NATIONAL DEFENCE UNIVERSITY

A CYBER SECURITY ARCHITECTURE FOR MILITARY NETWORKS USING A COGNITIVE NETWORK APPROACH

Thesis

Captain (Eng.)
Anssi Kärkkäinen

General Staff Officer Course 56
Army

July 2013

NATIONAL DEFENCE UNIVERSITY

Course **General Staff Officer Course 56**	Branch **Army**
Author **Captain (Eng.) Anssi Kärkkäinen**	
Title **A CYBER SECURITY ARCHITECTURE FOR MILITARY NETWORKS USING A COGNITIVE NETWORK APPROACH**	
Area of study Military Technology	Repository NDU Course Library
Date July 2013	Text pages 116 Appendixes -

ABSTRACT

Cyber security is one of the main topics that are discussed around the world today. The threat is real, and it is unlikely to diminish. People, business, governments, and even armed forces are networked in a way or another. Thus, the cyber threat is also facing military networking. On the other hand, the concept of Network Centric Warfare sets high requirements for military tactical data communications and security. A challenging networking environment and cyber threats force us to consider new approaches to build security on the military communication systems.

The purpose of this thesis is to develop a cyber security architecture for military networks, and to evaluate the designed architecture. The architecture is described as a technical functionality. As a new approach, the thesis introduces Cognitive Networks (CN) which are a theoretical concept to build more intelligent, dynamic and even secure communication networks. The cognitive networks are capable of observe the networking environment, make decisions for optimal performance and adapt its system parameter according to the decisions. As a result, the thesis presents a five-layer cyber security architecture that consists of security elements controlled by a cognitive process. The proposed architecture includes the infrastructure, services and application layers that are managed and controlled by the cognitive and management layers. The architecture defines the tasks of the security elements at a functional level without introducing any new protocols or algorithms.

For evaluating two separated method were used. The first method is based on the SABSA framework that uses a layered approach to analyze overall security of an organization. The second method was a scenario based method in which a risk severity level is calculated. The evaluation results show that the proposed architecture fulfills the security requirements at least at a high level. However, the evaluation of the proposed architecture proved to be very challenging. Thus, the evaluation results must be considered very critically. The thesis proves the cognitive networks are a promising approach, and they provide lots of benefits when designing a cyber security architecture for the tactical military networks. However, many implementation problems exist, and several details must be considered and studied during the future work.

KEY WORDS

Cyber security, cyber threat, cognitive networks, security architecture, architecture evaluation, military networks, communication networks

A CYBER SECURITY ARCHITECTURE FOR MILITARY NETWORKS USING A COGNITIVE NETWORK APPROACH

Table of Content

ACRONYMS

AACE	Application Access Control Element
AET	Advanced Evasion Technique
API	Application Programming Interface
C2	Command and Control
CC	Common Criteria
CE	Cryptography Element
CIA	Confidentiality, Integrity and Availability
CN	Cognitive Network
CSF	Cisco Security Framework
CyberSA	Cyber Situational Awareness
CyberSpt	Cyber Support
CyberWar	Cyber Warfare
CyNetOps	Cyber Network Operations
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoS	Denial-of-Service
EMP	Electromagnetic Pulse
FST	Full Scenario Table
HPM	High Power Microwave
IA	Information Assurance
ICT	Information and Communication Technology
ID	Identity
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol

IP	Internet Protocol
IPS	Intrusion Protection System
IPsec	Internet Protocol Security
ITSEC	Information Trust Security Evaluation Criteria
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MACE	Management Access Control Element
MLE	Management Log Element
MOD	Ministry of Defence
MODAF	Ministry of Defence Architecture Framework
NACE	Node Access Control Element
NAF	NATO C3 Systems Architecture Framework
NCSC	National Computer Security Center
NCW	Network Centric Warfare
NEC	Network Enabled Capability
OAM&P	Operations, Administration, Maintenance & Provisioning
OODA	Observe, Orient, Decide and Act
OSI	Open System Interconnection
OWASP	Open Web Application Security Project
PACE	Packet Access Control Element
QoS	Quality of Service
RAND	Research ANd Development
ROE	Rules of Engagement
RRM	Risk Rating Methodology
RSE	Routing Security Element
SABSA	Sherwood Applied Business Security Architecture
SACE	Service Access Control Element
SIP	Session Initiation Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

TCSEC	Trusted Computer System Evaluation Criteria
TMFE	Traffic Monitoring and Filtering Element
TSE	Traffic Shaping Element
TVM	Threat and Vulnerability Management
UK	United Kingdom
UN	United Nations
US	United States
VME	Vulnerability Management Element
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

A CYBER SECURITY ARCHITECTURE FOR MILITARY NETWORKS USING A COGNITIVE NETWORK APPROACH

1. INTRODUCTION

Lots of speak about cyber security and its importance have occurred in recent years worldwide. The various players have expressed cyber security the most significant factor in the near future. Many countries have drawn up cyber security strategies and the question arises how the cyber threats should take precaution. Cyber security is not only for governmental or business actors, but it is related to everyone's daily activities.

The internet and networks are revolutionizing our society worldwide by giving people, business and military new ways to work and co-operate with one another. This will drive the expansion of cyberspace. The networks on which everyone now relies for daily business transcend organizational and national boundaries. Cyberspace has become a domain where strategic or operational advantages of business or even military can be won or lost. The growing usage of cyberspace means that its disruption can affect armed forces' ability to function effectively during a crisis.[92]

Events in cyberspace occur at high speed. Traditional responses may not be sufficient to protect critical infrastructure and services. Although risks in cyberspace can be managed in several ways, they do not often match this complex and dynamic environment. Increasing dependence on cyberspace brings new benefits but also new threats. Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. While cyberspace raises open markets and open societies, this very openness can also make business and military actors more vulnerable to criminals, hackers, and foreign intelligence services who try to compromise or damage the critical systems. [92]

Security architectures and controls of legacy military networks were not built to face the new threats. Traditionally, the military networks were isolated from other networks, and access to them was very limited both to geographical areas and a number of authorized users. Physical security means played an enormous role in these systems and networks. In the legacy systems, security controls are often built after the network and service implementation causing vulnerabilities and potential threats. A holistic view to information and cyber security has been missing.

At the same time with growing cyber security threats, military troops are more dependent on networks and services than ever. A huge growth has occurred for example with situational awareness systems which all require reliable communications networks and servers. Today, all military capability areas (weapon systems, targeting, etc.) are related to information technology and applications. Usage of commercial technologies when providing these services means that the cyberspace threats of the internet are relevant threats also to the IT military systems.

Network Centric Warfare (NCW) has increased the significance of military communication networks during last decades. NCW is an operational concept enabling information superiority in which the main idea is to increase military combat power by networking the battlefield actors from perspective of processes, operations and information sharing [7]. NCW is primarily an operational model, but communication networks play an important role as an enabler of networking activities and information sharing.

From NCW and cyber security perspectives, Cognitive Networks (CN) is an interesting research area. These intelligent and self-learning cognitive networks are believed to generate more performance also for military networking systems. The cognitive networks are simply smart communications networks (made up of a network nodes, and wired and wireless connections between them) that are able to be aware of the network's internal and environmental situation [58]. CN has an ability to operate independently, make decisions and adapt according to the given goal. A key feature is learning which means that the network can exploit previously made decisions during a cognitive process.

From a military point of view, CN is a promising concept. On the battlefield, tactical cognitive networks would adapt automatically according to environmental changes. Network resources could be used dynamically and effectively. Network administration and configuration would no longer require human operators or manual configuration.

However, the cognitive networks may face the same cyber security threats than traditional networks, because data transmission in these networks is based on common and standardized network and link protocols. A management process of a cognitive network may bring even more cyber security challenges. The cognitive networks with a decision making process, sensors and adaptive layers are more complex, and thus enable new types of cyber attacks. An adversary may launch cyber attacks to influence e.g. sensor input data, information sharing between nodes, or the decision-making process.

This thesis focuses on architectural security aspects of military networks. The main purpose of the thesis is to consider how the features of cognitive networks could be used for building and designing a cyber security architecture for military communications networks. The cyber security architecture describes all the security functionalities and controls that are required when implementing the high-secure military networks. Cognitive features will create more knowledge on networks which could mean better performance, resource usage and higher security, but CNs may also push up new security threats, especially in a tactical battlefield environment. Growing cyber security threat demands that security requirements are already considered in the beginning of the network designing process. Thus, it is relevant and necessary to create a cyber security architecture that could be utilized at a starting point when modern military networks are planned and implemented.

1.1. Related Research

Related work consists of published books and research papers about cognitive networks, cyber security and network security. Cognitive networks are currently studied in various research programs. Previously, research was focusing more on the cognitive radios and spectral efficiency and usage of them, but now cognitive features are spread to an entire communication system and all the layers of a networking device. Cognitive networks research focuses largely on the decision-making mechanisms, and communication and optimization between the layers (cross-layer functionality). The basic idea behind the cognitive network is presented in the research papers by R. Thomas et al [95], [96][97]. A book called *Cognitive radio communications and networks: principles and practice* [105] explores the state-of-the-art in cognitive networks, compiling a roadmap to future research. It also covers cognitive radios with semantic aspects.

Network security is also a widely studied research field. The latest research and future developments of network security are provided in books *Network Security: Current Status and Future Directions* [30] and *Principles of Information Security* [103]. These books cover a wide range of topics dealing with secure routing, firewall design, mobile agent security, Bluetooth security, wireless sensor networks, and digital content security. Research papers dealing with cognitive network security mainly focus on the traditional security problems with a narrow sector or they have a very limited problem statement (e.g. access control, encryption, etc.).

For example, a research paper written by J. L. Burbank [14] discusses the topic of wireless security in cognitive radio networks, delineating the key challenges of wireless cognitive networks. The paper declares that securing the decision-making process is fundamental to a cognitive radio. G. Safdar and M. O'Neill [82] present a novel framework for providing common control channel security for co-operatively communicating cognitive radio nodes. The paper considers how cognitive radio network nodes can authenticate each other prior to any confidential channel negotiations to ensure protection against cyber attacks.

Also, Yi Peng et al [106] discuss security of cognitive radio networks. The paper proposes a novel architecture in which the dynamic radio channel access is reached by a cross-layer design between the physical and MAC layers. The research paper also shows by simulations that a novel centralized dynamic channel access mechanism can improve network performance. A problem with these previous references is that they are related to security of cognitive radio networks. It is challenging to find research papers (at least from IEEE Digital Library) concerning general cognitive networks and their overall security design. None of these research articles presents a high-level architectural view including security controls and functions for all layers and services.

Lots of cyber security and cyber threat related research papers are published during last years. Naturally, this research has also produced several books. Many of the books consider other than technical aspects of cyber security but we can find a few that focus on technology. Cyber threats are widely covered in books *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* [10], *Strategic Cyber Security* [39], *Inside Cyber Warfare* [16], and *Cyber Security Essentials* [41]. Cyber threats on cognitive networking are discussed for example by A. Fragkiadakis et al [36], Yuan Zhang et al [108] and Qingqi Peiet al [78].

1.2. Research Objective, Methodology and Structure

The main research objective is to describe a cyber security architecture with functional properties for military networks using the features of cognitive networking. A major goal is to design an overall architecture that includes sufficient security functionalities and controls to protect information processing and sharing especially in tactical military networking.

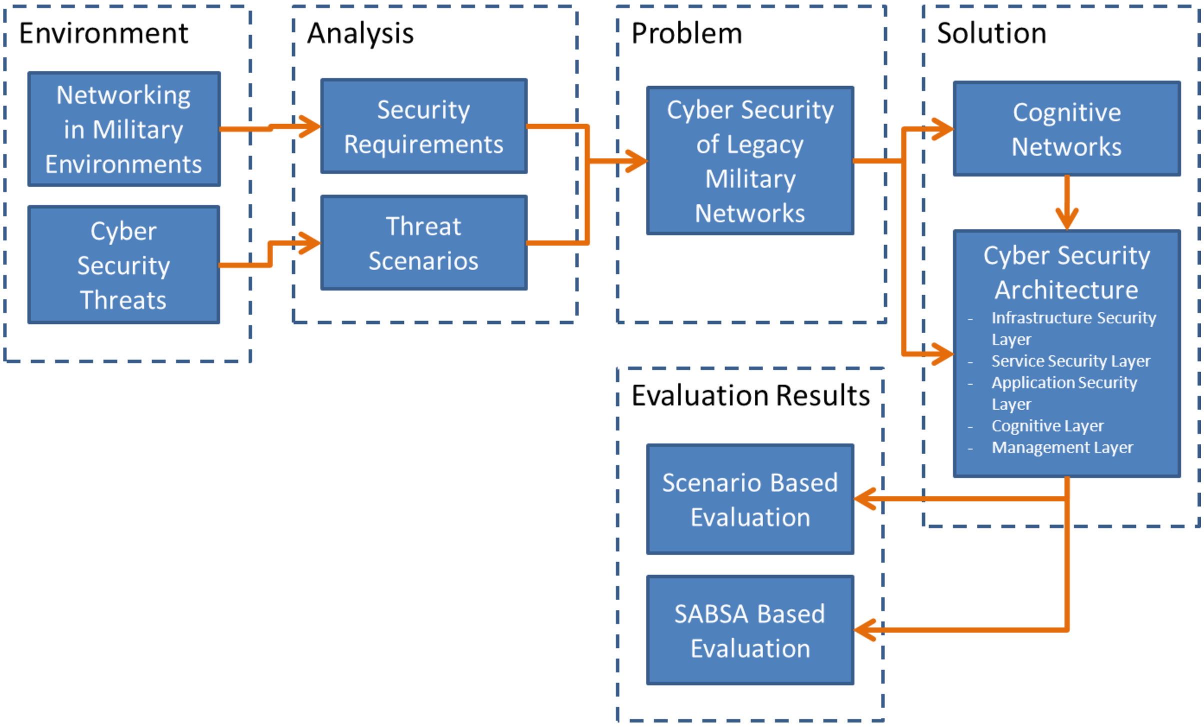


Figure 1: Research process.

