finnish defence projects. Findings from the survey revealed the most used project management practices, which were project meeting, project review, workshop, expert screening, negotiation, course of action comparison, brainstorming,

project audit and checklist (Table 3). Benefits of these practices were defined and how they can affect defence projects.

Table 3. Methods and techniques used in defence projects (n=53) (Ikonen & Pitkäkoski, 2025)

Method/technique	Used often n/ %	Not used n / %
Project meeting	52 / 98,11 %	1 / 1,89 %
Project review	44 / 83,02 %	9 / 16,98 %
Workshop	42 / 79,25 %	11 / 20,75 %
Expert screening	39 / 73,58 %	14 / 26,42 %
Negotiation	39 / 73,58 %	14 / 26,42 %
Course of action comparison	34 / 64,15 %	19 / 35,85 %
Brainstorming	33 / 62,26 %	20 / 37,74 %
Project audit	32 / 60,38 %	21 / 39,62 %
Checklist	30 / 56,60 %	23 / 43,40 %
Group discussions	26 / 49,06 %	27 / 50,94 %
SWOT-analysis	26 / 49,06 %	27 / 50,94 %
Prototype	24 / 45,28 %	29 / 54,72 %
Work breakdown structure	23 / 43,40 %	30 /56,60 %
Bencmarking	22 / 41,51 %	31 / 58,49 %
Document analysis	17 / 32,08 %	36 / 67,92 %
Cost benefit analysis	13 / 24,53 %	40 / 75,47 %
Gantt-chart	12 / 22,64 %	41 / 77,36 %
Interviews	11 / 20,75 %	42 / 79,25 %
Bottom-up estimate	9 / 16,98 %	44 / 83,02 %
Critical path method	8 / 15,09 %	45 / 84,91 %
Survey	8 / 15,09 %	45 / 84,91 %
Analytic hierarchy process	7 / 13,21 %	46 /86,79 %
Context diagram	4 / 7,55 %	49 / 92,45 %
Network diagram	3 / 5,66 %	50 / 94,34 %
Trends analysis	2 / 3,77 %	51 / 96,23 %

The study however does not examine success rate of the projects, therefore quality of these practices cannot be evaluated. Study also does not examine or study project management practices of the least used practices revealed by source material, which may be critical to the success of the project. Trend analysis, network diagram and context diagram are all data driven tools, which emphasize information use in decision making and identifying dependencies, and are also related to EA practices (network diagram in technology and high-level solution architecture and context diagram in business and data architecture). Niemi

(2024) defined that one of the benefits of EA practices is improved project management when enterprise architecture descriptions can be used as source material and can be mapped into high-level solution architectures, used in projects.

Information is the best product that EA provides, when it is relevant and defined clearly. Finnish Ministry of Defence (Puolustusministeriö) (2021) published information concept: Towards Information Superiority, which provides guidelines for developing information work within the defence administration. It emphasizes the strategic importance of information in defence planning, decision-making, and operational activities, and present principles that support achieving information superiority, such as ensuring the availability, enrichment, quality, security, interaction and interoperability of information. It also addresses information lifecycle management and the utilization of information at various domains like development, competence, leadership, information management, research and technology.

4.2 Features and problems of EA approaches in military context

There are several methods or frameworks to manage capabilities and interoperability in military context. Joint Capabilities Integration and Development System (JCIDS) (Defined in chapter 2.2.5) is process for capability management (supported by DoDaF) to manage capability requirements and solutions. It's a tool for Joint Requirements Oversight Council (JROC) to make military capability assessments, ensuring alignment with strategic defence objectives. JDICS provides documents for Sponsors, which refine capability requirements into solution requirements. Documentation also enables traceability to lifecycle of capability requirement process. (JCIDS Manual, 2021)

JDICS uses DOTMLPF-P analysis or framework to identify and evaluate capabilities and gaps from certain point of views. DOTMLPF-P is a acronym of Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities and Policy. These characteristics should be considered in every material and non-material capability solutions and their changes. Changes are evaluated from two perspectives: what is needed for integrating and what are enabling implementation and use (JCIDS Manual, 2021). Older version of the acronym was DOTMLPF (without policy) and in NATO context, interoperability is added to acronym (DOTMLPFI), which both emphasize the need for common ways of operating. JCIDS process is very bureaucratic and contains lot of assessment, validation and approval steps within multiple groups, which makes it very slow to use. JCIDS manual is hard to read and heavy to use, and is not usable as it own. It defines

how everything should be assessed and governed but does not include methods or guides how to manage development, therefore it answer to questions what and why, but not how.

Yue & Henshaw (2009) studied UK's capability planning processes and its complexity with multiple groups and organisations (Figure 14). AWG stands for Availability Working Group, CMG is Capability Management Group, CPG is Capability Planning Group, DEC is Directorate of Equipment Capability, DE&S is Defence Equipment and Support, IPT is Integrated Project Team, JCB is Joint Capabilities Board, S&T is Science and Technology Community and TLB is Top Level Budget Holder. They proposed a capability planning-centic approach for capability planning and development to manage the complexity (Figure 15).

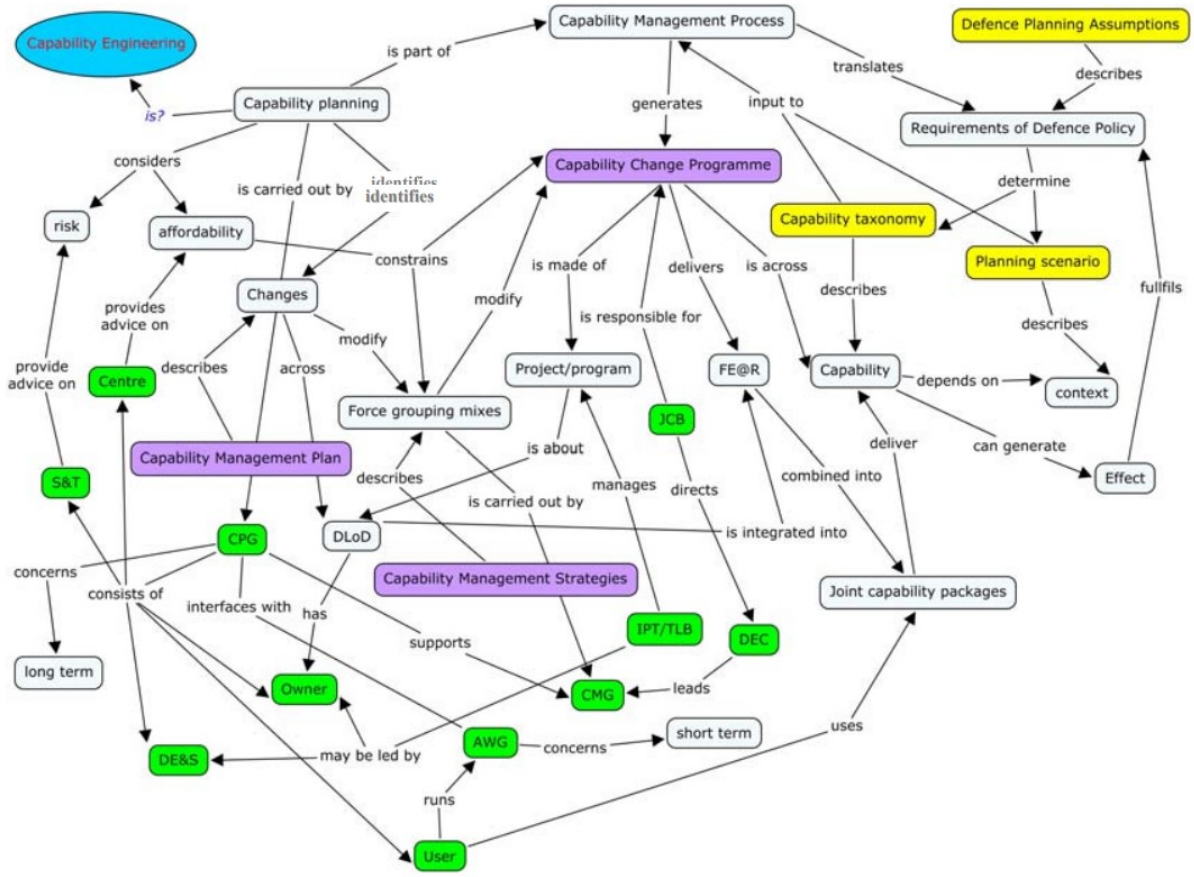

Figure 14. A capability management concept map (Yue & Henshaw, 2009). Licensed under CC-BY-NC-ND 2.5

Kerr et al. (2006) studied capability development in UK to form a common consensus of military capability and proposed a capability framework that views capabilities from different approaches in different layers: Building blocks, Functional Packages, Effects and Influencers. Building blocks are based on lines of development that forms acronym TEPID-OIL which

means: Training, Equipment, Personnel, Infrastructure, Doctrine and concepts, Organization, Information and Logistics. These blocks forms the core of the framework and other layers are built around it. The model presented in this thesis is based on a similar idea of simplified capability elements but approaches the whole in different way.