The research framework of the thesis is concretized through the research process that is depicted in Figure 1. The figure also illustrates the structure of this study that consists of the environment, analysis, problem, solution and evaluation phases. First, two environmental entities (networking in a military environment, cyber security threats) are studied resulting the analysis of security requirements and current cyber threats on military networks. The purpose is to show what kind of requirements Network Centric Warfare and a challenging operating environment set to military networking, and what the security goals of military networking are. After the environmental study, the current cyber threat is examined to present the picture of the latest information about the characteristics of cyber space, cyber warfare, threat concerning tactical military networks and the challenges legacy networks face.

Once the environment and cyber threats are analyzed, the features of cognitive networks are explained in the solution phase. This part of the study describes what the cognitive networks are, how they work, and what benefits they would bring to networking and especially its security design. The cognitive network concept is used as a basis when the cyber security architecture for military networks is designed in the next phase. Finally, the proposed cyber security architecture is evaluated using a scenario based evaluation and Sherwood Applied Business Security Architecture (SABSA) based approaches in the evaluation phase. The aim is to show how the designed architecture meets the requirements that were set in the beginning of the study.

The main research problem of this study is:

What are the overall design and functionalities of the cyber security architecture for military networking using the features of the cognitive networks?

The sub research questions are:

What are the requirements for military communications networks in the environment of network centric environment?

What are the security requirements for military networks?

What are the main cyber security threats to military networking?

What are the challenges of legacy military networks?

What are the cognitive networks and how do they function?

What kind is the overall cyber security architecture and what are the functional properties of the architecture?

What are the security functions and controls of the infrastructure, service and application layers?

How could the designed architecture be evaluated, and how does the architecture meet the desired requirements?

The research methodology mainly consists of literature analysis and planning. Security requirements and goals, and the characteristics of the cognitive networks are developed by using literature analysis. The thesis utilizes the planning method in the development of the cyber security architecture. Also, a method of mathematical analysis is used in the evaluation of the proposed architecture.

The thesis is divided into seven main chapters. The first chapter is introduction, and the second chapter considers networking in military environments. The chapter presents the requirements of NCW and tactical networking, and introduces the design goals and security dimensions for military networking systems. In the third chapter, cyberspace, cyber warfare and cyber security threats are studied, and the cyber threat scenarios are presented. Also, the challenges of the legacy systems are discussed. The fourth chapter describes the basic properties of the cognitive networks, and the challenges for networking in battlefield conditions. The fifth chapter proposes a cyber security architecture with the functional layers and security elements. In the sixth chapter, the proposed architecture is evaluated against the predefined scenarios. The seventh chapter concludes the study by representing the main findings of the thesis, discussion, and the future work.

1.3. Perspective and Scope

The main research perspective is to provide an architecture with technical functionality. The architecture describes technical security controls and functionalities required for secure military networking. In this study, a goal is to generate a cyber security architecture according to security requirements and other boundary conditions for secure military networking. The research perspective is also technical cyber security which means that political, law and business aspects are not considered. The architecture is designed for a tactical level networking.

The main scope is to design an overall architectural view with the description of the security features, and evaluate the proposed architecture. The purpose is to study how cognitive features could be utilized to provide more secure military networking. The architecture is a high level design, and it does not include algorithm or protocol level details. Implementation challenges and possibilities are discussed, but not analyzed in details.

1.4. Definitions

Cyberspace consists of computers (including programmable circuits), and the connections between them forming a virtual dimension. Cyberspace is the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems [93]. In cyberspace, individuals can interact, exchange ideas, share information, provide social support, trade, create various types of media, play games, participate in policy debate, etc, using the global network [92].

Cyber Defense includes actions that combine information assurance, computer network defense (to include response actions), and critical infrastructure protection with enabling capabilities to prevent, detect, and ultimately respond to an adversaries ability to deny or manipulate information and/or infrastructure. [10]

Cyber Security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. [72]

Military communication ensures that commanders and staffs at all levels are able to maintain continuous control of subordinate forces under any conditions and to communicate signals to the forces at the proper time concerning the threat of enemy attack and the implementation of combat readiness. The chief demands made on military communications are timeliness of establishment, reliability of operations, speed of action, and secrecy of transmitted information. [60]

Cognitive network is defined as a network with a cognitive process that can perceive current network conditions, plan, decide, act on those conditions, learn from the consequences of its actions, all while following end-to-end goals. The cognition loop senses the environment, plans actions according to sensor input data and network policies, decides which scenario fits best its end-to-end purpose using a reasoning engine, and finally acts on the chosen scenario as discussed in the previous section. The system learns from the past (situations, plans, decisions, actions) and uses this knowledge to improve the decisions in the future. [95]

Security architecture refers to cohesive security design, which takes into account security requirements and objectives (e.g. confidentiality, non-repudiation, authentication, authorization, etc.). The architecture addresses the risks of a particular environment/scenario, and specifies what security controls are to be applied where. The design process must be repeatable. [98]

Cyber warfare refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. Cyber warfare is politically motivated hacking to conduct sabotage and espionage to an enemy. [21]

Network Centric Warfare is an operating concept enabling information superiority, which develops growing battle power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of decision-making, higher operation speed, lethality, probability of survival and self-synchronization. [7]

2. NETWORKING IN A MILITARY ENVIRONMENT

A military networking environment, especially at the tactical level, is very challenging. At the same time, the paradigm and doctrine of Network Centric Warfare [7] increases demands on military communications and networking. This chapter concentrates on reviewing Network Centric Warfare and its requirements for information systems and networks. The chapter also describes the design goals of tactical military networks, and defines the security dimensions which act as the criteria for information and networking security in the military networks.

2.1. Network Centric Warfare

Network Centric Warfare (NCW), also called network-centric operations [104], is a military doctrine and also a war theory developed by the United States Department of Defense in the 1990s. The goal of NCW is to convert an information advantage, enabled in part by information technology, into a competitive advantage through the robust networking of well-informed geographically distributed forces. NCW networking combined with changes in technology, organization, processes, and people may allow new forms of organizational behavior.

As a solid concept, NCW was first time described in 1998 by the U.S. Naval Institute's journal, and more deeply in the same year in a book called *Network Centric Warfare* by Garstka, Alberts, and Stein [7]. The central network warfare is defined as information age warfare where the theory can be summarized through four tenets in its hypothesis [7]. These are:

1. A robustly networked force improves information sharing
2. Information sharing enhances the quality of information and shared situational awareness
3. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command
4. These, in turn, dramatically increase mission effectiveness.

As it is noticed from these four tenets, information sharing is a key element to operational success. Without an effective and continuous distribution of information the other basic tenets (2 - 4) will lose their meaning.

Figure 2 shows the value chain created from the basic tenets [7]. The value chain attempts to describe achievement of effectiveness and advantages of NCW through four tenets. In the figure, it is important to notice how the enablers (shared information and improved awareness) allow virtual collaboration and organizations that finally lead to increased tempo and responsiveness.

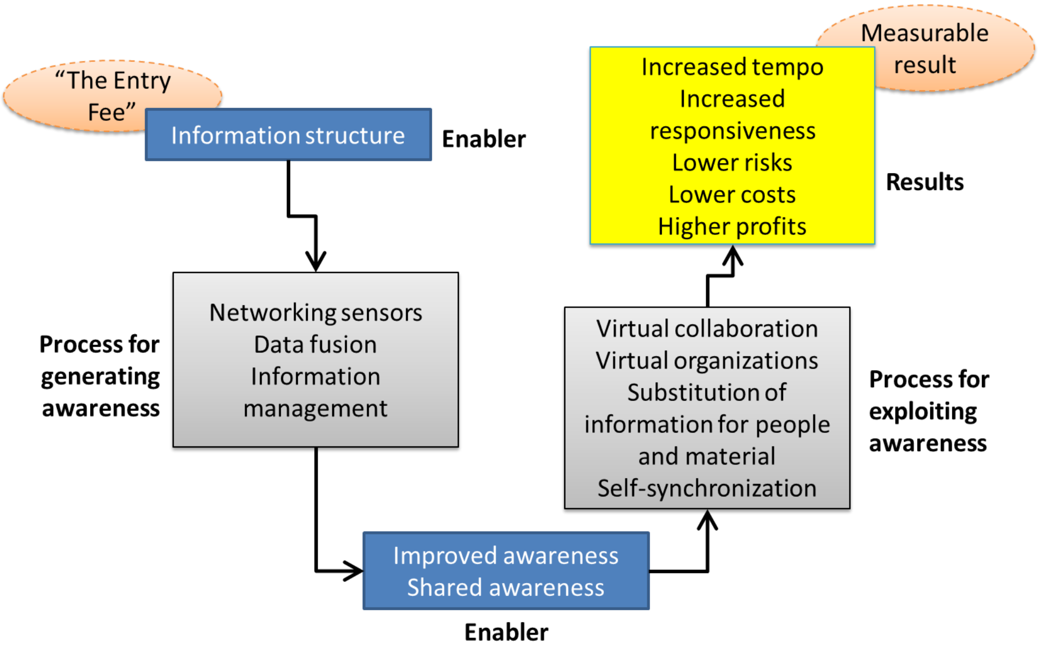


Figure 2: The chain of value.

The value chain starts with an information structure, which allows the processes that give a significantly better competitive environment by generating and sharing situational awareness through the entire organization. In turn, this improved awareness enables to create a number of processes which utilize this knowledge in such a way that the end result is improved. In war fighting, these results are increased battle speed (tempo), lower risks and costs (losses) and improved efficiency.

In the book called *Understanding Information Age Warfare* [8], published in 2001, the concept was further developed by building an operational theory of NCW. The key concept of the book is information superiority. The theory was developed by examining the perception of the environment in three domains which are *physical*, *information* and *cognitive*.

Events that can be detected by a sensor and an individual occur in the physical domain. The physical domain consists of the land, sea, air and space environments where the troops carry out operations. The communication networks combining the forces are also located in the physical domain. Data created in the physical domain is transported through the information domain. In the information domain, information is created, modified and shared. Collaboration, communications and commanding between the units take place in the information domain.

Sensors, data generated by them, and the analyzed information are situated in the information domain. Data is received and processed in the cognitive domain, where the data is valuated for a basis for further action. The cognitive domain is a fighter's mind. The elements of this domain include leadership, morale, level of education and experience, as well as situational awareness. Figure 3 shows the value chain linking information superiority and the above-mentioned domains.

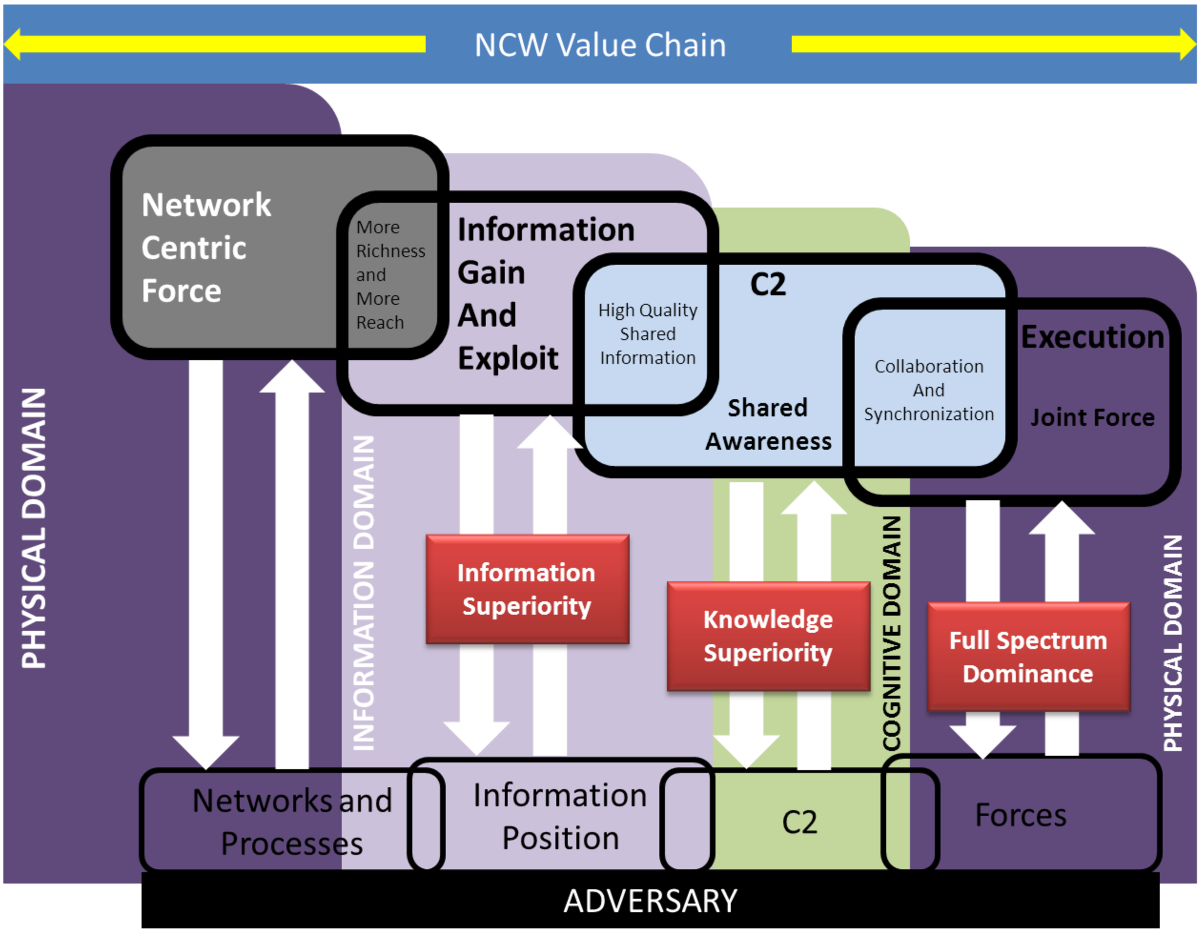


Figure 3: The value chain links of information superiority and NCW

Networks allow forces to gain and exploit information leading to information superiority, but achieving knowledge superiority requires that the C2 systems are able to provide shared awareness in the cognitive domain. Shared awareness enables the execution of joint forces and operations resulting in the full spectrum dominance in the physical domain.