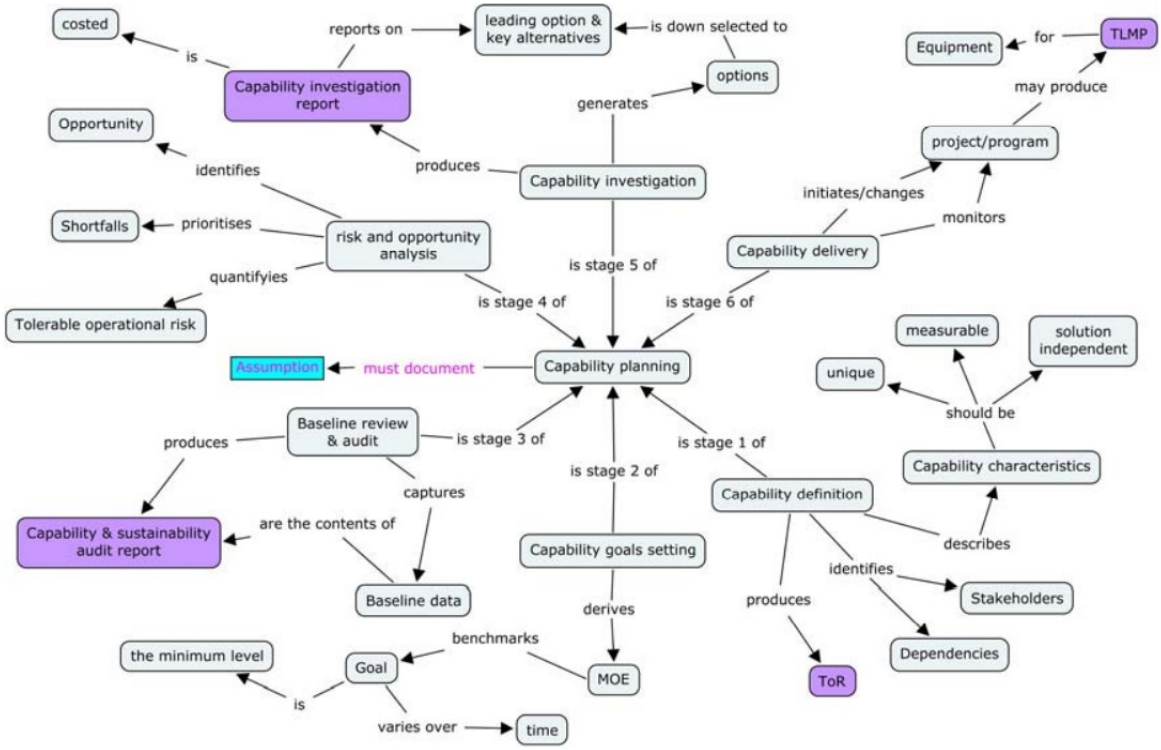

Figure 15. A concept map for the 6-stage capability planning process (Yue & Henshaw, 2009). Licensed under CC-BY-NC-ND 2.5

There is no common approach to develop capabilities, and different nations and organisations have their own needs and strategies in different levels, which may differ a lot. Armed forces and their procurement are controlled by individual member states in NATO and EU, therefore shared capability development is inherently limited. NATO's NDPP and EU's Capability Development Plan (CDP) offers guidance on capability priorities ensuring commitment on shared goals but not directly develop military capabilities (Figure 16). They assist member states in identifying capability gaps and enhancing their defence capabilities (Drent et al., 2017).

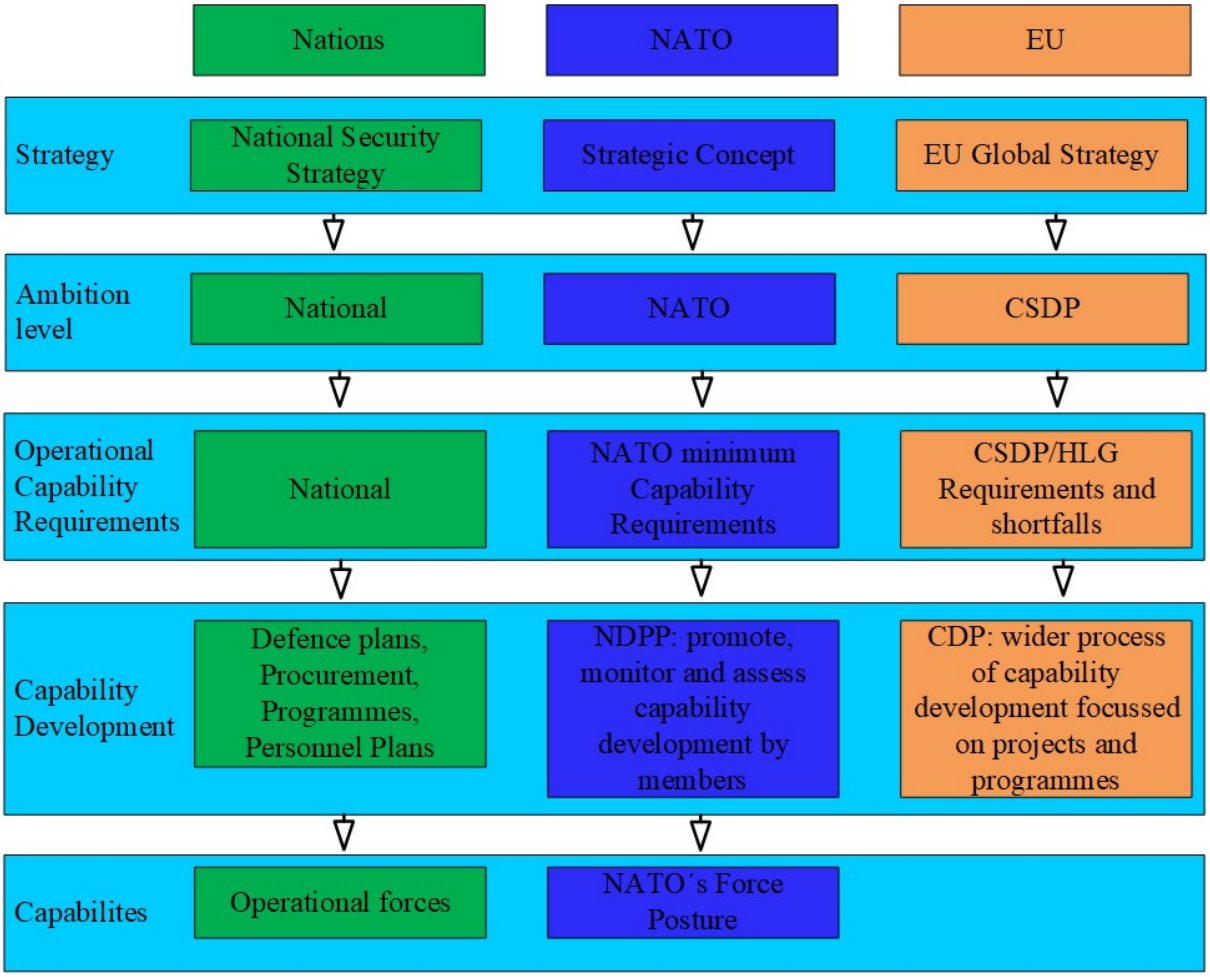

Figure 16. From strategy to capability development (Drent et al., 2017)

In military context, capability is often presented as the ability or readiness ("suorituskyky") to perform or affect something. It can be achieved with material solution (like weapon system) or non-material solution (like way of fighting or process). This however differs from definition in EA, where capabilities can be seen as defined activities ("kyvykkyys") done by the organization that connects strategy to the business and IT objectives of an organization (Kotusev & Alwadain, 2024; Niemi, 2024). There can be different level or differently classified capabilities, but the number should be reasonable for controlling the wholeness of EA (Niemi, 2024). Each capability is a fragment of an organization's business and operations, and their characteristics define the whole (Hosiaisluoma, 2022). The amount of capabilities in NATO is estimated to be over 400 (Gebhard & Crosby, 2010), so using EA approach with its capability definition is unfeasible, unless capability is defined by mutual agreement. Frameworks designed to military field also often focus on stakeholder needs at the expense of capabilities, which may challenge EA work.

Other problems are typical challenges with EA practices in public organizations (Defined in chapter 2.5). It is difficult to get a professional enterprise architect in a military organisation, because the need for EA is not usually recognized and, for example, Finnish special officers (Erikoisupseeri) in the technical field are required to have an engineering degree (Valtioneuvoston asetus puolustusvoimista 2007/1319 luku 2 § 11). Engineering degrees usually do not include EA studies, as they belong to information systems sciences. EA frameworks and practices can be hard to use, and requires skills and experience to implement in organisation. Few public organizations, even fewer military organizations, have enough architects, even fewer with EA-related titles. Choosing the right framework for the need, having best practices from multiple frameworks and successfully implementing and governing EA practices needs an experienced EA professional.

4.3 Developing EA application to develop capabilities in military context

Since DOTMLPF-P/I must be considered in all capabilities and solutions (JCIDS Manual, 2021), the domains of DOTMLPF-P/I can be thought as the capabilities of a military organization. This thesis presents a capability development model based on DOTMLPF-P/I perspectives, which should be usable in a defence organization. The deployment should be as easy and clear as possible, because implementing enterprise architecture practices can be challenging and defence organizations rarely have EA experts or department to do the job. Capability models provide organized and hierarchical representations of business capabilities, where essential resources can be identified to achieve organisational objectives (Kotusev & Alwadain, 2024).

Niemi (2024) presented an agile and light capability modelling approach in his book, that contains capability map (or canvas), business architecture consisting of business environment and process map, data/information architecture, information system architecture consisting of IS map and data flows, and technology architecture, which all can be used for EA practices and to bind enterprise architecture to high-level solution architectures. The model made in this thesis follows these steps to achieve streamlined and clear capability model for military organisation. This model is using ArchiMate modelling language, which is developed and maintained by The Open group and it's also aligning with TOGAF. It's a tool for EA practices and provides a structured way to visualize, describe, and analyze enterprise architectures from

different perspectives using clear notations. It helps controlling the interrelationships between EA elements and enables their ongoing management.

Niemi (2024) and Kotusev & Alwadain (2024) both emphasize that the capability map should be made with the organization's management to take everything into consideration, but this model includes the most important capabilities according to the author's own assessment. Also note the author is not highly militarily educated. The capability map should also be based on reality, but this model only has sought to identify the most important DOTMLPF-P related features of the possible capabilities of the military organization. According to Niemi (2024) the capabilities should also be of the same roughness category, but for example, in the presented organizational capabilities, the land, air and naval capabilities can be different level related to other capabilities (Figure 17). Capabilities consist of elements that produce them and their dependencies are be mapped into EA tool (Figure 18).

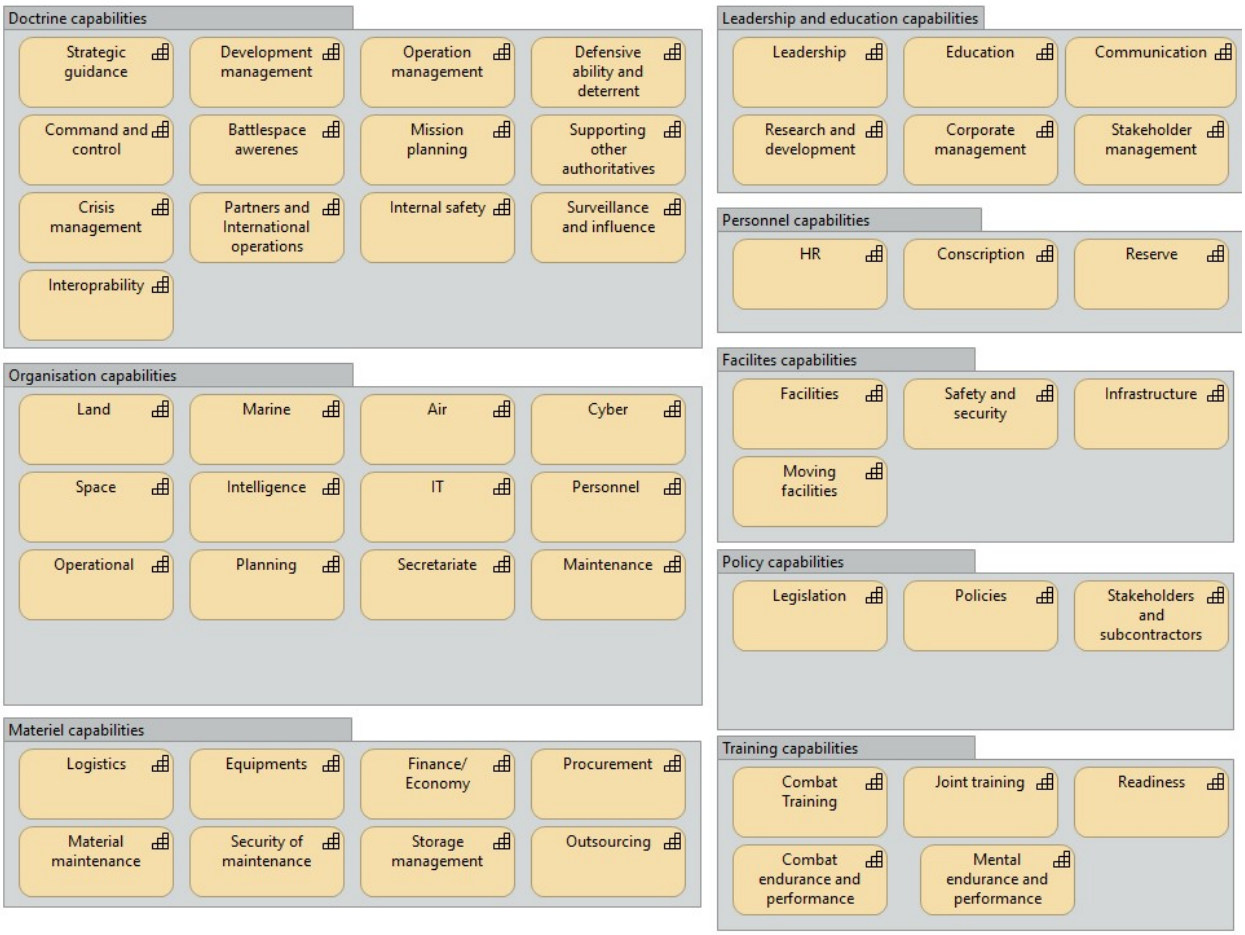

Figure 17. Capability map

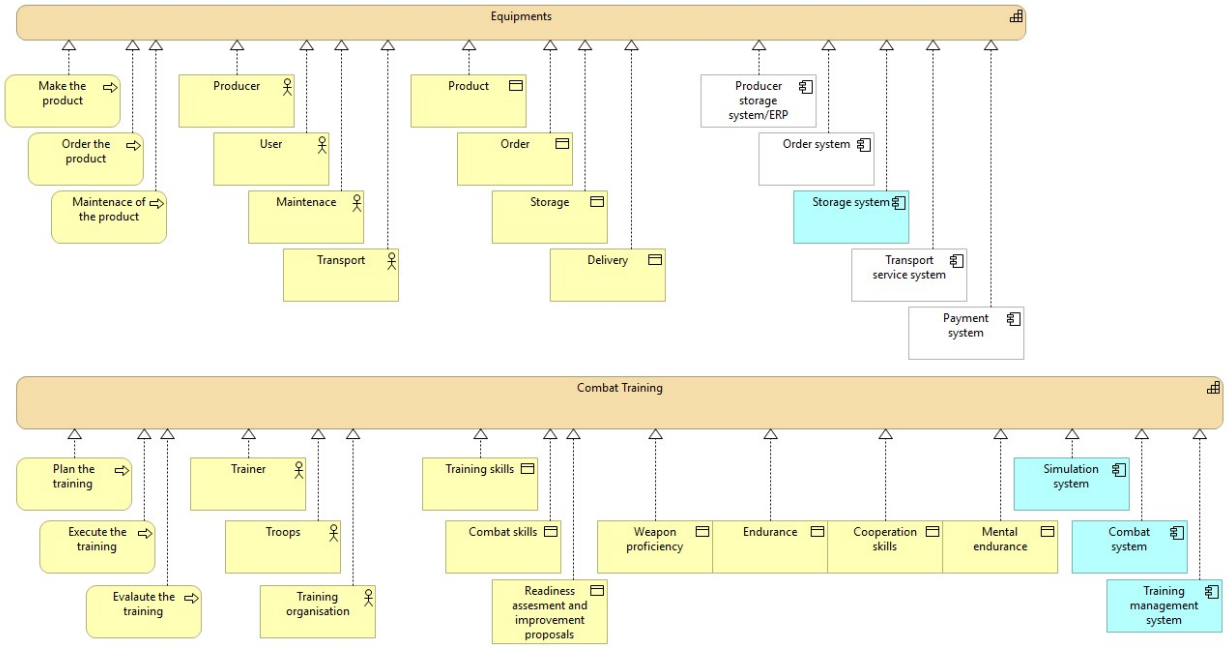

Figure 18. Example of capability elements and dependencies in EA tool

In business architecture the business environment (Figure 19) and processes (Figure 20) should be modeled for identifying dependencies between organizations and internal dependencies in business actions (Niemi, 2024). Only the most important actors and functions in terms of core operations should be included in the models to avoid excessive details for maintaining the usability.