The original NCW paradigm has been criticized for the admiration of technology and technology-driven development. The truth is that developing the concept was guided by new technologies for a long time. However, the recent war experience by the United States has demonstrated the current technology constraints in implementing the NCW concept. A large amount of information and superior information systems did not automatically mean information superiority.

Although NCW sets high requirements for information sharing, it is still believed that information networks and services may provide superiority by enabling better situational awareness, and more effective information sharing and processing. Even though social networking and human's role have been increasing, it is still seen that information sharing and communications systems play a vital, increasing role of building networks between the actors in the battle space. The effective linking of forces means that distributed units can generate synergy, and responsibility and current tasks can be dynamically reallocated to adapt to the situation. Effective information sharing requires the establishment of a robust, high-performance information communications systems and networks that are able to provide all required services for the warfighters. [104]

2.2. Military Networking Environment

The military networks function under extreme circumstances. The networks are deployed in harsh environments where temperature, weather and other factors set high requirements for functioning. For wireless communication, the movement of troops brings a challenge with the mobility of the networks. In addition to that, the military networks are located in a hostile environment, where an active adversary is always present. Hence, for network availability and usability, it is important that the networks are well secured from external and internal attacks.

Today's military networks are more and more based on legacy commercial technologies and protocols. Military specific technology is costly, and it requires special knowledge for maintenance and configuration. However, in a situation where commercial technologies do not fulfill the high-level military specifications, some modifications and development of commercial products are conducted. Thus, commercial hardware, applications and protocols are widely used from the strategic to even the tactical level of military networking.

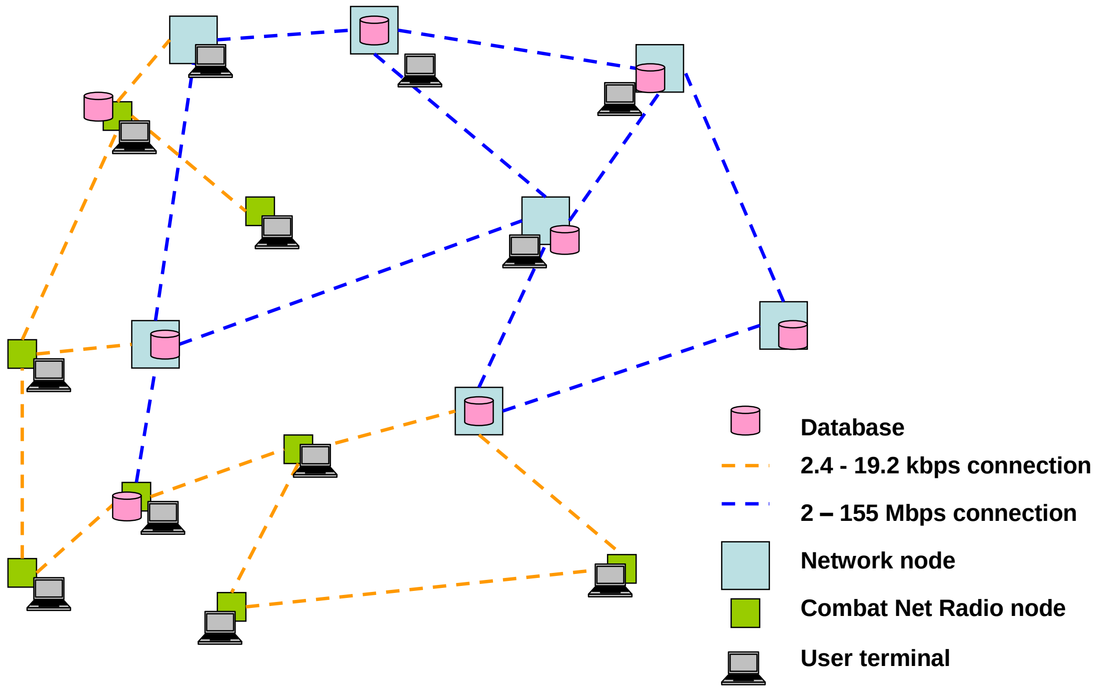


Figure 4: Characteristics of legacy military tactical networks.

For communications, the tactical environment or level of military operations is the most challenging. Figure 4 presents some fundamental characteristics of legacy military tactical networks. The network consists of nodes and communication links between them. It is essential to notice that the performance of these nodes and links is not as high as the performance of commercial or fixed networks. On the tactical level, basic communication infrastructure is based on combat network radios, mobile (typically IP) nodes and long-haul radio relays. Bandwidth capacity is low compared to commercial wireless technologies. Also, some specifications are not that important in the commercial systems.

Typically, a combat network provides the throughput of tens of kilobits per second, while the capacity of a radio relay is around two megabits per second. For example, priority features of the tactical network may cause traffic delay because data traffic on these networks may have to compete for bandwidth with other services at higher priority. Data traffic may have to unexpectedly wait several seconds or more while high-priority voice traffic is carried on the same underlying links. Such systems also may also have especially strong infrastructure protection requirements [34].

Military information services (servers and applications) are typically built using commercial technologies and products. However, some special information services are based on military specified protocols, applications and interfaces. Figure 5 illustrates a typical information service structure. The figure shows a simplified view of the many protocols that impact network communications. It is to be noted this is just a very small portion of the all available protocols and applications in use. It is important to realize that the military networks use several protocols that are also implemented in commercial networks (e.g. Internet). Each of these protocols could create cyber security problems because they are capable of being abused by potential adversaries [50].

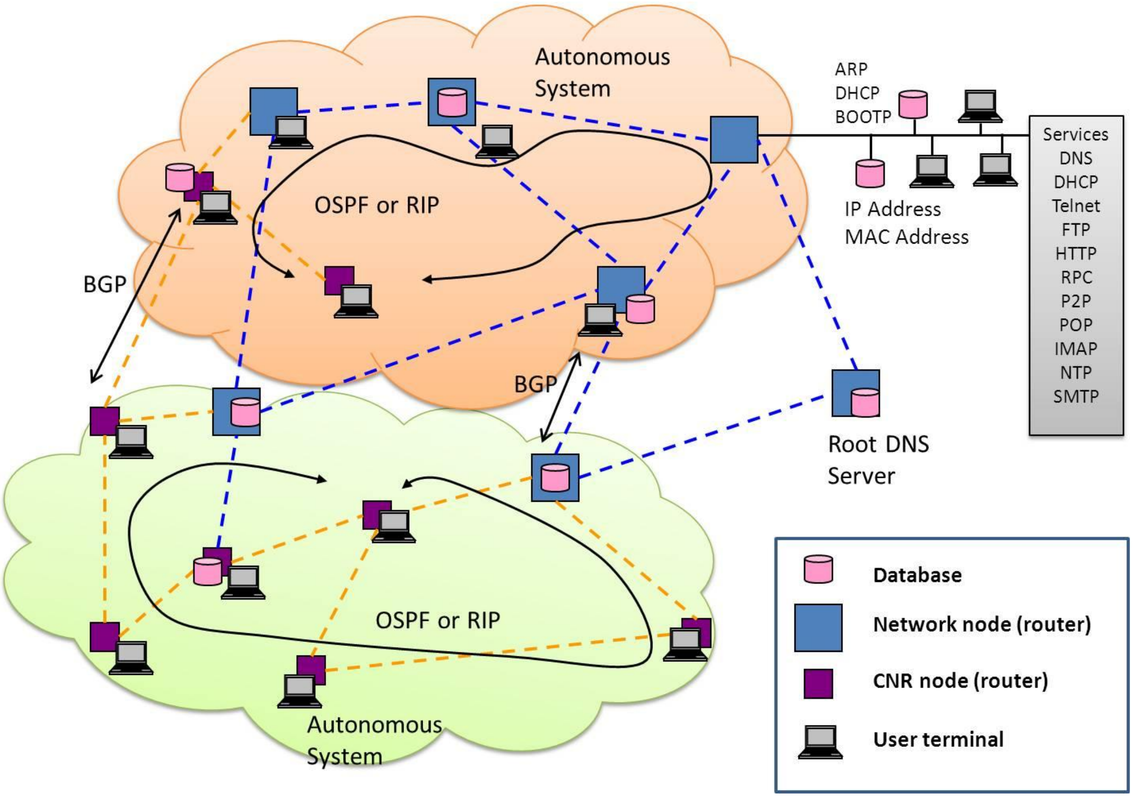


Figure 5: An example of military information service structure.

2.3. Requirements for Military Networks and Information Systems

The original NCW theory emphasizes the significance of technical networks, but, as already noted, the current theory addresses more on human dimensions and processes. Since the NCW theory was developed, current research is now aimed more towards operational management and planning processes [4], [6]. The role of information technology is to support and enable these processes. From a technology development point of view, the trend is appropriate, because the clear processes and procedures provide unambiguous requirements for technical systems. The technical systems must be adapted to the logic of modern warfare.

Figure 6 illustrates how the dimensions of NCW are associated into the requirements for the information infrastructure. The cognitive domain sets requirements of how to gain knowledge, understanding and awareness. These requirements establish demands in the information domain how battlespace monitoring and management is provided. Finally, the most of the requirements for the networks are generated from these demands of the functionality of the information system. On the other hand, the requirements for the information system are generated from the requirements that are derived from the processes and operational needs of the physical and information domains.

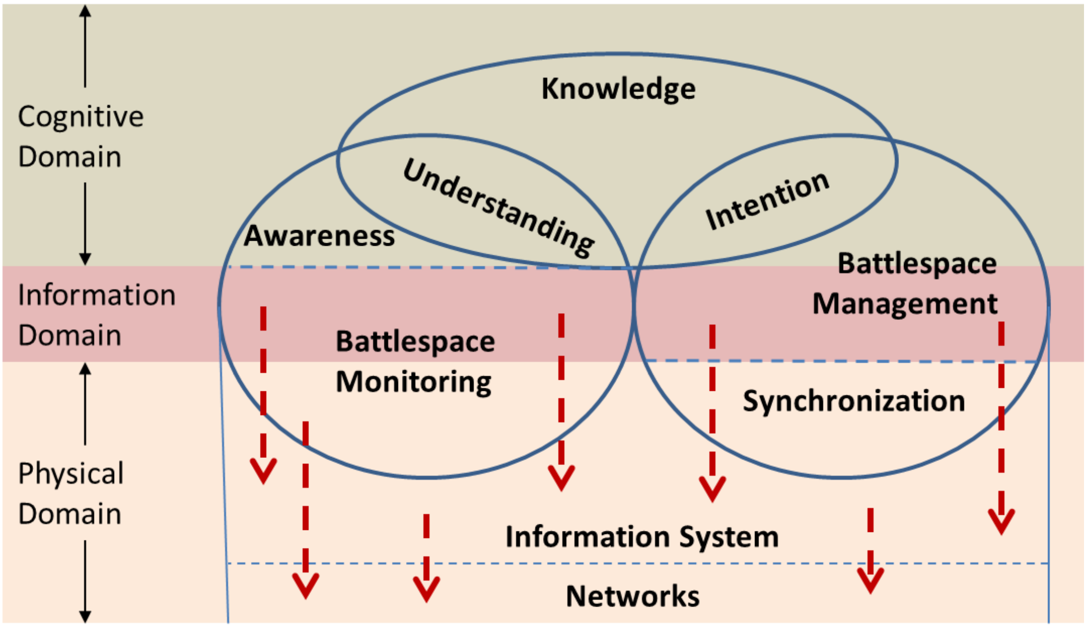


Figure 6: Deriving the requirements for the information system and networking.

The requirements of NCW for tactical military communication are challenging. The first NCW tenet [7] states that networking is the most important factor in terms of information sharing. While networking is not limited only to the technical systems and networks, it can be assumed that the technical information systems and communication networks are vital enablers to networking and information sharing, especially in distributed operations. The main purpose of networking is to build a communications system that integrates all sensors, weapon systems and operators to each other throughout the entire battlespace. In addition, military operational planning and execution requires that databases are connected into the network in such a way the data content is accessible to all stakeholders. The communication system should be able to forward information reliably throughout the battlespace from a strategic level to a tactical level.

Two case study reports by RAND Corporation [40], [74] describe five performance areas for information sharing and processing. These are Collaboration, Network Connectivity, Discovery and Collection, Network Control and Net-Ready Nodes. Two performance areas (Collaboration, and Discovery and Collection) are provided by information processing that typically occurs above the networking layer. Thus, the performance areas relevant to data transport and communication are:

1. *Connectivity Capability*. The ability of the communication network to allow warfighters and troops to transmit data and information among themselves and databases.

2. *Net-Ready Nodes Capability*. The degree of the ability to connect warfighters and troops to the network.

3. *Network Control Capability*. The ability to control and adjust the communication networks according to the mission conditions and circumstances.

Table 1 describes these previous capability areas, their factors, measures and requirements for military networking in NCW [38], [74]. The purpose of the table is to show how networking requirements are derived from three capability areas (connectivity, control and net-readiness). The requirements are derived by considering a single factor and its importance to military communications. The requirements describe very high level demands from which more detailed functional and technical requirements are derived. The technical requirements are dependent on an operational concept and use cases that exactly describe how a network system is supposed to provide communication and networking capabilities to military troops in different battlespace circumstances.

Table 1: Requirements for military networking.