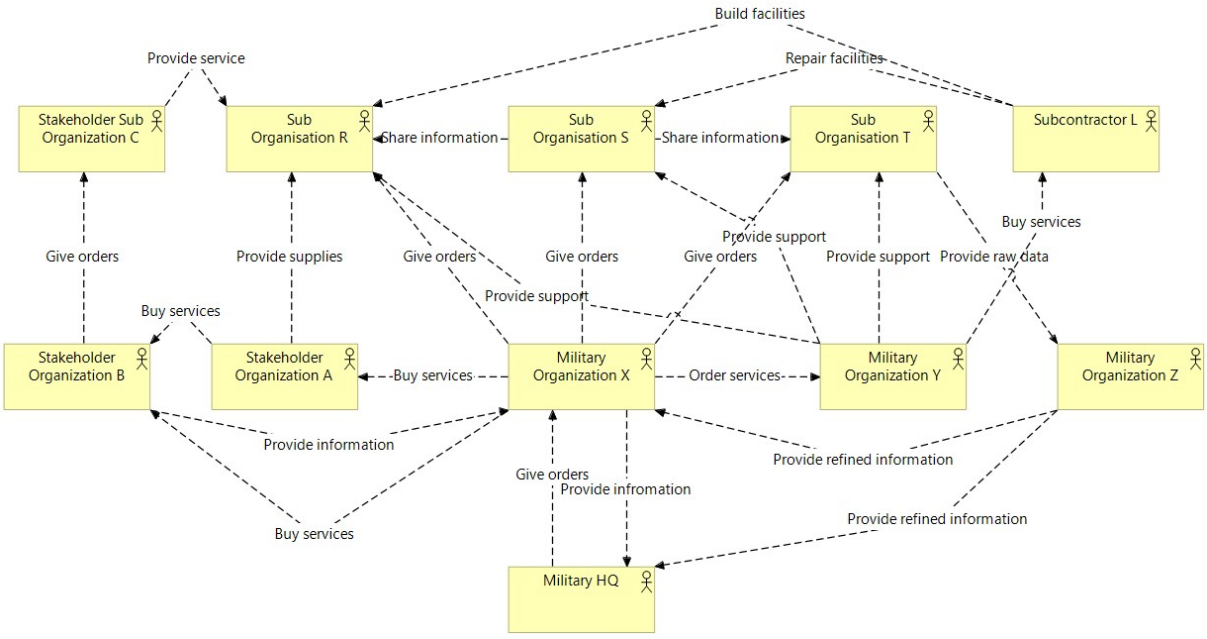

Figure 19. Business activity environment

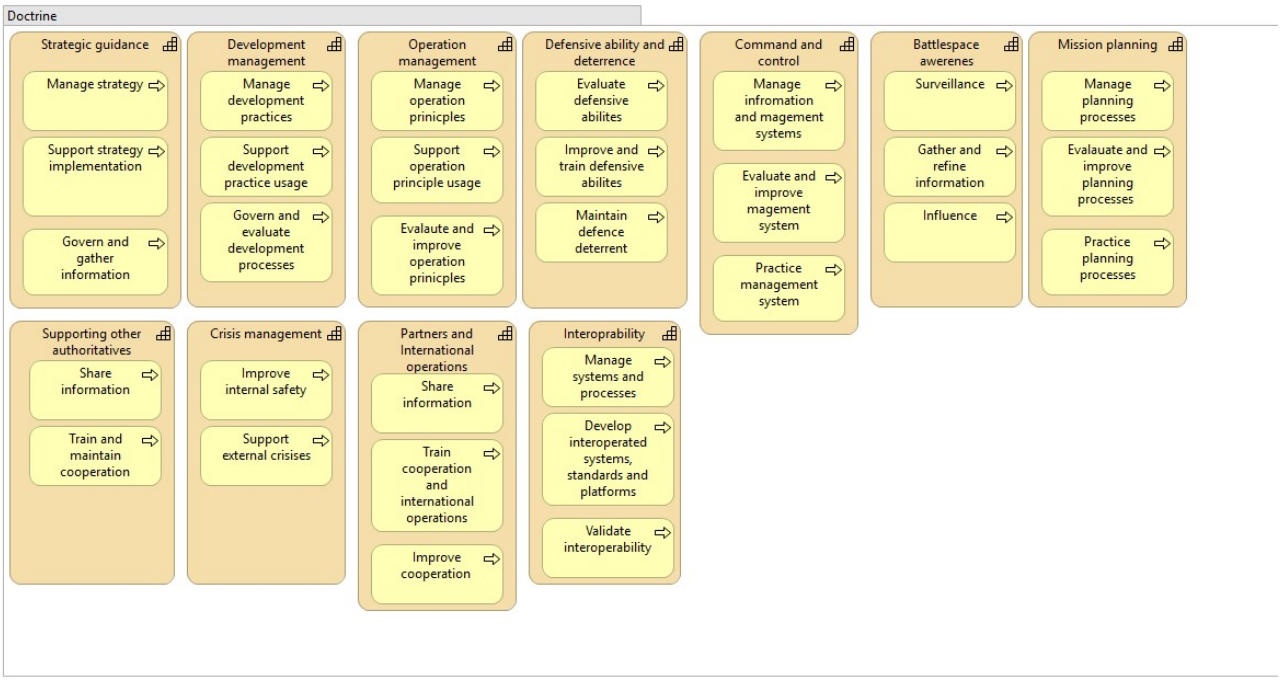

Figure 20. Example of business processes of capabilities

Data architecture level aims to model data sets used in organization and to identify how they are linked to business actors and information systems (Figure 21). This model can be enriched and clarified with attributes, but the number of elements (10-50) should be the low enough to preserve the whole (Niemi, 2024). Information system architecture consists of information system map (Figure 22) and information system data flows (Figure 23). Information system map describes used internal and external information systems and information system data flows dependencies between them (Niemi, 2024). Technology architecture describes and models used technologies (Figure 24) and should be used, when technical landscape is really wide. Also in technology architecture the level of description should be evaluated to avoid going too deep in details, which would hinder the management of the model and EA.

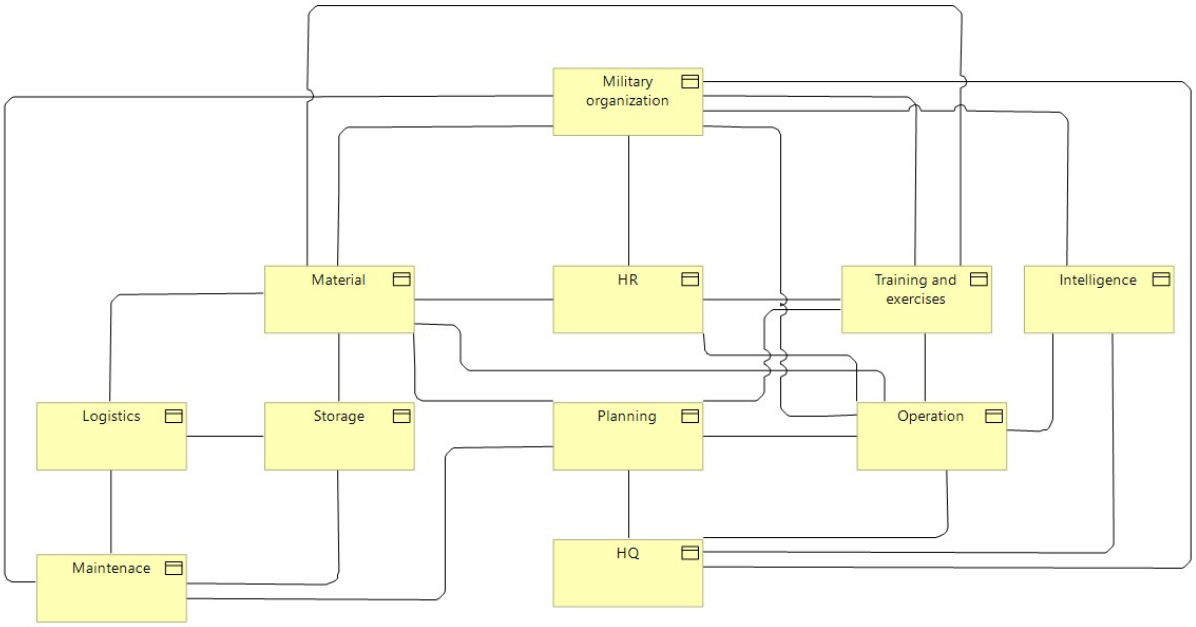

Figure 21. Data architecture

Figure 22. Information system map

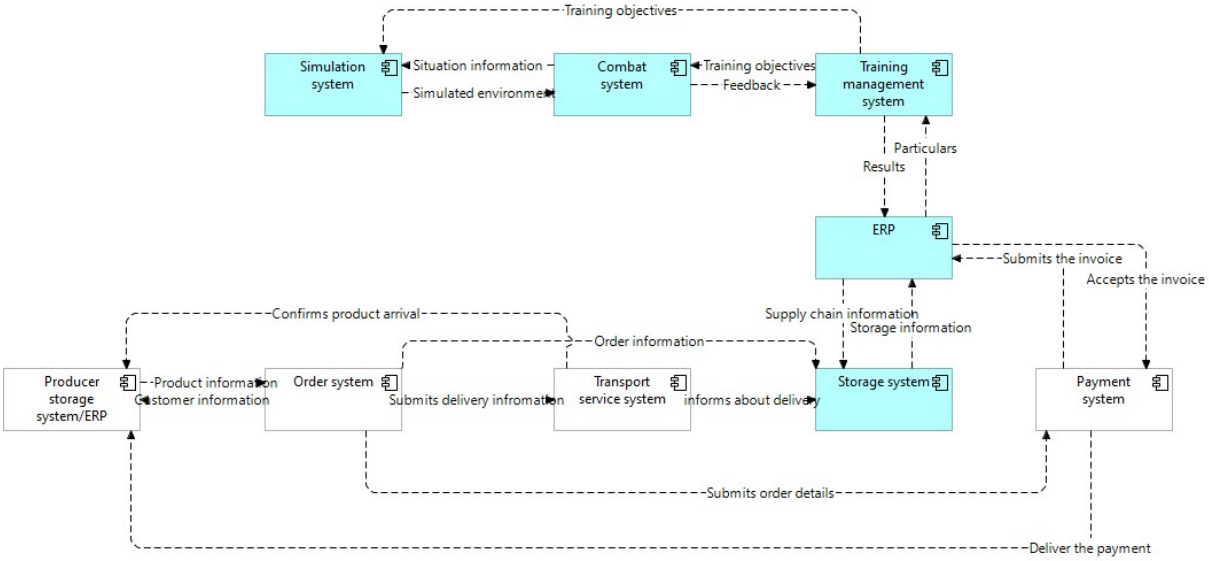

Figure 23. Information system data flows

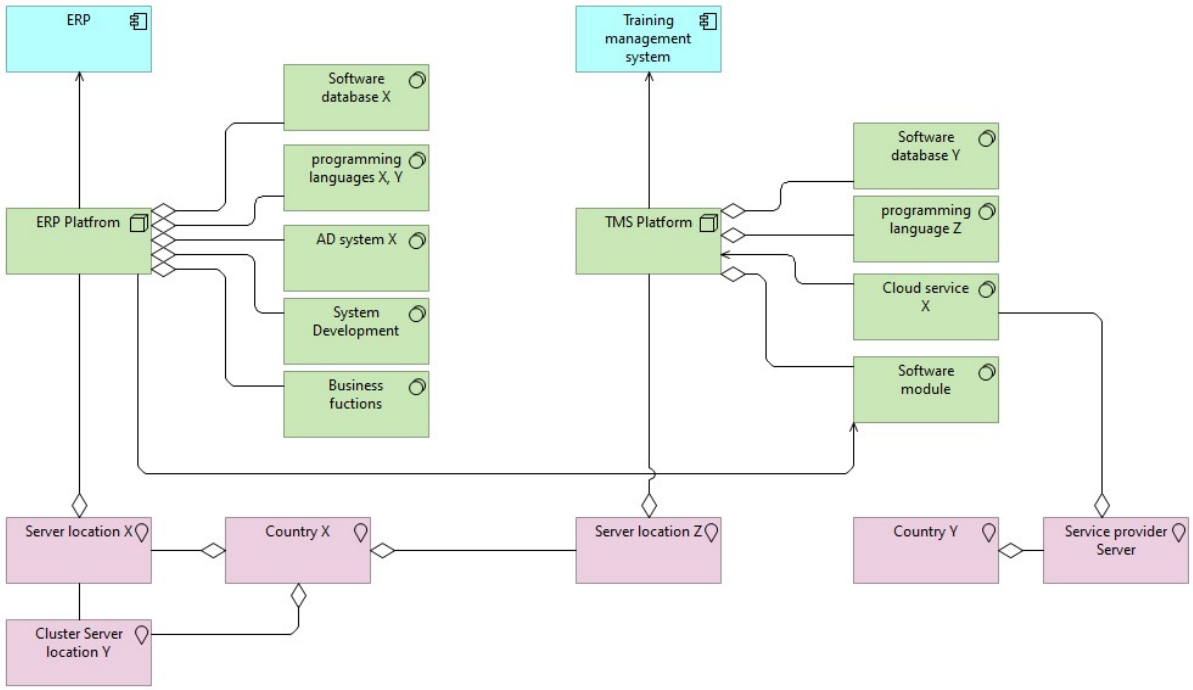

Figure 24. Example of technology architecture

Presented capability development model and descriptions above provide a clear, high-level view of what an organization can do, helping in aligning business goals and IT, improve strategic planning, identify gaps or overlaps, develop capabilities and to guide organizational transformation. To improve the usage of the model, it is recommended to test and validate how it fits for the organization before wider implementation (Niemi, 2024). Depending on the size of defence organisation, there can be lesser or more identified capabilities.