Capability Area	Factor/Measures	Requirements for Networking
Network Connectivity	*Connectivity reach* - The number of network links between all operational entities required to support the ongoing mission.	Connection to all other operational entities (nodes), also during movement.
	Connectivity robustness - The number of network links that can be cut without a loss of desired reach.	A node has more than one network link. Link protocols are robust.
	Connectivity capacity. The number of required links supporting the ongoing mission with capacity that exceeds a preset threshold (kbps).	Link capacity is sufficient to run C2 applications.
	Link security. The number of required links supporting the operational function that allow for encryption.	Link security fulfills the requirements for information content (public-secret).
Network Control	*Monitoring.* The degree to which an operational function requires a network controller to detect a significant change in network status.	Network control is aware of the current status of the network.
	Access control. The amount of time in which a network controller is able to activate or deactivate network access.	Network access management occurs in (almost) real time.
	Bandwidth control. The amount of time in which a controller is able to reallocate bandwidth among the network's nodes.	Bandwidth reallocation is conducted in real time (automatically).
	Reconstitution. The amount of time in which a controller is able to find and activate alternative communications paths between disconnected network nodes.	A network system has an ability to reroute packets and establish alternative network links.
	Access security. The maximum number of network facilities that cannot be penetrated by unauthorized users.	Network devices and links are secured against unauthorized access.
	Capacity control. The amount of time in which a controller is able to add or remove a node from a network while maintaining required security and timeliness constraints.	The network system has an ability to connect and disconnect nodes automatically or with a minimum manual configuration.
Net-Ready Nodes	*Access time*. The amount of time in which a network node is connected to the network.	A node has a plug-and-play function. No manual configuration is required when the node is connected.
	Node capacity. The maximum bandwidth a network node requires being addressable by other nodes in the operation.	Capacity requirements depend on the applications running in a node. Varies from kbps to Mbps.
	Node connectivity. The number of media modes (modem, on-the move wireless, high-bandwidth wire, etc.) that are supported.	The network system must support all necessary media modes.
	Information accessibility. The number of information format types (HTML, XML, VMF, etc.) that the ongoing operation requires the nodes to support.	The network system must have common network and link protocols supporting higher level protocols (voice, video, data etc.).
	Node security. The number of nodes that the ongoing operation requires to support security requirements (encryption, ID validation, access, etc.).	All the nodes must support and use required security protocols and policies.

Networking simply consists of network nodes, links between the nodes and network management. Communication links allow the data transfer between the network nodes. From a networking point of view, the nodes are functional entities, which are able to process and share information with the other nodes, and are capable of mutual cooperation. Thus, networking simply refers to the connectivity between force entities. Two network entities are connected if either a physical or logical communications channel exists between the two. Logical connectivity denotes that the two connected entities are able to communicate directly or to communicate indirectly through some other node or nodes. When we discuss functional operations, we are normally concerned with logical connectivity. However, operational functions also require assessing physical connectivity, because no logical connection exists without a physical communication link. Connectivity requirements are a main indicator when evaluating network interaction levels.

A number of those operational entities (nodes) generating information and making decisions directly affect the level of interaction. Several units or service components may be required to work together or they can be quickly brought together temporally and spatially in order to achieve the desired effect.

Net-ready nodes are operational entities that are capable of connecting to the network to support operational functions. Equipping these players to gain access to networks can add to operational costs. Net-ready nodes, another measure of network interaction, include both the warfighters and the equipment and devices needed to access the network. The level of network readiness endures directly on the level of network interaction. Some operational functions might require very little direct access to the network while others might require considerable access. Readiness can be measured in terms of time, capacity, bandwidth, connectivity, information accessibility and level of security required for a warfighter to access the network.

The management and control of a network are extremely important to network based operations. Without some control or direction, it is impossible to simply build a network and assume subscribers to use it. This is also true for both the network infrastructure and the operational functions that use the network. Network control and management functions include monitoring changing conditions in the network, determining subscribers’ access to other subscribers and network information, resource allocation and reallocation, reconstituting the network by rerouting traffic, and enforcing security restrictions on the network.

Although a network infrastructure must be robust and reliable, it must also be dynamic so that operational actors are able to join the network. The operational actors must be equipped with devices including necessary connection capabilities. The net-ready nodes capability requires both actors themselves but also communication equipment which interoperable with the other nodes. The readiness level of the network nodes directly affects the level of interaction in the network. Some of the operational functions may require very little direct access to the network, but others may require continuous and unlimited access.

The NCW requirements culminate in the interoperability of different communication systems. The importance of the interoperability is understood when we for example look at the tasks of the Finnish Defence Forces [33]. The network system supporting the NCW paradigm should be able to connect military troops, governmental authorities and even international partners. Interoperability is a significant requirement to conduct planning and management in joint operations. NCW will bring these cooperation demands to a very low tactical level, which also requires high system and process interoperability.

Reliability and ease of use are the basic requirements for information systems and networks. If a data network is not experienced as reliable, its use can be reduced or ignored at all. Ease of use is also associated with the intensity of the network usage. Using a difficult-to-use system a warfighter may fall into learning the system instead of planning and conducting a military operation. Ease of use also covers the plug-and-play features of a network device that can speed up and facilitate network configuration and maintenance on the battlefield.

2.4. Design Goals and Security Dimensions

The purpose of security is to protect an information environment in all forms [39]. In a military context, information exposition may have greater consequences than information of other (e.g. civilian) areas. In a military environment, lives can be lost on a large scale or the balance of power can be shifted significantly. Protected information includes e.g. operations orders, war plans, troop movements, technical specifications for weapons or intelligence collection systems, identities of undercover intelligence agents, and any number of other items critical to the functioning of military and government.

In the military environment, a system wide, overall network architecture is required because the various systems, coupled with the large number of units and other stakeholders, make it difficult at times to maintain a holistic view ("big picture") while working separately [37]. During last decades, lack of an overall architecture has led to system solutions that are limited in scope, sub optimized, and not interoperable within and across military and governmental organizations and services. Similarly, lack of overall security architectures has caused challenges and problems of vulnerable, complex, poorly managed, and non-interoperable solutions. Military networking systems should be designed and implemented so that they provide battlefield networks that are highly automated, adaptive, interoperable, secure, and resilient to all types of attacks. These military networks should achieve the following goals [37]:

- Graceful degradation. Battlefield networks should be developed with a degree of fault tolerance along with the capability to degrade gracefully. The creation of critical nodes should be minimized, and move toward distributed systems. A certain level of redundancy should be built into these networks, also with all security services.

- Robustness. A natural first phase in reducing cyber vulnerabilities within a system is to enhance overall quality of software and devices. Identifying and preventing to use those products that include easily exploitable vulnerabilities will surely reduce the number of attacks. Automated tools to detect and mitigate malicious codes should be developed.

- Rapid reconstitution. Physical attacks can and often do target multiple sites which means that one backup location may be insufficient. Although diversity has benefits, recovery may be easier and faster with homogeneous, readily available systems. These two attributes must be addressed carefully. Another critical element that affects the ability to reconstruct destroyed systems is system experts with unique knowledge or experience, especially with respect to integration issues.

- Security up front. Many security vulnerabilities in both hardware and software result from inadequate consideration of security during the design process. Information technology companies must be encouraged to carry out security training for designers and software developers and improve their efforts to build in security up front.

The most common security concept presented in many references is known as the CIA triad [30], [41], [44], [84]. The security dimensions included in the CIA triad are *confidentiality*, *integrity* and *availability*. However, Whitman and Mattord [103] present four other measures which are *accuracy, authenticity*, *possession* and *utility*. These seven measures are listed in Table 2 which shows the purpose, threats and protection methods of each measure. The ITU-T X.805 [85] standard describes eight security dimensions that include some of those presented in Table 2, but the standard also introduces a few new dimensions. The ITU-T dimensions are *access control*, *authentication*, *non-repudiation*, *data confidentiality*, *communication security*, *data integrity*, *availability*, and *privacy*.

The security dimensions mean the precautionary measures taken toward possible danger or damage to information. The value of information comes from the features (equals to security dimension) it has. When a feature of information changes, the value of that information either increases, or, more commonly, decreases. Some characteristics affect the value of information to users more than others do. This can depend on circumstances; for example, timeliness of information can be a critical factor, because information loses much or all of its value when it is delivered too late. [37]

The secure dimensions provide information protection requirements for military information services and networks. It is difficult to prioritize the dimensions but information confidentiality plays a critical role in military operations. Classified information is protected by all means to keep operational intentions secret. Integrity is important when a message carries time critical, sensitive information such as firing or attacking orders. A level of required information availability may vary during the operation in according to needed services and information.

Also, some balancing between the dimensions may be required [37]. It is possible to make a system with complete availability (available to anyone, anywhere, anytime, through any means). However, such unrestricted access poses a high danger and threat to the security of the information. On the other hand, a totally secure information system would not allow anyone access to information or services. To gain balance, in which an information system satisfies both the user and the security professional, the security level must allow reasonable access, and at the same time, protect against the most likely threats.

Table 2: The security dimensions.

Measure	Purpose	Threat	Protection methods
Availability	Data can be accessed when needed to do so	Corrupt or delete data, DoS	Robust environment (system outages, communication problems, power issues) Use of redundancy and backups
Accuracy	Data is free from mistakes or errors	Data modification in all forms	Encryption (difficult to successfully manipulate data without the proper authorization) Hashes or message digests (e.g. MD5 and SHA1)
Authenticity	Data is kept authentic (data is in the same state in which it was created, stored, or transferred)	Data modification in all forms	
Confidentiality	Keeping data out of the hands of those that should not be seeing it	Information disclosure	Access controls Encryption
Integrity	Prevent data from being manipulated in an unauthorized manner	Altered to reverse their meaning or to alter the outcome of decisions based on the data in question	Encryption Hashes or message digests
Possession	Data is owned or controlled by a proper user	Data removal from the secure environment, data theft	Physical security, access control
Utility	Data has value for some purpose or end	Data modification in all forms	Encryption Hashes or message digests

From a networking point of view, availability means that end users are able to reach necessary databases and services during a mission. Availability should be guaranteed in all situations and circumstances. On the tactical level, this means that wireless links are establishes securely, and access control does not limit user access when network topologies are changing. Data accuracy and authenticity requirements are also challenging in tactical networks. Errors in data may occur due to a continuously changing network configuration. A mechanism should be implemented that guarantees a data packet arrives with no errors and modifications although the network topology was changed during transmit.

Confidentiality is typically provided by using encryption so that captured packets could not be opened by an adversary. Use of encryption is very critical in wireless communication systems, because an enemy can easily listen and record radio signals. Integrity requirements mean that data packets are not modified by an authorized user during transportation. Security functions should provide mechanisms that verify packets to include the original content.

2.5. Conclusions

In the Network Centric Warfare paradigm, the most important factor is the networking people, processes, information sources, and information. Although the main focus of NCW is not on technologies and technical networking, data communications system play a very important role as an information sharing enabler. An effective and comprehensive communication system allows fast, safe and timely information sharing between the network centric actors. Without the communications network systems the benefit of the C2 data processing systems may turn out to be minimal. A challenge is to link together the NCW actors reliably and safely, and to develop the processes and procedures of these actors to support the network centric processes. Main challenges with communications are system interoperability, communication security, information sharing policies and network management.

The tactical communication environment differs a lot from the strategic or operative level environments. From a networking point of view, the tactical environment is very dynamic compared to the higher level environments. In those static environments, connections are typically based on fixed optical fibers providing the communication speed of gigabytes per second. The networks are reconfigured using manual processes preceded by often lengthy negotiations and contracting.

At the tactical level, the rapid changes of the service requirements cause demands for the communication network's ability to adapt quickly. Thus, communication is mostly based on combat net radios to provide a reliable and rapid deployable communication infrastructure. However, the transmission speed of the combat net radios is very limited providing connections up to only hundreds of kbps. Movement of troops changes the topology of the network continuously. This sets high demands to network operators to reconfigure routing, security functions, frequency allocation, etc. Terrain obstacles and long distances between network nodes cause connectivity failings. The nodes must be operational during connection breaks by having all information required to conduct operations.

Security challenges concern electronic and cyber warfare. With electronic warfare capabilities the enemy is able to listen to and record radio signals generated by friendly forces. Thus, wireless tactical systems must have mechanisms to protect data packets that are to be transmitted in the air. Another threat is a node capture in which the enemy is able to take over a whole network node. The node should have security features that prevent the enemy to access classified data inside the node, and the features that inform the network operator about the capture. The security controls built in the node should consider all the security dimensions.

The design goals (robustness, graceful degradation, rapid reconstitution, and security) are challenging to achieve. At the same time, the network should be distributed and centralized. The network should be functional in all conditions even if it is broken into separated network segments. Services should be built so that they are distributed, but still under centralized control.

Implementing new capabilities and features increases the system complexity which grows the importance of network management. Human network operators are good in perceiving situation, but the status of a complex system could be impossible to recognize completely. Thus, automation and artificial intelligence should be used to take care of the management processes that require lots of computational capacity.

Today’s security features and performance requirements are not trivial to implement in the tactical networks. New security or communication protocols increase the overhead of data packets which cause troubles in the already narrow wireless channels. The protocols decrease the payload throughput. New security protocols should be light-weight and rather built-in to the other protocols.

All the requirements and limitations described previously must be considered when designing the cyber security architecture for the tactical military networks is started. The architecture should include the features of 1) distributed security controls 2) centralized management 3) dynamic system configuration and 4) resource-efficient functionalities.

3. CYBER SECURITY THREATS TO MILITARY NETWORKING

Cyber security threats and requirements are both extremely growing higher in societies around the world. Daily life is based on networked computers that offer a new way to do business, maintain social relationships or just share information. This high-dependence in the networks and information systems creates new opportunities also for criminals and other hostile parties. Every piece of infrastructure including a programmable microcircuit can be a potential target of a cyber attack. Thus, it is vital to consider cyber threats in a very detailed way when building a hardware or software. This chapter discusses on cyberspace as a new domain, cyber warfare, and threat and exploitation methods. The main purpose of the chapter is to define the threat scenarios for military networks. The chapter also presents the main problems and challenges in legacy military networks.

3.1. Cyberspace

Cyberspace is a key feature of modern life. Individuals, communities and even militaries connect, socialize, and organize themselves in and through cyberspace. From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people [28]. As Internet usage and networking keeps expanding, cyberspace will become the domain in which everyday life is depending across the globe.