To evaluate the model, the organization must first evaluate its enterprise architectural maturity level, for example according to some maturity model like CMMI. CMMI (Capability Maturity Model Integration) is a widely recognized framework used to assess and improve an organization's processes, performance, and capabilities (CMMI Institute, 2025). It uses Six-level maturity scale:

- Level 0: Incomplete, functions and processes are unknown and unmanaged
- Level 1: Initial, functions are unpredictable and processes reactive, success depends on individuals.
- Level 2: Managed, functions and processes are defined at a project level but not standardized across the organization.
- Level 3: Defined, functions and processes are standardized and documented for organization-wide use.
- Level 4: Quantitatively managed, performance is measured, monitored, and managed based on data.
- Level 5: Optimizing, continuous improvement with innovations and efficiency.

Main problems with maturity models is their very static and obsolescing nature in rapidly evolving technology environment, and they usually only consider the current state of maturity, therefore iterative cycles of evaluations must be made to govern and manage the change.

The purpose of this model is to facilitate the identification and management of capabilities and their relationships. A major challenge is ensuring that only elements and relationships directly relevant to requirements and objectives are included in EA models, but simpler model structure and multiple iteration cycles can provide better results. This also mitigates ambiguities and misunderstandings, since different programs, organisations or nations might interpret and apply complex frameworks differently; causing divergence and incompliance that makes multinational collaboration harder.

With current approaches and used frameworks in FMN context, the minimum viable architectures are created, rather than full comprehensive models. This approach can pose risks

to interoperability and cause inconsistency, incomplete views, and difficulties in leveraging models and integrating systems at coalition or program levels later on.

5 Improving security in FMN using EA approach

5.1 Security in complex systems

Increasing number of interacting systems and complexity is also challenge for cyber security. Implementing single security mechanisms in complex systems can be demanding and does not necessarily take all needs into account, therefore also security must be considered holistically. Many frameworks and analysis tools are designed for organisations and their systems, and may not be suitable for complex systems of systems. Boxer & Miller (2009) made the same observation that improved approaches are needed for more complex system of systems and Span et al. (2018) addressed the critical need for structured approaches to enhance cyber security in complex cyber-physical systems.

Theron et al. (2018) presented the concept and architecture of an Autonomous Intelligent Cyber-defence Agent (AICA)**,** aiming to enhance cyber defence capabilities in military systems. It is based on intelligent software agents that are autonomously observing military network and responding to anomalies faster and more effectively without human intervention. Reference Architecture for AICA (AICARA), developed by NATO's IST-152 Research and Technology Group, provides a structured framework for implementing AICA, outlining functions, components and interactions necessary for agents to operate effectively within complex and interconnected military systems.

Velazquez et al. (2023) studied automated and machine based cyber defence mechanisms that are essential in large military networks (software-defined networking (SDN) in PCN context) to protect critical information systems against cyber threats, operational disruptions and system failures. In complex and large systems, agent-type solutions are needed in rapid and constantly changing environments where they can execute security mechanisms independently. ACD (Autonomous cyber defence) is also agent based solution (Figure 25) ACD have two different types of agents: ACD-Core and ACD-CC, which can analyze network patterns and implement security measures across different layers of OSI-model. ACD-Core agents synchronize network wide state-information in PCN core-network and communicate it for each ACD-CC agent. ACD-CC agents within the coloured clouds functions independently and exchange information if necessary.

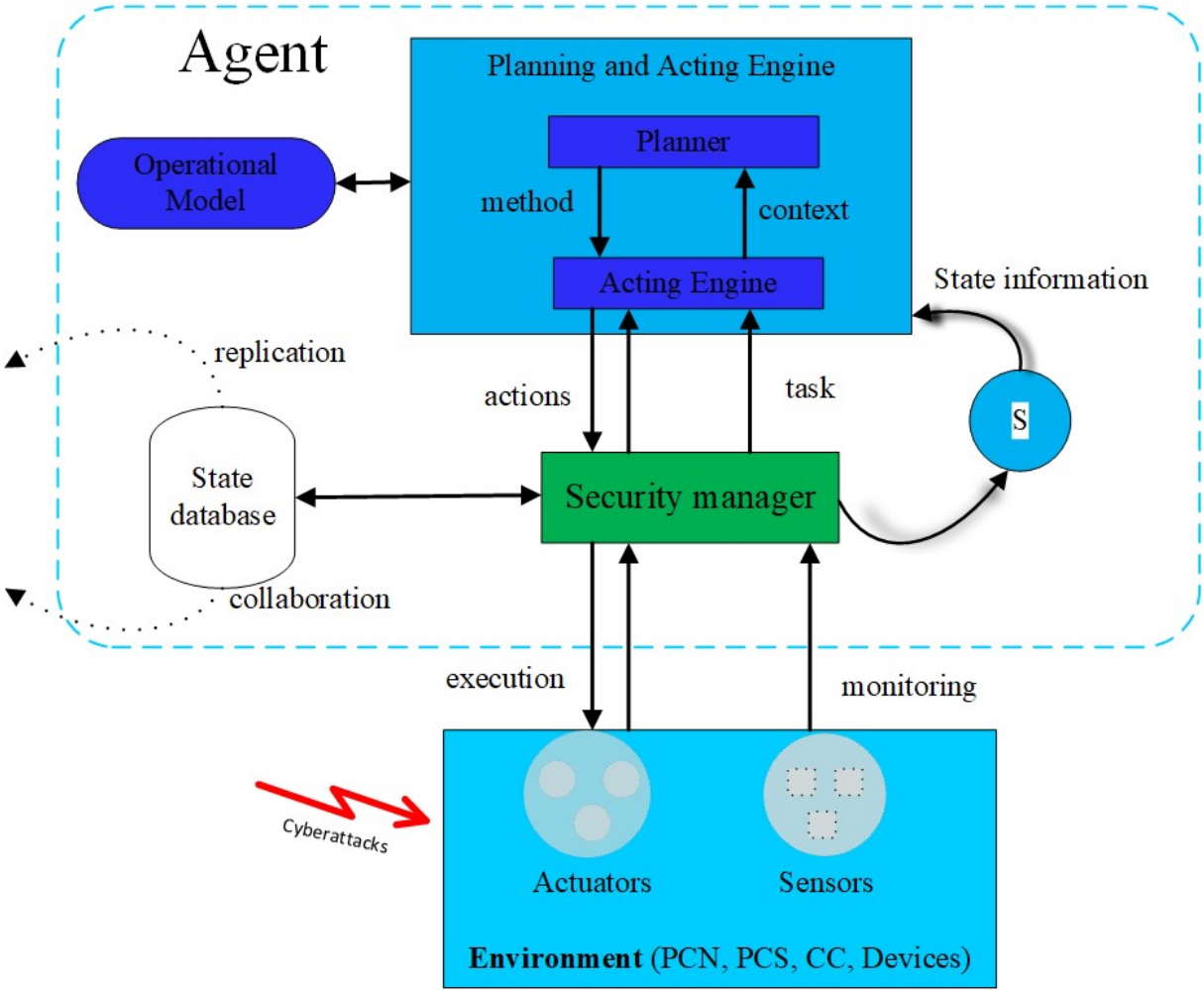

Figure 25. Autonomous agent architecture (Velazquez et al., 2023)

Two different agents are needed to respond for the different needs of static networks near HQs and dynamic and unreliable networks in the tactical edge, where centralized management and monitoring is challenging or unfeasible. This architecture enables connection between enterprise and tactical networks within the PCN (Figure 26) while ensuring continuous cyber defence, even when CCs become isolated from PCN core network (Velazquez et al., 2023).