A key character of cyberspace is the speed of events. In cyberspace, businesses trade goods and services by moving assets across the globe in seconds. In addition to facilitating trade in other sectors, cyberspace is itself a key sector of the global economy. Cyberspace has become an incubator for new forms of business, advances in technology, the spread of free speech, and new social networks. The security and effective operation of critical infrastructure including energy, banking and finance, transportation, communication, and defense rely on cyberspace of industrial control systems, and information technology that are vulnerable to disruption or cyber exploitation. [28]

It is a fact that cyberspace is full of vulnerabilities. The continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities for both defenders and attackers. Thus, it is natural that many nations are working to exploit cyberspace, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of information infrastructures. Moreover, non-state actors increasingly threaten to penetrate and disrupt networks and systems around the world. It is recognized that malicious activities that are not yet even detected may occur on networks and systems. [28]

The US National Military Strategy for Cyberspace Operations [90] defines cyberspace as the domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. The United States Department of Defense describes cyberspace as a global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Within cyberspace, electronics, and the electromagnetic spectrum are used to store, modify, and exchange data via networked systems. Cyberspace operations employ cyberspace capabilities primarily to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. [10]

United Nations (UN) states cyberspace as “the global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net.” This mostly means the Internet, but the term may also be used to refer to the specific, bounded electronic information environment of a corporation or of a military, government, or other organization. [101]

In a context of military operations, cyberspace is seen as one of five warfighting domains. The others are air, land, maritime, and space. The domains are interdependent, and cyberspace nodes physically exist in all the domains. Activities in cyberspace can enable freedom of action for war fighting activities in the other domains, and activities in the other domains can also create significant effects in and through cyberspace. Cyberspace can be viewed as three layers that are physical, logical, and social. At the same time, cyberspace is built of five components (geographic, physical network, logical network, cyber persona, and persona) [93]. The structure of cyberspace is shown in Figure 7.

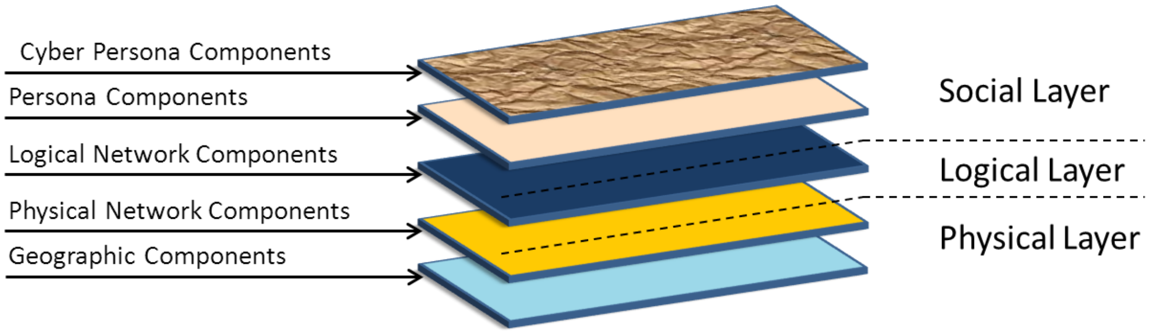


Figure 7: The structure of cyberspace (three layers, five components).[93]

The physical layer consists of the geographic component and the physical network component. The geographic component is the physical location of elements of the network. While geopolitical borders can easily be crossed in cyberspace at a rate about the speed of light, a physical aspect still ties cyberspace to the other domains. The physical network component contains all the hardware and infrastructure that supports the network and the physical connectors (e.g. cables). [93]

The logical layer includes the logical network component that consists of the logical connections that exist between network nodes. It is which technical in nature. Network nodes are devices connected to a computer network. Nodes can be computers, servers, routers, personal digital assistants, cell phones, or various other network appliances. [93]

The social layer contains the human and cognitive aspects and includes the cyber persona component and the persona component. The cyber persona component includes a person’s identification or persona on the network (e-mail address, computer IP address, cell phone number, and others). The persona component includes the people actually on the network. A single person can have multiple cyber personas (e.g. different e-mail accounts on different computers) and a single cyber persona can have multiple users (e.g. multiple users accessing a single service account). This holds important implications for military forces in terms of attributing responsibility and targeting the source of cyber action. This also means that military forces need significant situational awareness, forensic, and intelligence capabilities to counter the complex cyber threat. [93]

Table 3 lists the major characteristics of cyberspace. The three first characteristics of cyberspace consider cyberspace from a human action perspective [53]. People use cyberspace for social interaction, search information and virtually manage and conduct their daily routines such as shopping, finance and reading newspapers. The last three characteristics are more related to the technical features of cyberspace. As it is known, events occur very fast in cyberspace. In theory, the maximum speed of data is limited to the speed of light (at least in near future). Thus, in practice, communication and interaction takes place in real time. The global Internet has no spatial boundaries. A global routing system guarantees that everyone has access to all places in the world (to where the Internet reaches). Cyberspace is a space in which we have no “distances” between actors. All the actors are the same distance away.

Cyberspace is a very complex environment. There were over 2.2 billion Internet users in 2011 [80]. Several Internet users have more than one device to connect the Internet which makes the number of devices very high. To provide Internet access, network operators around the world need to have global communication infrastructures. The end result is a huge complex ecosystem, serving billions of people 24 hours every day.

Table 3: Characteristics of cyberspace.

Characteristic	Description
Virtuality	A person can make electronic personality. People can take part in activities on cyberspace.
Interaction	People share their ideas and information for business or private. Social interactions include chatting, online gaming, and social media.
Information source	Internet resources are open to everyone. Everyone can also be an information creator.
Speed of events	Events and transactions occur at almost the speed of light which makes cyberspace different from the physical space.
No spatial boundaries	The global network is not limited by spatial boundaries such as national borders. Everyone has mainly access to all other addresses on Internet.
Complexity	The ecosystem of cyberspace is very complex to perceive and understand completely. Monitoring and management of cyberspace is challenging.

3.2. Cyber Warfare

Cyber warfare is unlike traditional warfare, but it shares some characteristics with the historical role of aerial bombardment, submarine warfare, special operations forces, and even assassins. Specifically, it can inflict painful, asymmetric damage on an adversary from a distance or by exploiting the element of surprise.[39] The term warfare is strongly connected to the military perspective. However, it could be benefit to expand the perspective, because commercial and civilian communications systems are connected to the same battlefield on which the nation states are fighting [10].

Cyber warfare is also defined as actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption [16]. Cyber warfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. A challenge is that no legal entity known as cyber war exists. The only issue that has been well-defined by international agreement is a nation’s right to self-defense when attacked, and that applies only to the traditional manner of attack, i.e., “armed” attack. [16]

Figure 8 illustrates how cyber warfare is related to cyber network operations, cyber situational awareness and cyber support activities [93]. Cyber Situational Awareness (CyberSA) is the instant knowledge of friendly, enemy and other relevant information regarding activities in cyberspace. Awareness gained by combining intelligence and operational activities in cyberspace and in the other domains. CyberSA enables informed decision-making at all levels via flexibly tailored products and processes that range from general bulletins to extremely sensitive and classified tools and services. CyberSA enables and derives from Cyber Network Operations, Cyber Warfare, and Cyber Support as depicted in Figure 8.

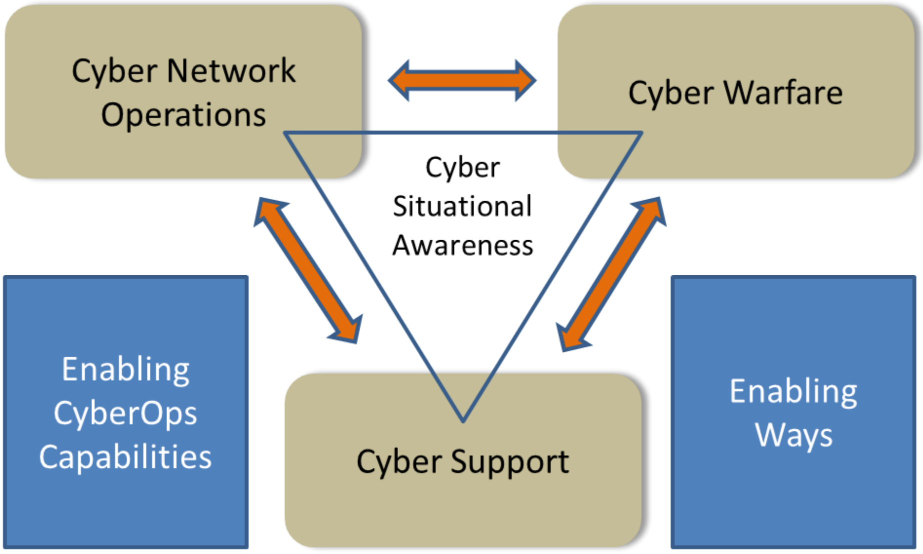


Figure 8: Cyber warfare related to the other components of cyber operations [93].

Cyber Network Operations (CyNetOps) is the component that establishes, operates, manages, protects, defends, and commands and controls networks, critical infrastructure and key resources. CyNetOps consists of enterprise management, cyber content management, and cyber defense, including information assurance, computer network defense with response actions, and critical infrastructure protection. CyNetOps supports Cyber Warfare by providing information for offensive operations. [93]

Cyber Warfare (CyberWar) is the component that extends cyber power beyond the defensive boundaries of the operational networks to detect, deter, deny, and defeat enemies. CyberWar capabilities are used against computers, communication networks, embedded processors and microcircuits in equipment, systems and infrastructure. CyberWar is conducted through cyber exploitation, cyber attacks, and dynamic cyber defense which combines highly automated processes (sensors, intelligence analysis, etc.) to identify and analyze malicious activity, simultaneously executing response actions to defeat attacks before they can affect. [93]

Cyber Support (CyberSpt) is a varied collection of supporting activities which are created to specifically enable both network operations and cyber warfare. These activities are called-out in this unifying category due to their unique and expensive nature as high-skilled, low-density, time-sensitive/intensive activities requiring specialized training and processes. Additionally, some of these activities also require specialized coordination, synchronization, and integration to address legal and operational considerations. CyberSpt activities are carried out by multiple stakeholders. Examples of support activities contain vulnerability assessment, threat-based security assessment, reverse engineering and law enforcement-based cyber forensics. [93]

Enabling Cyber Operations Capabilities include activities that enable cyber operations in certain conditions. An example of this is electronic warfare (EW) that must be deconflicting, fully coordinated, and synchronized with CyberOps. Enablers improve the effectiveness and integration of military capabilities and their consequent effects. Enabling ways improve the effectiveness and integration of cyber operations capabilities. Cyber operations require continuous actions taken to form the operational environment and set the conditions to be successful to operations. Law and policy set limitations on what can be conducted operationally and feed the development of rules of engagement (ROE). [93]

3.3. Cyber Threats and Exploits

Threat is a function of an enemy’s motivation, their capabilities, the opportunity, and the impact that a successful attack on a target [12]. Motivation is considered to be identification of both the reason why somebody would start attacking and a measure of the degree to which the attack would be conducted to the end. Table 4 categorizes potential attackers by their motivation. The attackers can be divided into five groups that are criminals, hackers, nations, terrorists and activists. The table shows the more detailed description of the motivations and activities of each group.

Capability is defined as power to do something [12]. In terms of cyber warfare the term capability is used as a measure of the availability of different tools and techniques to conduct an attack and the ability to use the tools and techniques correctly. Capability also includes the availability of training and education to support the efficient use of the tools and weapons. In other words, capability can be seen as the degree to which the attacker is able to implement a threat.

Opportunity is defined as a favorable occasion for action. An attacker must have correct conditions before attacking. The target must be in a vulnerable condition so that the adversary's capabilities are effective and have correct impact on the target. The term impact is used to represent the concept of effect that an attack can gain against a target system. The measurement of the attack can be made in direct or indirect terms.

Table 4: Potential attackers and their motivations. [25]

Attacker	Motivations/Activities
Criminals	Criminal groups seek to attack systems for monetary benefit. Typically, organized criminals use spam, phishing, and malware to conduct identity theft, online fraud, and computer extortion.
Hackers	Pure hackers break into network systems for the thrill of the challenge and bragging rights in the hacker community. Decades ago, unauthorized access required a fair amount of skill or computer knowledge, but today hackers can use several advanced attack scripts and protocols.
Nations	Nations use cyber weapons alongside with conventional weapons. Several nations are working to develop cyber warfare strategies, doctrine, and capabilities. Cyber capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures around the globe.
Terrorists	Terrorists want to destroy, damage, or exploit critical infrastructures in order to threaten national security, cause casualties, affect the economy, and damage public morale and confidence. Terrorists use different schemes to achieve monetary gain, to gather sensitive information or to damage critical infrastructure.
Activists	Cyber activist use cyberspace to achieve their political objectives. Activists use several activities to affect political decision-makers. These activities vary from information publication to large scale denial-of-service attacks.

Cyber based threats are evolving and growing and arise from a wide array of sources. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. [25]

According to the desired effect, cyber attacks can be categorized into three basic forms from which all others derive [39]. *Confidentiality* attacks comprise any unauthorized acquisition of information, including undisclosed information analysis in which an attacker gathers traffic content. Because global network connectivity comes a way before network security, hackers can easily steal huge amounts of information. *Integrity* attacks include the unauthorized modification of information. Attacks can contain the disruption of data for criminal, political, or military purposes. Confidentiality and integrity attacks are penetration attacks that involve breaking into a system using known security vulnerabilities to gain access to target resources.

The goal of *availability* attacks is to prevent authorized users from accessing into the systems or data that is required to conduct operations. Attacks are commonly described as a Denial-of-Service (DoS) attack and cover a wide range of malware, network traffic, or physical attacks on computers, databases and the networks that connect them. The purpose is to affect the system through diminishing the system's ability to function.

A large variety of cyber exploitation and attacking techniques and methods are found in literature, and thus it is not possible to explain all of them in the scope of this research. In Table 5, the most common attack types and exploits are described. The purpose of the table is not to give the complete list of attacking methods, but rather show how complex and multidimensional the cyber threat is. One must also remember that different methods can be used together, and the boundaries between the attack and exploit types are not always very tight and well-described.