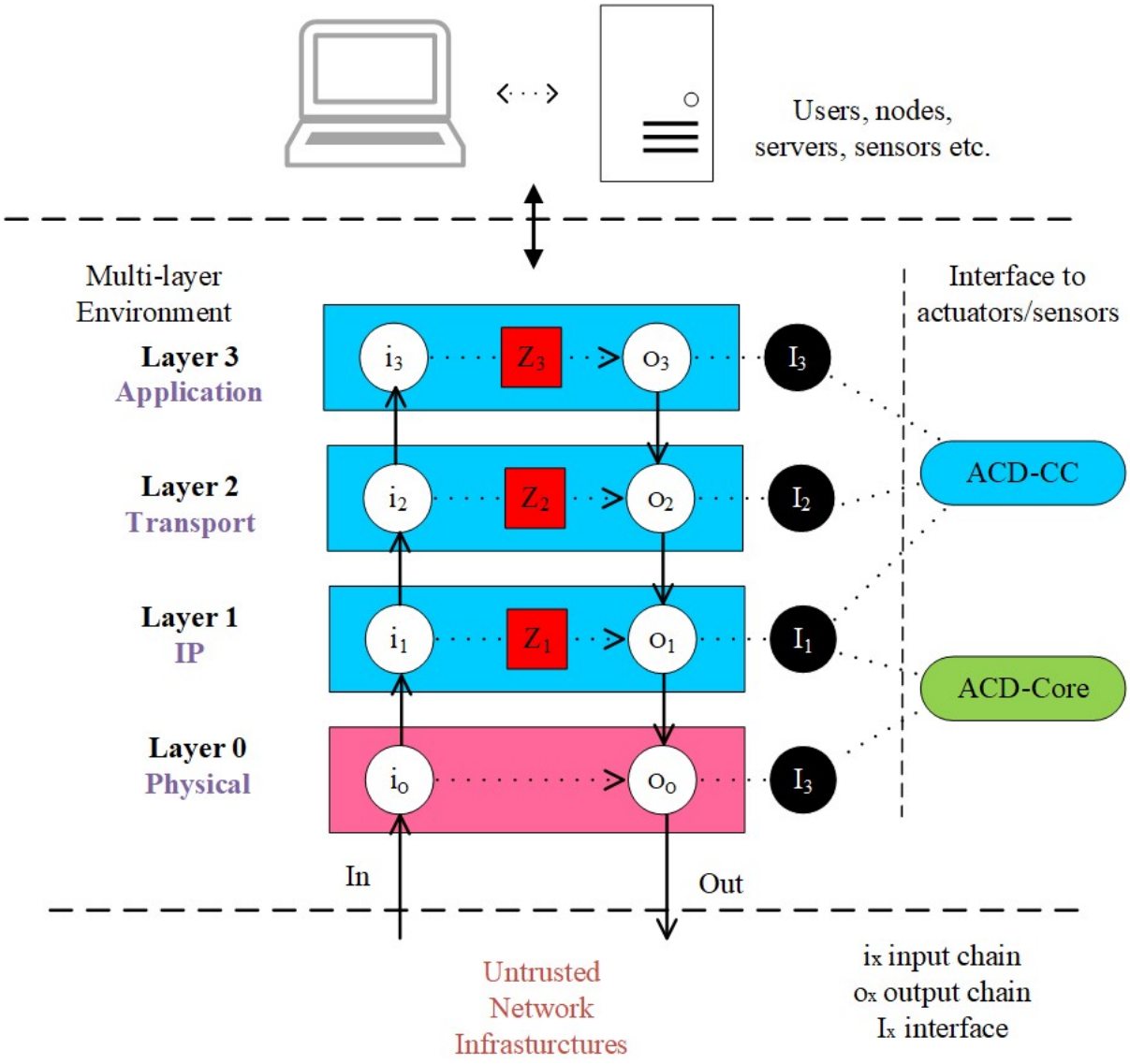

Figure 26. Environment for two different agents (Velazquez et al., 2023)

One challenge in military networks is different information security levels, which requires controlled access, data protection, and interoperability between security zones. It makes networks more complex due increasing numbers of interfaces and cryptographic systems and devices. Boonstra et al. (2012) propose a MILS concept (Multiple Independent Levels of Security) which provides one physical system containing multiple virtualized layers for differently classified security compartments. Required level of security cannot be achieved with typical virtualization solutions, therefore the combination of hypervisor and separation kernel is needed to separate physical resources of the differently classified information systems.

5.2 Using developed EA approach to improve cyber security in FMN

Generally EA approach improves cyber security by providing a structured approach to align and integrate security measures across an organization's IT and business landscape. It helps organizations in identifying and aligning security policies with regulation and compliance requirements. Identifying system and business process requirements early will mitigate the need for additional adjustments, security mechanisms or interfaces afterwards which reduces possible attack surfaces and vulnerabilities. Ignoring the entirety in cyber security can lead to partial optimization, which may cause security flaws, usability or performance problems impairing the functionality of the whole system. If organization does not have realistic data about its systems or technologies, it is difficult to assess and control vulnerabilities (like CVEs) and their coordinated repair is almost impossible.

Even though security architectures like AICA provides interoperability in security monitoring and control in network, it is still relies heavily in tailoring the agent based solution into environment's technical configuration. From EA perspective, focus should be on system requirements and compatibility to avoid excessive customization and ad hoc solutions. Boonstra et al. (2012) emphasize the need for technology alignment, since fundamentally different systems and technologies are unfeasible to reconcile effectively.

Security requirements should be implemented into EA practices so that they are realized in processes and developed solutions. It is not unusual that security requirements are neglected in development phase and security mechanisms are implemented afterwards, which is consuming more resources and can hinder the functionality.

Many security oriented frameworks help achieve adequate level of security within an organization, but problems may arise when system functions and processes are expanded outside the organization, forming more complex systems. Mtsweni et al. (2018) presented cybersecurity framework for complex environments, which is using a ICM based (Integrated Capability Management) approach. It uses partially same elements with DOTMLPFI: POSTEDFIT-B, which stand for Personnel, Organization, Support, Training Equipment, Doctrine, Facilities, Intelligence, Technology and Budget.

Presented model emphasize a holistic view of people, technology and processes in complex cyber environments, whose interconnectedness should be evaluated and considered every time (Mtsweni et al., 2018). Authors have not yet tested this framework at the time of writing, but

it might have similar flaws than DOTMLPFI: Neither approach provide any kind of tool or practice to manage capabilities, focusing mainly on governance from certain viewpoints.

Capability development model presented in this thesis improves security by providing holistic view of organisations capabilities in different levels, which enables identifying gaps and managing essential assets and resources. This information helps focusing security measures and resources in right place and enables holistic security planning in every architecture level. In FMN context, nations and partners using similar approach or model to manage and develop capabilities improves their interoperability and common cyber security objectives.

The problem with current frameworks used in defence sector is that interoperability is usually considered and tested in technology architecture level. Frameworks such as NAF or DODAF are difficult to use and implement effectively, so many aspects can be misunderstood and ignored. Traditional frameworks and capability models in defence sector rarely consider cyber elements and threats because they are included as part of overall security, which can cause gaps and challenges on cyber security mechanisms and related capabilities.

This model is lighter and more comprehensible to use, making it easier to deploy. When common systems, APIs or migrations are made or planned in NATO or other military organization, capabilities described with the same notation enables better reconciliation and facilitate easier coordination. Identifying own capabilities and related security aspects makes it easier to collaborate with others, enabling common security baseline. Instead of defining minimum interoperability requirements, we should focus what systems need to be interoperating and what information we should share and use in those systems.

6 Conclusions

This thesis examined Enterprise Architecture, its frameworks to implement and manage it and related standards and frameworks. Literature reviews provided background information to form an idea of EA and its complexity. EA related research in the public sector highlighted challenges in EA implementation and practices, which should be considered in the military context. The concept of Federated Mission Networking (FMN) and EA related military studies emphasize capability requirements and development efforts. Capability-based development work has been carried out in the military for a long time. This thesis aims to unify and align the requirements and terminology of the EA and military capabilities, distinguishing capabilities from their attributes.

The thesis presents a capability development model based on DOTMLPFI viewpoints to implement, manage and govern EA in military organisation and alliance. Model helps identifying organisation's strengths and weaknesses in current state and provided information can be used to holistically improve and manage capability development and cyber security. It enables shifting from minimum viable architectures to full comprehensive models, which improve interoperability in larger scale.

Research Question 1: What challenges are there for using Enterprise Architecture approach and practices in military context?

Applying Enterprise Architecture in military contexts presents several challenges. One major difficulty lies in the differing interpretations of key concepts such as "capability", which can be context dependent (Yue & Henshaw, 2009) and may vary significantly between strategic, operational, and technical stakeholders. While EA frameworks aim for alignment and improvement, the military environment is often characterized by bureaucratic structures, hierarchical decision-making and complex chains of command, which all challenge structured architectural and systemic development. Using the presented capability development model will highlight differences in current definitions, enabling common consensus and better capability development.

Research Question 2: How could Enterprise Architecture support capability development and security measures in multinational military federation?

Enterprise Architecture can play a crucial role in enhancing capability development and security coordination within multinational military federations. EA facilitates common

understanding of operational needs, technological assets and capability gaps, ensuring that development initiatives align with collective strategic goals. It enables interoperability by standardizing processes, information flows and system interfaces, which is critical in multinational environments such as Federated Mission Networking. From cyber security point of view, EA ensures that security measures are systematically embedded into all layers of development, from initial planning to operational deployment and use. Through governance, shared situational awareness, and coordinated development of capabilities, EA strengthens the collective cyber resilience, interoperability and operational effectiveness of defence coalition. The presented capability development model tries to align military capability development with EA practices to make it easier to implement and use in a military organization.

From a theoretical perspective, this research contributes to the understanding of how EA can be used in military context. Practically, the results highlight the need for structured and aligned EA strategies that can respond to changing capability requirements, interoperability and evolving cyber threats. Capability development model can improve the identification of the capabilities and their attributes, enabling their management and aligned development in multinational defence context.

A limitation of this study is its reliance on publicly available data and case studies from NATO member states. Future research could incorporate classified military information (made by military researchers) and real-world implementation cases for a more comprehensive analysis. Additionally, further studies could compare EA implementations and practices across different military organisations and alliances to identify gaps in the presented model and share best practices.

Within NATO, ensuring interoperability among allied forces is essential for seamless collaboration, secure information exchange, and coordinated cyber defence. A well-structured and common EA framework or model enables military organisations to build resilient, adaptive and scalable operating models and systems that can withstand cyber attacks and threats. Achieving a unified cyber defence strategy supports also multi-domain operations ensuring interoperability, cyber security, and operational efficiency across land, naval, air and space domains. By increasing EA-driven approaches to improve FMN capabilities, NATO and allied defence forces can enhance joint mission effectiveness, better manage cyberspace and maintain technological superiority in constantly evolving battlefield.