It is obvious that security threats and attacks may involve any layer, from physical to the application. It is possible that a successful attack in one layer may appear useless against the security measures in the other layers [30]. On the other hand, some advanced attacks utilize vulnerabilities from many layers and protocols, and thus make the attack difficult to detect and protect by legacy devices (firewalls, IDSs, IPSs, etc.). A good example of these advanced hacking methods exploiting combination of different vulnerabilities and weaknesses is advanced evasion techniques (AETs) [64].

Evasion techniques are a means to disguise cyber attacks in order to avoid detection and blocking by information security systems. Evasions enable cyber criminals to deliver malicious content to a vulnerable system without detection that would normally stop the threat. Network security systems are ineffective against evasion techniques in the same way a stealth fighter can attack without detection by radar or other similar defensive systems. [64]

Table 5: Types of cyber exploits and attacks [25], [41], [103].

Exploit/attack	Description
Malicious code	The malicious code attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information. The state-of-the-art malicious code attack is the polymorphic or multivector worm.
Hoaxes	A more devious attack on computer systems is the transmission of a virus hoax with a real virus attached. When the attack is masked in a seemingly legitimate message, unsuspecting users more readily distribute it.
Backdoors	Using a known or previously unknown and newly discovered access mechanism, an enemy can gain access to a system or network resource through a backdoor. Sometimes these entries are left behind by system designers or maintenance staff.
Password crack	Attempting to reverse-calculate a password. A cracking attack is a component of many dictionary attacks (to be covered shortly).
Brute force and dictionary attack	The application of computing and network resources to try every possible password combination. The dictionary attack is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random word combinations.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Spoofing	Spoofing is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host.
Man-in-the-middle	In the well-known man-in-the-middle or TCP hijacking attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network.
Spam	Spam is unsolicited commercial e-mail. While many consider spam a trivial nuisance rather than an attack, it has been used as a means of enhancing malicious code attacks.
Mail bombing	Another form of e-mail attack (also a DoS) is called a mail bomb, in which an attacker routes large quantities of e-mail to the target.
Sniffers	A sniffer is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information.
Cross-site scripting	An attack that uses third-party web resources to run script within the victim’s web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data while they are being transmitted over a communications link. Wiretapping is done without altering or affecting the data.
Social Engineering	The target of Social engineering is to attack the human element of a system to gain sensitive information or access to target systems.
Pharming	In Pharming, traffic is directed to an illegitimate site for the purpose of obtaining private information. Pharming often uses virus technologies to attack the Internet browser’s address bar so that the valid URL typed by the user is modified to that of the illegitimate web site.

Advanced evasion techniques can be identified according to certain underlying principles:

- Delivered in a highly liberal way
- Security devices are designed in a conservative way
- Use of rarely used protocol properties
- Use of unusual combinations
- Craft network traffic that disregards strict protocol specifications
- Exploit the technical and inspection limitations of security devices: memory capacity, performance optimization, design flaws, etc.[64]

3.4. Threat Scenarios for Military Networks

In many cases, threat scenarios in the military environment vary from those concerning the civilian or commercial networking environment. In the military environment, a hostile adversary attempts to affect information and network infrastructures to prevent the normal use of information services. The enemy may use electronic warfare capabilities, physical effects, or cyber weapons to disturb network and service availability or steal and modify critical information.

The threat scenarios to military information systems can be examined in the following four areas [37]:

- Physical attacks on critical information and networking nodes
- Electromagnetic attacks against information assets
- Cyber attacks against information systems
- Attacks and system failures made possible by the increased level of complexity inherent in the variety of advanced systems.

Physical attacks and effects are still seen as important means of attack to affect the information processing and sharing of the opponent’s force. Physical (kinetic) attacks can use low technology but still be highly effective. Critical network nodes, satellite ground stations, server centers, and other dedicated military and commercial infrastructure can be attacked directly with high explosives or other physical means to disrupt information processing and sharing, and thus, entire military operations. Also, if enemy forces capture one of the many computers in the future battlefield, and possibly along with the legitimate user, the adversary may be able to access the battlefield networks and C2 systems, and use the captured node to disrupt operations by cyber attacking.

Electromagnetic threats cover a wide range of possible weapons that includes the means of directed energy such as electromagnetic pulse (EMP) and electronic warfare. EMP weapons can destroy or injure electronic systems without physical attack or explosives. Electronic warfare (EW) systems utilize the electromagnetic spectrum, and they can be used to deny the use of sensors and radio frequency communications. Typical EW means include jamming, and signal intelligence and positioning.

Cyber attacks are attractive because they can be launched from remote locations, offering the hostile attackers a degree of anonymity and safety. Advanced attackers can hide their tracks and make it challenging to identify not only who the attacker is but also from where the attack was launched.

The quantity and sophistication of the information technology introduced will increase significantly the level of complexity. From a technical point, as the complexity increases, the networks become less reliable and less predictable. Systems that are appropriately complex can allow unexpected interactions of failures. If the information systems are tightly coupled, they can permit failures to cascade, sometimes enough to bring down the entire system. This chain of unexpected events can be started by hardware failure, natural hazards, or, in the case of military operations, a cyber attack on the system.

From a cyber security architecture point of view, the area of cyber attacks is the most interesting, and the main purpose of the security architecture is to provide necessary security controls to protect against cyber attacks. However, the other areas must be also considered because they may have indirect effects to the architecture. For example, the threat of node capture sets requirements to security controls to prevent the misuse of a captured node.

In this study, the cyber threat scenarios on communication networks can are considered by analyzing the objectives of a cyber attack and the ultimate outcome the attack may have. The objectives are in line with those attack categories presented in the previous chapter. The effects of cyber attack align generally into four threat scenarios based on the attacker's ultimate purpose [24]:

1. Integrity Violation. Data integrity is a basic security requirement for end users, but it is also very critical for military operations. If the loss of data integrity is not corrected, continued use of the corrupted data could result in inaccuracy, fraud, or incorrect decision-making or operation of information systems and networks.

2. Prevention of Availability. If a mission-critical network is attacked and all services are made unavailable to its end users, the mission or operation will most likely be affected. Loss of system functionality and operational effectiveness may result in loss of productive time, or military decision-making.

3. Confidentiality Violation. Successful military operations require high information confidentiality. Information services and networks should provide appropriate confidentiality services so that operational data is kept secret as desired. Communication channels, data processes and databases must be secured against untrusted parties.

4. Physical Destruction. Physical destruction is conducted by using cyber weapons or traditional explosives. Physical destruction requires positioning of target systems. Cyber weapons can be use supervisory control and data acquisition (SCADA) systems that control for example airspace, water systems or power plants.

In each threat scenario, several exploits and attack techniques are utilized depending on available tools, a structure of the target system, and overall operational design. The exploits may be used in different phases of a cyber attack process. Typically, a cyber attack consists of five main phases [49]; *reconnaissance*, *penetration*, *privilege escalation*, *malicious activity*, and *covering trails*. The phases are illustrated in Table 6 that presents the attack phase for each scenario. It is remarkable that all the five phases may not exist in all the threat scenarios.

The first phase of an attack is reconnaissance of the target system. By observing the normal operations of a target, useful information can be discovered and collected. This information includes such as installed hardware and software, regular and periodic communications traffic, and the formatting of communications.

The second phase is penetration. To achieve a desired effects the attacker must be able to enter into the target system. However, penetration is not required when the purpose is to disrupt the availability or access to a given service provided by the target. During the third phase, the attacker identifies and expands the internal capabilities by viewing resources and increasing access rights to more restricted and critical areas of the target system.

Table 6: The main phases of a cyber attack.

Scenarios	Phase 1 Reconnaissance	Phase 2 Penetration	Phase 3 Privilege escalation	Phase 4 Malicious activity	Phase 5 Covering trails
Integrity Violation	Information collection of a target's security controls and application protocols.	Entering into the target system.	Increasing access rights to get access to information or processes.	Violating data or a process. Modification of data or a process.	Hiding the trails of the penetration and violating/ modification.
Prevention of Availability	Information collection of a target's application protocols.	May not be necessary for availability prevention.	May not be necessary for availability prevention.	Crashing or flooding services (protocols).	Hiding traffic sources and control nodes.
Confidentiality Violation	Information collection of a target's security controls and service protocols.	Entering into the target system.	Increasing access rights to get access to information or processes.	Stealing or disclosing information. Decrypting secret information.	Hiding the trails of the penetration and information disclosure.
Physical Destruction	Information collection of a target´s information locations and physical protection.	Physical penetration e.g. by special force operations.	May not be necessary in physical destruction.	Destruction using kinetic or non-kinetic (e.g. High Pulse Microwave) weapons.	(Hiding physical trails.)

The fourth phase includes the actions by which the attacker's cyber weapon damages the target system, or steals or modifies selected data and/or information. In the last phase, the attacker removes all the evidences of the penetration, theft, and modifications. The attacker electronic trail can be covered by editing or deleting log files and other data files including user or access information.

During an attack, the attacker wants to complete all these five phases successfully. However, the conducted phases are dependent on the type of attack method utilized, the desired goal, and the target's individual defensive capabilities. For example, armed forces may not have any reasons to hide trails in war time operations when both parties are heavily involved with full war fighting.

Table 7 depicts cyber attack threats included in different phases of each threat scenario. The attacker may exploit several vulnerabilities and attack tools to achieve the desired end state. The table shows the typical threats that are relevant for each scenario concerning military communications especially on a tactical level where a high risk of a node falling into enemy hands is present. On the other hand, wireless connections that are widely used in the tactical environment are facilitating the adversary to collect information from radio signals. We should notice that Table 7 is not a complete list of all cyber threats against tactical networks. Cyber threats may rapidly change over time, and new attack techniques and tools are to be developed all the time. The purpose of the table is to determine a threat scenario reference that could be used for the evaluation of the cyber security architecture (see Chapter 6).

3.5. Security Challenges with Legacy Military Networks

This section examines the implementation of current military ICT systems and technical challenges and problems in a changing threat environment. The oldest military C2 systems still in use were built up in the 80's when the security threats were totally different. Typically, the military communication networks were isolated example from the networks of commercial operators. The systems were simple compared to today’s technologies and implementations, and the networks and services were often built for a single functionality or service. A security level of information defined the level of implementation. The security protection in the systems was largely based on physical protection, because the military information systems and networks were not connected to other networks and systems. Thus, the main threat was a hostile actor who could import a malicious code to this closed system causing interference or break-outs in a target system.

The aim of this section is not to describe all the possible problems and challenges of existing military communication systems, but rather focus on the four entities which the author believes the most weaken the current security level of the legacy military communication systems. The entities to be reviewed are static configuration, lack of light-weight security protocols, centralized security services and overall security management.

Table 7: Cyber threats for the threat scenarios of military networking.

Threat Scenario	Threat	Description
Integrity Violation	Control message alteration	An attacker intercepts control messages in the middle of communication entities and alters certain information to reroute traffic or change control information.
	End-user data alteration	An attacker manipulates an end-user's data packets or files. Unauthorized modification, deletion, creation, and replication of end-user data.
	Configuration alteration	An attacker alters information in network configuration files.
	Node capture	An attacker captures a network node and uses it for violating information content or system processes.
	Routing violation	An attacker modifies routing information packets and thus prevents a node to reach correct destinations.
Prevention of Availability	Flooding	An attacker generates a huge traffic load that prevents authorized users to access services.
	Node capture	An attacker captures a network node preventing end-users to access services.
	Malformed control messages	An attacker injects malformed control messages that cause the loss of service availability.
	Connection hijacking	An attacker hijacks a communication connection and prevents an authorized user to access services.
	Quality-of-Service abuse	An attacker modifies QoS control messages providing the degradation of service level.
	Server impersonating	An attacker captures an information server, and closes services.
Confidentiality Violation	Node capture	An attacker captures a network node disclosing end-users or network control data.
	Exploitation of software vulnerabilities	An attacker exploits known or unknown software or hardware vulnerabilities to discovering unauthorized data.
	Masqueraders	An attacker uses stolen access information for authorized access.
	Unauthorized user activity	An attacker manages to access unauthorized data because of poor protection.
	Unprotected network access	An attacker uses unprotected access points to entering the network and data.
	Unprotected data links	An attacker taps to an unprotected data link.
	Eavesdropping end-user data	An attacker is able to eavesdrop the transferred end-user data.
	Traffic tracking	An attacker captures network traffic, and is able to locate communication nodes and to examine e.g. network topology.
	Eavesdropping control messages	An attacker captures control messages, and is able to examine used communication and security protocols.
Physical Destruction	Kinetic destruction of a critical network service	An attacker uses kinetic force to destroy a node that is critical for network services (e.g. routing), leading to loss of data transport.
	Kinetic destruction of a critical network node	An attacker uses kinetic force to destroy a node that is critical for data transport between a server and client.
	Kinetic destruction of a critical control node	An attacker uses kinetic force to destroy a node that is critical for network control and management.
	Non-kinetic destruction	An attacker uses non-kinetic weapons to destroy a network node.

Static Configuration

Today, legacy military networks and information systems use static configurations to provide desired services to end users. Configuration files are once loaded into the systems, and no modifications are made until the service requirements have been changed enough. Thus the current day military network is static in nature, and it is not aware of its state at any point of time [97].

Reconfiguration is provided manually by a network operator. Traditionally, network service production and management involves complex labor intensive processes performed by these network operators. The systems are configured according to service level and security requirements. A problem is that especially the security requirements change continuously and often very rapidly. A cyber threat environment reshapes fast due to the discovery of new vulnerabilities and the development of hacking techniques.

Lack of Light-Weight Security Protocols

All communication protocols create overhead to communication channels. Certain bits are required for the protocols, and thus they decrease the number of payload bits in each packet. Similarly, security services are not resource-free as security protocols consume valuable system resources including such as bandwidth, memory, processing power and battery power in mobile devices (e.g. tactical radios, soldier’s terminals). Thus, tactical-level devices cannot implement system programs with high computational requirements. Providing tactical military networks with appropriate security services must be resource efficient [2].

Several security protocols and algorithms have been discovered to solve the security issues of mobile wireless systems. Typically, security services are added on legacy military networks afterwards by implementing existing solutions to the wireless, tactical environment. The existing solutions are not designed for the tactical environment causing performance reduction [3].