References

AltexSoft. (2023). *Scaled Agile Framework: Overview, pros and cons, alternatives*. Retrieved July 30, 2024, from https://www.altexsoft.com/blog/scaled-agile-framework-safe/

Anteroinen, J. (2013). *Enhancing the development of military capabilities by a systems approach*. [Doctoral thesis, National Defence University]. Doria. https://urn.fi/URN:ISBN:978-951-25-2484-6

AXELOS. (2020). *ITIL4 Foundation Book.* The Stationery Office

Banker, R., Hu, N., Pavlou, P., Luftman, J. (2011). CIO reporting structure, strategic positioning, and firm performance. *MIS Quarterly, 35*, 487–504. https://doi.org/10.2307/23044053

Blomvall, P., Hirvi, M. (2024). *A dynamic and decentralised headquarters to thrive in uncertainty.* Journal of Military Studies. https://doi.org/10.2478/jms-2024-0008

Boonstra, D., Hartog, T., Schotanus, H., Verkoelen, C. (2012). *A secure NEC-enabling architecture disentangling infrastructure, information and security.* NATO Science & Technology Organisation (STO). Retrieved March 23, 2024, from https://doi.org/10.14339/STO-MP-IST-111-06-pdf

Boxer, P., Miller, S. (2009). Enterprise architecture for complex system-of-systems contexts. *2009 3rd Annual IEEE Systems Conference* (pp. 211–216)., Vancouver, BC, Canada. https://doi.org/10.1109/SYSTEMS.2009.4815807

Brée, T., Karger, E. (2022). Challenges in enterprise architecture management: Overview and future research [Special issue]. *Journal of Governance & Regulation, 11*(2), 355–367. https://doi.org/10.22495/jgrv11i2siart15

Buckman, T. (2005). *NATO network enabled capability (NNEC) feasibility study (Version 2.0)*. NATO C3 Executive Summary. Retrieved March 23, 2024, from http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf

C3B Interoperability Profiles Capability Team. (2023). *Allied Data Publication 34 (ADatP-34(K)): NATO Interoperability Standards and Profiles, Volume 1, Version 11* NISP Volume 1,ADatP-34(K)-REV1. Retrieved March 23, 2024, from https://archive.nisp.nw3.dk/nisp-11.0/pdf/NISP-Vol1-v11-release.pdf

CMMI Institute. (n.d.). *CMMI levels of capability and performance*. Retrieved March 5, 2025, from https://cmmiinstitute.com/learning/appraisals/levels

Conexiam. (n.d.). *Three types of EA frameworks*. Retrieved March 18, 2024, from https://conexiam.com/the-three-types-of-enterprise-architecture-framework/

Dang, D., & Pekkola, S. (2016). Root causes for enterprise architecture problems in the public sector. *In Proceedings of the 20th Pacific Asian Conference on Information Systems 2016.* PASIC 2016. *287.* Chiayi, Taiwan, Association for Information Systems AIS. pp 1-16.

Daoudi, W., Doumi, K., Kjiri, L. (2021). Complexity and adaptive enterprise architecture. *In Proceedings of the 23rd International Conference on Enterprise Information Systems - Volume 2: ICEIS*. pp 759-767. https://doi.org/10.5220/0010475707590767

Dekker, M. D., & Phogg2. (2008). *Zachman Framework Detailed* [Diagram]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Zachman_Framework_Detailed.jpg

Digi- ja väestövirasto. (n.d.). *JHS-suositukset*. Retrieved September 12, 2024, from https://dvv.fi/jhs-suositukset

Digi- ja väestövirasto. (n.d.). *Arkkitehtuuri.* Retrieved September 12, 2024, from https://dvv.fi/arkkitehtuuri#

DoD CIO. (n.d.). *DoD Architecture Framework (DoDAF 2.0)*. Retrieved March 10, 2024, from https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_background/

Drent, M., Wilms, E., Zandee, D. (2017). *Making sense of European defence: Capability development (pp. 10–15)*. Clingendael Institute. Retrieved March 30, 2025, from https://www.clingendael.org/sites/default/files/2017-12/Making_Sense_of_European_Defence.pdf

Eie, K. M. (2016). *Authentication in protected core networking*. [Master's thesis, Norwegian University of Science and Technology]. NTNU Open. http://hdl.handle.net/11250/2403226

European Union. (2022). *NIS 2 Directive.* Retrieved July 30, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

Fenng (dbanotes). (2011). *TOGAF* [Diagram]. Flickr. Retrieved April 5, 2025, from https://www.flickr.com/photos/fenng/3671841856/in/photostream/

Capability Planning Working Group (CPWG) (2018). *Spiral 3 Standards Profile, Final FMN Spiral 3 Specification.* Retrieved March 23, 2024, from https://storage.nisp.nw3.dk/20181118_Final_FMN_Spiral_3_Standards_Profile_Bundle.pdf

Gebhard, P., Crosby, R. (2010). *NATO defense capabilities: A guide for action.* Strategic Advisors Group. Retrieved March 23, 2024, from https://www.atlanticcouncil.org/wp-content/uploads/2010/04/NATODefense_SAGIssueBrief.pdf

Greefhorst, D., Proper, E. (2011). The role of enterprise architecture. In *Architecture principles.* (Vol. 4, pp. 5–13). Springer. https://doi.org/10.1007/978-3-642-20279-7_2

Hosiaisluoma, E. (2022). *Capability-based development of an organization*. Retrieved February 24, 2025, from https://www.hosiaisluoma.fi/blog/capability-based-development/

Hussain, B., Imran, A., & Turner, T. (2016). Key Challenges for Establishing CIO Position in the Public Sector of LDCs: A Case of Bangladesh. In *Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016*. Association on Information Systems (AIS). pp. 1-11.

Hämäläinen, R., Jones, R., Saarinen, E. (2014). *Being better better: Living with systems intelligence.* Aalto ARTS Books.

Ikonen, I., Pitkäkoski, H. (2025). Project management practices in defence projects. In *Proceedings of the 9th International Conference on Research in Management and Economics*.2(1):49-58. Cambridge, United Kingdom. https://doi.org/10.33422/imeconf.v2i1.879

International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection*. ISO/IEC 27001:2022, Edition 3. https://www.iso.org/standard/27001

JCIDS Manual. (2021). *Manual for the operation of the Joint Capabilities Integration and Development System.* Related to Document CJCSI 5123.01I. Retrieved March 23, 2024, from https://www.dau.edu/sites/default/files/2024-01/Manual%20-%20JCIDS%20Oct%202021.pdf

Johnsen, F. T., Hauge, M. (2022). Interoperable, adaptable, information exchange in NATO coalition operations. *Journal of Military Studies, 11*(1), 1–12. https://doi.org/10.2478/jms-2022-0005

Jonkers, H., Lankhorst, M., ter Doest, H. W. L., Arbab, F., Bosma, H., Wieringa, R. (2006). Enterprise architecture: Management tool and blueprint for the organisation. *Information Systems Frontier, 8*(2), 63–66. https://doi.org/10.1007/s10796-006-7970-2

Kansallinen turvallisuusviranomainen. (2020). *Katakri 2020: Tietoturvallisuuden auditointityökalu viranomaisille.*Ulkoministeriö. Finland.

Kappelman, L. A., Zachman, J. A. (2013). The enterprise and its architecture: Ontology & challenges. *Journal of Computer Information Systems, 53*(4), 87–95. https://doi.org/10.1080/08874417.2013.11645654

Kerr, C., Phaal, R., Probert, D. (2006, September). *A framework for strategic military capabilities in defense transformation*. Paper presented at the 11th International Command and Control Research and Technology Symposium (ICCRTS): Coalition Command and Control in the Networked Era. Cambridge, United Kingdom.

Kotusev, S., Alwadain, A. (2024). Modeling business capabilities in enterprise architecture practice: The case of business capability models. *Information Systems Management, 41*(2), 201–223. https://doi.org/10.1080/10580530.2023.2231635

Kotusev, S. (2018). *Fake and real tools for enterprise architecture: The Zachman Framework and Business Capability Model. Enterprise Architecture Professional Journal* Retrieved March 8, 2024, from https://eapj.org/fake-and-real-tools-for-enterprise-architecture/

Kotusev, S. (2019). *The process view of enterprise architecture practice*. Published September 2019 by the British Computer Society (BCS). Retrieved March 8, 2024, from https://www.bcs.org/content-hub/the-process-view-of-enterprise-architecture-practice/

Kotusev, S. (2016). *Enterprise architecture is not TOGAF*. Retrieved March 8, 2024, from http://www.bcs.org/content/conWebDoc/55547

Kotusev, S. (2017). Enterprise architecture: What did we study? *International Journal of Cooperative Information Systems, 26*(4), 1–84. https://doi.org/10.1142/S0218843017300029

Kotusev, S. (2021). *A comparison of the top four enterprise architecture frameworks.* Retrieved August 12, 2024, from https://www.bcs.org/articles-opinion-and-research/a-comparison-of-the-top-four-enterprise-architecture-frameworks/#19

Lankhorst, M. (2017). *Enterprise architecture at work: Modelling, communication, and analysis*. (4th ed.) Springer. https://doi.org/10.1007/978-3-662-53933-0

LeanIX. (n.d.). *A definitive guide to Zachman framework*. Retrieved July 22, 2024, from https://www.leanix.net/en/wiki/ea/zachman-framework

Lemmetti, J., Pekkola, S. (2012). Understanding enterprise architecture: Perceptions by the Finnish public sector. *Electronic Government (EGOV 2012)* (Vol. 7443, pp. 162–173). Springer. https://doi.org/10.1007/978-3-642-33489-4_14

Maltusch, T. (2020). *Kokonaisarkkitehtuurin hyödyntäminen Maanpuolustuskorkeakoulun strategian suunnittelussa.* [Master's Thesis, Tampereen ammattikorkeakoulu]. Theseus. https://urn.fi/URN:NBN:fi:amk-2020122029732

Marion, R. (2008). Complexity theory for organizations and organizational leadership. In M. Uhl-Bien & R. Marion (Eds.), *Complexity leadership, part 1: Conceptual foundations* (pp. 1–15). Information Age Publishing

Mtsweni, J., Gcaza, N., Thaba, M. (2018). A unified cybersecurity framework for complex environments. In *Proceeding of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists. SAICSIT '18.* Port Elizabeth, South Africa. *pp 1-9.* https://doi.org/10.1145/3278681.3278682

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* https://doi.org/10.6028/NIST.CSWP.29

NATO Architecture Capability Team. (2018). *NATO Architecture Framework Version 4.* Document Version 2020.09 (AC/322-D(2018)0002-REV1) Retrieved March 23, 2024, from https://www.nato.int/nato_static_fl2014/assets/pdf/2021/1/pdf/NAFv4_2020.09.pdf

NATO Architecture Capability Team. (2025). *ArchiMate Modeling Guide For the NATO Architecture Framework Version 4*. Document Version 2025.04. Retrieved March 23, 2024, from https://www.nato.int/nato_static_fl2014/assets/pdf/2025/4/pdf/2504-NAFv4-ArchiMate.pdf

NATO. (n.d.). *FMN Public Site*. Retrieved March 23, 2024, from https://coi.nato.int/FMNPublic/SitePages/Home.aspx

NATO Industrial Advisory Group (NIAG). (2021). *NIAG study on the feasibility to achieve FMN Milestones 2 and 3.* Document NIAG-N(2021)0003. Retrieved March 23, 2024, from https://www.ndia.org/-/media/sites/ndia/divisions/international/niag/niag-n_2021_0003_calling_notice_fmn_milestones.ashx

Niemi, E. (2024). *Kokonaisarkkitehtuuri: Oppaasi organisaation muutosmatkalla.* Alma Insights.

Pavlak, A. (2006). *Enterprise architecture: Lessons from classical architecture*. Retrieved March 17, 2024, from https://scispace.com/pdf/enterprise-architecture-lessons-from-classical-architecture-26r386iaka.pdf

Phelan, S. E. (1999). A note on the correspondence between complexity and systems theory. *Systemic Practice and Action Research, 12*, 237–246. https://doi.org/10.1023/A:1022495500485

Pullen, J. M., Ruth, J., Ventura, P., van den Berg, T., de Reus, N., Dechand, M. (2022). *Validating M&S standards interoperation in CWIX 2022.* Retrieved March 23, 2024, from https://www.mscoe.org/document/validating-ms-standards-interoperation-in-cwix-2022/

Puolustusministeriö. (2021). *Tavoitteena tietoylivoima: Puolustushallinnon tietokonsepti*. http://urn.fi/URN:ISBN:978-951-663-178-6

Putta, A., Paasivaara, M., Lassenius, C. (2018). Benefits and challenges of adopting the Scaled Agile Framework (SAFe): Preliminary results from a multivocal literature review. In M. Kuhrmann, S. McIntosh, & M. Shepperd (Eds.), *Product-focused software process improvement (PROFES 2018)* (Vol. 11271, pp. 324–339). Springer. https://doi.org/10.1007/978-3-030-03673-7_24

Ross, J. W., Weill, P., Robertson, D. C. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution.* Harvard Business School Press.

Scaled Agile, Inc. (2019). *Achieving business agility with SAFe® 5.0. A Scaled Agile, Inc.* [White Paper]. Retrieved March 25, 2025, from https://www.icescrum.com/edof/safe-white-paper.pdf

Scaled Agile, Inc. (2025). *Full SAFe configuration* [Diagram]. Retrieved Retrieved March 25, 2025, from https://framework.scaledagile.com/posters

Schutz, R. (2010). *Protected core networking – Concepts & challenges*. In RTO-MP-IST-091: Information assurance and cyber defence symposium (Paper P06). NATO Research and Technology Organisation. https://doi.org/10.14339/RTO-MP-IST-091-P06-doc

Seppänen, V., Penttinen, K., Pulkkinen, M. (2018). Key issues in enterprise architecture adoption in the public sector. *Electronic Journal of e-Government, 16*(1), 46–58. Management Centre International

Sherwood, J., Clark, A., Lynas, D. (2009). *TSI-W100-SABSA white paper: Enterprise security architecture* [White paper]. SABSA. Retrieved March 25, 2025, from

https://sabsacourses.com/wp-content/uploads/2021/02/TSI-W100-SABSA-White-Paper.pdf

Sowa, J. F., Zachman, J. A. (1992). Extending and formalizing the framework for information systems architecture. *IBM Systems Journal, 31*(3), 590–616. https://doi.org/10.1147/sj.313.0590

Span, M. T., Mailloux, L. O., Grimaila, M. R. (2018). *Cybersecurity architectural analysis for complex cyber-physical systems. The Cyber Defense Review,* 3(2), 115–134.

The NATO C2COE. (2020). *FMN, a project by NATO C2COE | Expertise Management Branch | Quick Reference List 2020.* Retrieved March 23, 2024, from https://c2coe.org/wp-content/uploads/Library%20Documents/QRL/2020/QRL_C2COE%202020%20Federated%20Mission%20Networking%20%28FMN%29.pdf

The Open Group. (2022). *TOGAF Standard, 10th Edition.* Digital edition. The Open Group. Retrieved July 24, 2024, from https://www.opengroup.org/standards

The Open Group. (2011). *TOGAF version 9.1 enterprise edition.* The Open Group. Retrieved July, 2024, from https://www.opengroup.org/standards

Theron, P., Kott, A., Drašar, M., Rzadca, K., LeBlanc, B., Pihelgas, M., Mancini, L., Panico, A. (2018). Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture. *In Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS). IEEE. Warsaw, Poland. pp. 1-9.* https://doi.org/10.1109/ICMCIS.2018.8398730

Valtioneuvosto. (2007). *20.12.2007/1319 Valtioneuvoston asetus puolustusvoimista.* Retrieved February 24, 2025, from https://www.finlex.fi/fi/laki/ajantasa/2007/20071319#L2P10

Valtioneuvosto. (n.d.). *Digitalisaation ja datatalouden vastuualueen yhteistyöryhmä (Digitoimisto).* Retrieved September 16, 2024, from https://valtioneuvosto.fi/hanke?tunnus=LVM066:00/2021

Valtiovarainministeriö. (n.d.). *Digitoimiston yhteistyöryhmät*. Retrieved September 16, 2024, from https://vm.fi/yhteistyoryhmat

Valtiovarainministeriö. (n.d.). *Digitoimisto.* Retrieved September 16, 2024, from https://vm.fi/digitoimisto

Valtiovarainministeriö. (n.d.). *First common strategy to address challenges in public sector ICT utilisation*. Retrieved September 16, 2024, from https://vm.fi/en/-/first-common-strategy-to-address-challenges-in-public-sector-ict-utilisation

Valtiovarainministeriö. (n.d.). *Julkisen hallinnon tietohallinnon neuvottelukunta*. Retrieved September 16, 2024, from https://vm.fi/hanke?tunnus=VM007:00/2010

Valtiovarainministeriö. (n.d.). *Julkisen hallinnon yhteisen kokonaisarkkitehtuurin (JHKA) työryhmä.* Retrieved September 16, 2024, from https://vm.fi/hanke?tunnus=VM130:02/2015

Valtiovarainministeriö. (n.d.). *Julkisen hallinnon kokonaisarkkitehtuurityöryhmä (JHKA).* Retrieved September 16, 2024, from https://vm.fi/hanke?tunnus=VM036:00/2019

Valtiovarainministeriö. (n.d.). *Julkisen hallinnon toiminnan kehittämisen arkkitehtuuriyhteistyöryhmä*. Retrieved September 16, 2024, from https://vm.fi/hanke?tunnus=VM142:00/2020

Valtiovarainministeriö. (n.d.). *Kokonaisarkkitehtuurijaosto*. Retrieved September 16, 2024, from https://vm.fi/hanke?tunnus=VM006:03/2013

Valtiovarainministeriö. (n.d.). *Tiedonhallinnan yhteistyöryhmät*. Retrieved September 16, 2024, from https://vm.fi/tiedonhallinnan-yhteistyoryhmat

Valtiovarainministeriö. (n.d.). *Tiedonhallinnan yhteistyöryhmät*. Retrieved September 12, 2024, from https://vm.fi/tiedonhallinnan-yhteistyoryhmat

Valtiovarainministeriö. (n.d.). *Tiedonhallintalaki*. Retrieved September 12, 2024, from https://vm.fi/tiedonhallintalaki

Velazquez, A., Mathews, J., Lopes, R. F. R., Braun, T., Free-Nelson, F. (2023). Toward autonomous cyber defense for protected core networking. *In Proceedings of the 2023 International Conference on Military Communications and Information Systems (ICMCIS).* IEEE. Skopje, North Macedonia. pp. 1-7 https://doi.org/10.1109/ICMCIS59922.2023.10253614

Vinarcik, M., Gibson, M. (2019, October). *The problem with DoDAF models.* [Ppt presentation] NDIA 22nd Annual Systems and Mission Engineering Conference. Tampa, FL, USA. https://ndia.dtic.mil/wp-content/uploads/2019/systems/Wed_22358_Gibson.pdf

Von Bertalanffy, L. (1950). An outline of general system theory. *The British Journal for the Philosophy of Science, 1*(2), 134–165. https://doi.org/10.1093/bjps/i.2.134

White, S. K., Greiner, L. (2022). *What is ITIL? Your guide to the IT Infrastructure Library. CIO.* Retrieved July 20, 2024, from

https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html

Wolff, M. (2019). *Architecture Development Method* [Diagram]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Architecture_Development_Method.png

Ylinen, M., Pekkola, S. (2018 , December). *Enterprise architecture as a scapegoat for difficulties in public sector organizational transformation*. In Proceedings of International Conference on Information Systems (ICIS'2018). San Francisco, CA, USA. pp 1-11.

Yue, Y., Henshaw, M. (2009). *An Holistic View of UK Military Capability Development. Defense and Security Analysis. 25*(1), 5–19. https://doi.org/10.1080/14751790902749900

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal, 26*(3), 276–292. https://doi.org/10.1147/sj.263.0276