A good example of a security protocol causing a significant overhead is the Internet Protocol Security (IPsec) suite for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet of a communication session. The IPsec encryption solution decreases a maximum throughput especially at smaller packet frame sizes. At 512-byte, 1024-byte and 1280-byte frame sizes, approximately 100% the maximum theoretical throughput was achieved. However, at 256-byte frames, the performance was just 73 %, and at 128-byte frames it dropped down to 47%. Finally, at 64-byte frames the performance was approximately 27% of the maximum theoretical throughput. [99]

Centralized Security Services

Many security services are today based on centralized service structures in which the security services are produced in a single location. In a case of fixed networks and locations, this may not be a problem as long as a user is able to be connected to these centralized services. The centralized service production has lots of benefits such as easier management, need for less network operators, and the cost-effective maintenance of infrastructure.

Most of the legacy military networks are still dependent on the centralized security services such as authentication and authorization. For example, in centralized networks, the network is governed by a trusted third party - a central entity providing security certificates which is trusted network wide [56]. The central certificate source is not relevant for the today’s tactical networks which are desired to operate autonomously, and therefore, to be equally responsible for different types of security functionality, such as user access, node admission, or revocation.

The centralized security service structure weakens reliability of the network. By affecting a single server or database an attacker may prevent services to be accessed. Legacy systems include firewalls and IDS/IPS systems to filter traffic and prevent malicious data to reach the target service or application, but in a case of advanced DDoS the reconfiguration of system parameters and restoring service availability may take a moment [103].

Lack of Overall Security Management

Security management of the military communication networks is both technical and administrative security process including security policies and controls. Security management also includes monitoring and evaluation of effectiveness of the security policies and controls. The most effective method to fulfill the security requirements is to create a risk assessment process involving the entire network from security policies to a single security component. Therefore, security management by itself remains very complex. [54]

With the legacy military networks the management process should cover all the layers and entities of the network. However, the reality is often different as the oldest tactical network systems were built decades ago without an overall sight to network security. Security management functions and processes have been implemented along with new network components and features without considering the overall security management in each updating phase. Different applications may have separated access-granting and restricting policies and methods. The criteria on which access decisions are based may vary vastly among different services or systems or even between different instances inside the same application [54].

Traffic Flow Confidentiality

Traffic flow confidentiality is even more critical in tactical networks where communication links are wireless, and thus easy to eavesdrop. Traffic flow refers to the information that can be observed by looking at the traffic flow rather than the information content within the payload of the transferred packets. Traffic flow can expose that there is data communications, the volume of communications, and the traffic sources and destinations. Traffic flow can be protected by using encryption at the lowest layer of the OSI stack, and simultaneously padding data flow so that the link always seems to be fully utilized regardless of the actual traffic rate. [103]

The legacy military networks lack of traffic flow confidentiality. Various encryption schemes have been implemented, but they typically encrypt only a user payload, and in some cases also network control traffic. The legacy systems are not capable of generating bulk traffic to fill silent periods in traffic flows

3.6. Conclusions

Cyberspace is growing all the time. New devices and systems are connected to the Internet every day. Computers and microcomputers are installed in places that seemed to be utopia a few decades ago. People's daily life is increasingly dependent on the Internet; servers, computers, and networks that link all them together. Business actors, different organizations, governments and also defense forces rely increasingly on computer networks and services. It is difficult to conduct daily business without networked ICT services.

Cyberspace is easy to access and even operate. Access to cyberspace requires only a laptop with a wireless or wired Internet connection. In cyberspace, a person can be anonymous if necessary. An actor may have a number of cyber persona roles. Hiding attack trails is easy, and the trails often disappear before the origin of an attacker is reached. On the other hand, cyberspace is still very dependent on the physical world. Cyberspace does not exist without physical devices; computers, routers, optical fiber cables, wireless base stations and server with databases.

Cyber warfare has become a new dimension for warfighting. In the past, the motivation of actors in cyberspace consists of pure mischief, political extortion and criminal monetary gain. Today, cyberspace is used as a battlespace for nations which develop furiously intelligence, monitoring, protection and offensive cyber capabilities. Cyber warfare must be considered carefully in the development of new military information systems and networks.

From perspective of a cyber security architecture, the cyber threats are challenging. Current threat scenarios contain a number of methods to attack the target against the system. The target of an attacker varies which affects what vulnerabilities and tools are exploited and used during the attack. The threat is continuously changing at a high speed. Attackers are constantly seeking new vulnerabilities, which they are going to exploit at the right moment. A challenge with today’s ICT systems is that the more complex the systems become the more attack vectors and surfaces they offer to the attacker. A complex infrastructure is difficult to maintain updated and patched in real time.

The task of the security dimensions is to describe the security requirements set for information. When developing a network security architecture these requirements must be taken account. The security dimensions concern information content, and thus military network capabilities should be design and implemented so that processed, transported and stored information is secured throughout the network in all conditions.

Battlefield conditions cause high requirements for the performance of tactical networks. The communication network must be secure, but also reliable and recoverable at the same time, and it must provide the necessary services to warfighters in very difficult environmental conditions. Network nodes must be mobile offering secure C2 services in all situations. Besides of the rough conditions the hostile enemy is always present on the battlefield seeking to influence continuously on the opponent's communications network and its services.

A security architecture design should respond to the threat in the best possible way. The architecture should be design to protect against the threat scenarios described above. The architecture should provide sufficient security functionalities and controls that could be dynamically controlled in order to adapt network configuration in different combat and threat situations. The architecture should allow the flexible modification of the security functions according to the changing threat scenarios. This requires constant updating of a threat library and software controlled security controls.

Security services in legacy military networks are more or less implemented with the mainstream and commercial technologies which create challenges in security management and availability. Many of the security services are provided by centralized servers that do not support node mobility at the tactical level very well. The security protocols used in the systems are originally designed for fixed environments where network capacity is much higher than in tactical networking systems. Amount of a security protocol overhead is not very critical in broadband connections, but in low bandwidth tactical radio networks the issue becomes vital. The currently used military information systems are based on static configuration causing a network node or server to be a moving target for the enemy.

Security management is lacking an overall view within the legacy systems. Security controls are managed and controlled separately generating for example a risk of unknown role combinations that may create new vulnerabilities in the system. Privacy issues are typically considered carefully in the legacy systems but traffic flow confidentiality is not at the satisfactory level. Due to the above-mentioned weaknesses, designing a new security architecture is very relevant. The new architecture allows the construction of security services and controls to an integral part of the military communication system.

Impact of cyber threats on the security architecture can be summarized in four points. First, the architecture must support changing threat scenarios. As the threat model changes, security controls described in the architecture have to adapt to the prevailing environment. Secondly, the architecture must take into account the defense in depth because it is impossible to build one hundred percent secure and invulnerable systems. With a layered approach, system penetrations by the enemy can be confused and slowed down. By monitoring the different layers an intruder can be detected in time to start counter actions. Third, military communication networks must fulfill the requirements for information protection which vary according to classification and different levels of security. An end-user must be able to trust the network, also from a security point of view.

Fourth, the network cyber security related functionalities must be automated as much as possible. Rapidly changing threats require a network operator to reconfigure network parameters fast and continuously. A risk is that manually provided changes increase the number of configuration errors. On the other hand, a human operator may not notice the complete status of the network and current threats when the network is monitored with manual methods. Using automated security controls the security processes and functions of the network could be speeded up and improved in quality. However, it is good to remember that a human being still has a unique ability to understand the cause-and-effect relationships in complex situations and environments.

4. COGNITIVE NETWORKS

In recent years, terms *cognitive* and *smart* are strongly related to computer networks and communication systems, but these terms are not often defined very accurately from a communication networks perspective. However, it is generally understood that the above terms describe the ability of technology to adapt to changes in the environment [95]. By a definition described by Thomas, DaSilva and MacKenzie [95], cognition refers to consciousness and its content as a whole. Consciousness is associated with the ability to observe and analyze the environment, think, reason and solve problems.

This chapter introduces the cognitive networks, and presents the main features of these networks. The chapter also discusses the new security threats concerning the cognitive networks. The aim is to show how cognitive capabilities could improve military communications networks, especially from a security point of view.

4.1. Cognitive Networks Overview

The basic functions of the cognitive networks include observation, learning, decision-making, self-management, and automatic configuration [58]. Thomas et al [94], [97] describe cognitive networks as:

”A cognitive network is a network with a cognitive process that can perceive current network conditions, and then plan, decide, and act on those conditions. The network can learn from these adaptations and use them to make future decisions, all while taking into account end-to-end goals.”

The cognitive aspect of this description is similar to those used to describe a cognitive radio and broadly includes many simple models of cognition and learning. Unlike cognitive radios, cognitive network do not restrict its scope in radio spectrum. CN tries to exactly perceive the current network situation and plan and decide to meet the end-to-end goals in an entire network aspect. CN learns through this adaptation and uses information of these previous actions in future decisions. As new aspects, the definition introduces the terms network and end-to-end goal. Without the network and end-to-end approach, the system may only perform as a cognitive device or network layer, but not as a cognitive network in a wide scale.

In the definition, end-to-end represents all the network elements involved in the transmission of a data flow. In military communications, this includes e.g. the tactical radios, radio relays, routers, switches, virtual connections, encryption devices, interfaces, or wireless waveforms. The end-to-end goal which is typically defined by a client-server type of service, gives a cognitive network its network-wide scope. This separates the scheme from other adaptation approaches, which usually have a scope of single element, layer or resource.

4.2. Cognitive Process

A cognitive process in the cognitive networks could be viewed as the commonly known OODA loop [13], in which the network observes, orients, decides and acts. Figure 9 shows the phases of the OODA loop in context of cognitive networking. The observation phase is critical because the effect of a cognitive network's decisions on the network performance depends on how much network state information is available. If a cognitive network has knowledge of the entire network's state, cognitive decisions should be more "correct" than those made in ignorance. For a large, heterogeneous system such as military tactical networks, it is unlikely that the cognitive network would know the total system state. It could be very high costly to communicate status information beyond those network elements requiring it, meaning CN will have to work with less than a complete picture of the network resource status.

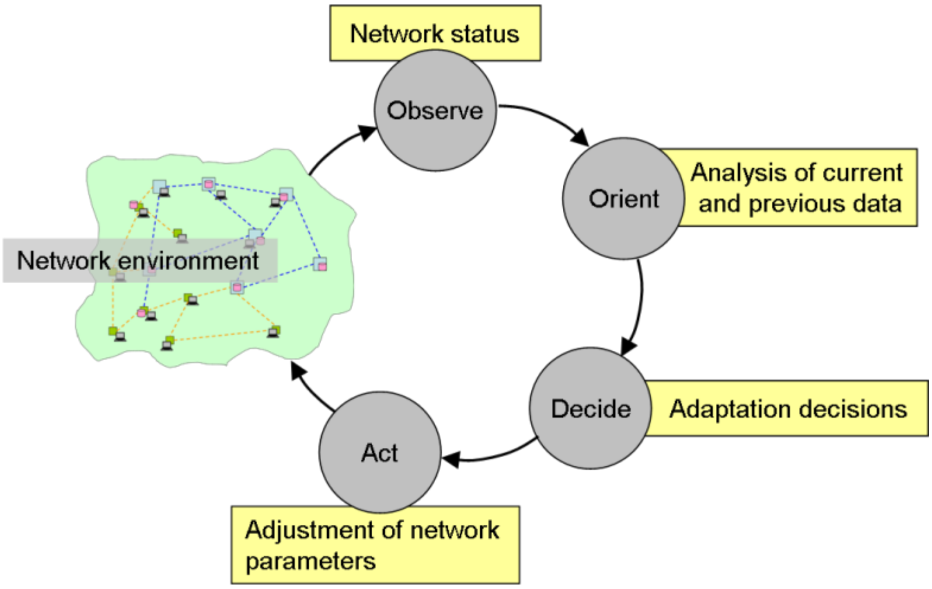


Figure 9: The OODA loop in context of cognitive networking.

The orientation phase also plays an important role in the cognitive process. In this phase all observed information and previous knowledge are added together and analyzed. Filters and weighting are examples of methods used in the orientation phase. In the decision phase, the best decision for the required end-to-end data flow capability is made. Learning is an important part of the orientation phase, because it can prevent the recurrence of past mistakes in future decisions.

Finally, a network adjustment is provided in the acting phase. The adjustment includes modifications and reconfiguration of cognitive network elements. The network elements are also allowed to act selfishly and independently (in the context of the entire network) to achieve local goals, but the local goals must be resulted from the end-to-end goal. The actions taken have straight effect to the observed environment or network state, thus a feedback loop is created in which past interactions with the environment guide current and future interactions.

4.3. Cognitive System Framework

Figure 10 illustrates a cognitive system framework [97] which consists of three functional levels. The end-to-end level includes applications, users and resources which form the end-to-end goals to be achieved at an appropriate service level. The cognitive level consists of three components: the specification language, cognition layer, and network status sensors. These components provide the actual intelligence of the cognitive level, and allow the level to interface with the configurable network elements and the users and applications on the end-to-end level.

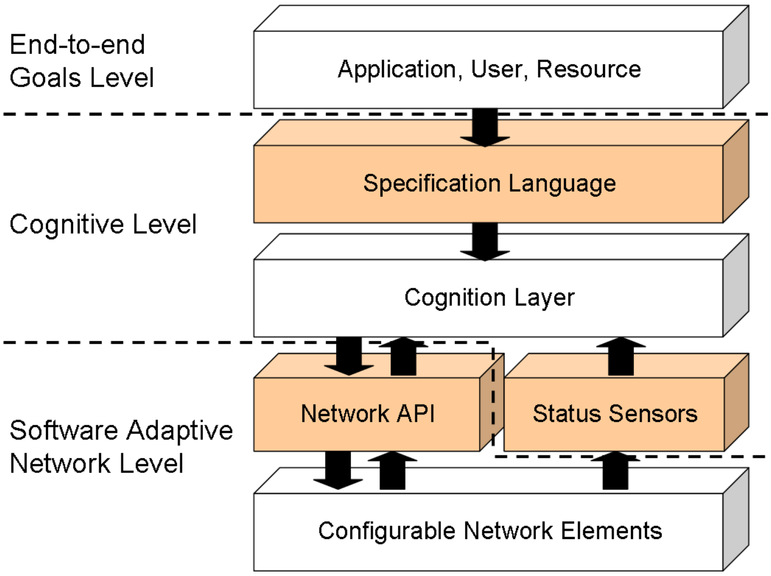


Figure 10: A cognitive system framework.

For connecting the top level requirements to the cognitive level, an interface layer must exist. Information about the goal must not be globally known, but needs to be communicated between the source of the requirements and the local cognitive processes. Other requirements for the specification language include at least support for distributed or centralized operation including the sharing of data between multiple cognition layers. The specification language does not actually perform the cognitive process which is done by the cognition layer, but the language is required to translate application level requirements for the cognitive layer.

The cognitive process of the network can be either centralized or distributed. In the military environment, the requirements for high-resilience mean that each node should be able to maintain a cognitive process, providing an argument against the centralized solution. The cognition layer contains the cognitive element of the framework. Typically, cognition is provided through various machine learning algorithms as neural networks, genetic algorithms, artificial intelligence, Kalman filters and learning automata algorithms [94]. The network status sensors provide feedback from the network to the cognition layer, and the sensors also allow the cognition layer to observe patterns, trends, and thresholds in the network for possible action. To be able to report a connection status the cognitive layer must have an ability to manage the sensor. The sensor layer is also capable to distribute their information to the entire network.

The software adaptive network layer consists of the network application programming interface (API) and configurable network elements. The network API provides a generic interface to adjust network parameters according to actions decided by the cognitive layer. Another responsibility of the API is to notify the cognitive network of what the operating states of the network elements are. Many modifications to the network stack require that all the links and nodes are synchronized and operating in the same mode. The communication required to synchronize these states is the responsibility of the software adaptive platform and could be realized either in or out of channel.

4.4. Characteristics of Cognitive Networks

The basic assumption is that the cognitive network provides better end-to-end performance than traditional, non-cognitive communication networks. Cognitive processes improve network resource management, quality of service (QoS), security, access control, and many other network-determined objectives [96]. The performance of the cognitive networks is only limited by the adaptation ability of the network elements. An ideal cognitive network functions proactively rather than reactively so that adaptation takes place before actual problems appear.

Cognitive networks have three basic characteristics: situational awareness, learning and decision-making abilities, and fully controlled network parameters and settings [58]. Situation awareness is generated through network's ability to observe the environment and the state of the network, and thus to form “understanding” of external and internal conditions. For network optimization, it is important that the network nodes share their status information with other nodes. In cognitive radio networks, an important factor is the ability of sensing the electromagnetic spectrum in place or time to find free radio channels. Learning consists of a network's ability to learn from past events, and decision-making is the ability to make decisions based on situational awareness and learning.

During the learning and decision-making process, network node behavior can range from purely selfish and individualist to social and unselfish. Although the selfless and social behavior may seem natural for the end to end requirements, the selfish behavior can sometimes be more effective while adapting the network [94]. Selfish behavior of the network may be reasonable, because in real world communication systems nodes are often not under a global management system. In addition, the selfish node requires less centralized coordination, thereby reducing control traffic overhead. Selfishness can be considered with Equation (1) [95], [96]. An action *a* of a network node is selfish when the utility u_i for element *i*, as a result of this action, given that every other element plays the actions that element *i* believes them to, is no less than the current utility u_i for element *i*.

$$u_i(a_i^{t+1}, a_{-i}^{\sim t+1}) \geq u_i(a_i^t, a_{-i}^{\sim t+1}) \tag{1}$$

The *belief* in Equation (1) is important, since ignorance may make this vector different than the actual strategies the other elements are employing. The network shows the feature of *selfishness* when every network element plays a selfish strategy, meaning that all cognitive elements only select actions that continuously improve their individual objectives.

An unselfish network attempts to meet the end-to-end requirements. An objective function, called *cost* (detonated *C*), quantifies the performance of a network in achieving the goals for a specific action vector. This function is determined from the objectives of the network and, unlike the utility function, is enhanced as it is decreased.

An action is *unselfish* when an element sacrifices its utility to decrease the cost function. The network activity is unselfish, when the following are valid [96]:

$$\begin{array}{l} u_i \;\; a_i^{t+1}, a_{-i}^{\sim t+1} \;\; < u_i \;\; a_i^t, a_{-i}^{\sim t+1} \\ C_i \;\; a_i^{t+1}, a_{-i}^{\sim t+1} \;\; \leq C \;\; a_i^t, a_{-i}^{\sim t+1} \end{array} \tag{2}$$

The network can be said to function *unselfishly*, where at least one of the nodes operates unselfishly in some point of the decision chain.

Decision-making based on the information is not always complete, and information gaps must be considered in decision-making. The lack of information may mean that the nodes do not know the precise objectives or use of the other nodes. Variable Y_i is defined as the set of signals that cognitive element i observes to learn about the actions of all elements in the network (including itself). The probability that action a was the action given that y_i belongs to Y_i was observed is denoted by $P[a|y_i]$. The feature of *ignorance* [94], [96] occurs when at any stage in the decision sequence an ignorant decision is made. An ignorant decision occurs when a cognitive element has partial knowledge. This means for some *i* that there exists an

$$ay_i \in Y_i\ such\ that\ P\ \ \mathrm{a}\ y_i\ \ < 1 for\ all\ \mathrm{a} \in A \qquad (3)$$

Ignorance occurs when at least one cognitive element in the decision sequence makes an ignorant decision.

When the network operates under fully observable actions, and has the feature of *knowledge*. A knowledgeable decision occurs for some *i* when there exists an

$$\mathrm{a} \in A\ such\ that\ P[\mathrm{a}|y_i] = 1\ \ for\ all\ \boldsymbol{y_i} \in \boldsymbol{Y_i} \qquad (4)$$

Full knowledge occurs when all elements make knowledgeable decisions at every stage in the decision sequence.[94], [96]

Fully controllable or partially controllable network elements are essential for cognitive network to gain maximum performance. In an ideal situation, all the network elements and parameters are controlled by the cognitive layer. In this case, the network can be optimized for each situation or end-to-target perfectly. For a cognitive network with *k* instances of the functionality in the network, and *x* instances of the functionality under cognitive control, *partial control* [96] occurs when

$$\frac{x}{k} < 1 \qquad (5)$$

For a cognitive network with *k* instances of the functionality in the network, and *x* instances of the functionality under cognitive control, *full-control* [96] occurs when

$$\frac{x}{k} = 1 \qquad (6)$$

4.5. Security Threats to Cognitive Networks

Security of the cognitive networks is widely researched and discussed [15], [17], [20], [62], [77]. Although, the most of the traditional cyber threats (e.g. TCP/IP threats, man-in-the-middle, etc.) are valid, cognitive networks also face some unique security challenges not faced by conventional wireless or wired networks. In an ideal CN, security of the network is provided as a result of a cognitive process, which generates new threats. For instance, incomplete situation awareness or a disturbed decision-making process may lead to the decision not to use any security controls for certain communications although it is extremely required.

Table 8 presents three new cyber security threats related to cognitive networking. The first column of the table describes the threats that are sensor input violation, information sharing violation and data storage attack. In the second column, description is given, and the third column states the implication when the threat has been triggered.

Table 8: Major security threats in cognitive networks.

Threat	Description	Implication
Sensor Input Violation	Sensor data is altered by an attacker or other means	Learning and decisions are made according to false SA which results faulty performance.
Information Sharing Violation	Information sharing between network nodes is damaged	SA of the surrounding environment is false.
Data Storage Attack	Data storages are injured	History data, as a basis for decision-making, is incorrect.

In the cognitive network, locally-collected and exchanged information is used to construct a perceived information environment that will influence both current and future behaviors. By violating sensor data, information sharing and history data (databases), an attacker is able to change the information environment. Training with the incorrectly perceived environment will cause the CN to adapt incorrectly, which affects short-term behavior. Unfortunately, the CN uses these adaptation experiences as a basis for new decisions. Thus, if the malicious attack perpetrator is clever enough to disguise their actions from detection, they have the opportunity for long-term impact on behavior. Furthermore, the CN collaborates with its fellow nodes to determine behavior. Consequently, this provides an opportunity to propagate behavior through the network in much the same way that a malicious worm.

One of the main security concerns in CNs is an attacker spoofing faulty sensor information causing a network node to select an undesired configuration. By manipulating the receiving information the attacker can feed faulty statistics data to be stored in the knowledge database of a network node. Further decisions based on the current situation and information in the knowledge database may not be optimal as the stored information is not valid.

Ensuring security of information sharing between cognitive nodes will be vital. To function optimally the nodes of cognitive network must exchange lots of control information. Corrupting control data causes a reduced capability to optimize network behavior within all the other nodes in the network. A single node may still be able to make optimal decisions, but cognitive behavior is limited to the single node. In that case, the cognitive network no more exists.

4.6. Conclusions

The cognitive networks create a new perspective to the development of military communications systems. In the future, the cognitive networks will offer better possibilities to support the high requirements for battlefield communications. From a technical performance point of view, four value-added factors can be highlighted. The first factor is time. A cognitive, self-adaptive network is able to respond quickly to the required network changes, primarily caused by the movement of troops and individual soldiers, and by establishing situational awareness and C2 capabilities on the battlefield. Cognitive networking can reduce the delay of manual network planning and configuration. Faster network convergence accelerates the deployment of tactical networks, and thus information sharing between the troops and actors.

The second factor is the interoperability of heterogeneous communication system devices. Achieving the maximum effectiveness of NCW the full interoperability between the actors' networking systems, interfaces and protocols is required. Interoperability is a key for today's joint operations where military services and branches conduct operations side by side. Cognitive, software-programmable network devices allow adaptation of networking protocols and parameters. For example in radio networks, this means that waveforms can be modified in such a way that the nodes do not interfere with each other. The cognitive process allows the actors equipped with different types of systems to communicate with the others. Improved interoperability enhances also reachability of network nodes. The more nodes are compatible the wider area of network coverage can be obtained. The gateways between cognitive network elements are transparent which enables information transfer between the network elements, and thus the quality of information can be maintained at the high level.

The third factor to which cognitive networking affects in the network infrastructure is more efficient use of network resources. In tactical military networking, this particularly means the efficient utilization of electromagnetic spectrum. Legacy tactical combat radios utilize the frequency spectrum only partially. The cognitive radio network is able to identify and utilize unused parts of the spectrum. In the future, dynamic spectrum usage will be an important capability as the number of wireless devices keeps growing. The effective use of network resources is not limited to the efficient use of spectrum, because the cognitive network is able to utilize available bandwidth capacity, security controls and other resources. The efficient use of network resources also means that information services do not allocate too much network capacity or resources.

From the perspective of this thesis, security as the fourth factor is the most interesting. In theory, a cognitive system is able to take into account all the security requirements throughout the entire communication network. The network is able to adapt its security mechanisms and parameters according to the end-to-end-goals derived from security policies. The network adapts automatically to the desired security level, which minimizes security vulnerabilities caused by human errors and omissions. The cognitive process can control and monitor overall security instead of having separated management processes for each security control.

The cognitive networks introduce promising features to support and enhance security of tactical military networks. However, we must remember that when a communication system becomes more and more complex, a number of vulnerabilities in the system increase. The cognitive process, control channels, input sensors and additional databases are new targets for the enemy, and they open new attack surfaces to be exploited.

5. CYBER SECURITY ARCHITECTURE

The main purpose of this chapter is to present an overview and comprehensive description of the cyber security architecture and the functionalities of the architectural elements and layers. Describing the functionalities of the architecture excludes technical details such as protocols and algorithms, because the overall purpose of the architecture design is to define the functional elements. The presented architecture is built to meet the requirements and conditions set out in the previous chapters. After presenting the overview of the architecture, each element of the architecture and their tasks are defined in more details.

Before the actual presentation of the architecture, different types of security architecture models and frameworks are reviewed in the beginning of the chapter. The purpose is to prove that existing models and frameworks fit poorly into describing a cyber security architecture for tactical military networks. Thus, the proposed architecture is described as a layered functional block diagram without a tight coupling to the reviewed models.

5.1. Security Architecture Frameworks and Models

Security architecture can be defined as the design artifact that describes how the security controls and security countermeasures are positioned, and how they relate to the overall information technology architecture. These controls serve to maintain the system's security quality attributes which typically are confidentiality, integrity, availability, accountability and assurance services. [71]

The purpose of the network security architecture for cognitive military networks is to reduce security risks according to risk analysis and security policies. It is not possible to create an architecture having no holes, and trust in the provided security mechanisms in all battle space conditions. Thus, the focus is on reduction risks and enforcing policy through the design and configuration of network equipment. Traditional network security design and architectures have focused on creating a secure network perimeter around the organization placing security devices and controls at the point where the network is connected to the other networks or the Internet. Especially in military networks, the isolation (no connection to any other networks) was a key deign factor for decades. [57]

An architecture framework is used for an architecture design. The architecture framework [1] establishes a common practice for creating, interpreting, analyzing and using architecture descriptions within a particular domain of application or stakeholder community. Typically an architectural framework consists of a standard set of views, which each have a specific purpose.

Lots of different architecture frameworks have been developed [88], but most of them have a scope on enterprise and business level architectures. These frameworks present design models for generating layered architectures supporting enterprise and business process. Information sharing is a key issue with these enterprise level architecture frameworks, but not too many of them discuss on communication networks or network security although security is somehow considered at least on high level.

An enterprise information security architecture framework is only a subset of enterprise architecture frameworks. Figure 11 simplifies the conceptual abstraction of a high-level conceptual security architecture framework within a generic enterprise information framework [32]. Security is connected to all three architectural areas. At the business architecture, security concerns policies and rules, and at the information architecture, the goal is to ensure secure data processing. At the technology architecture, security must ensure that applied technological solutions support security requirements and goals.

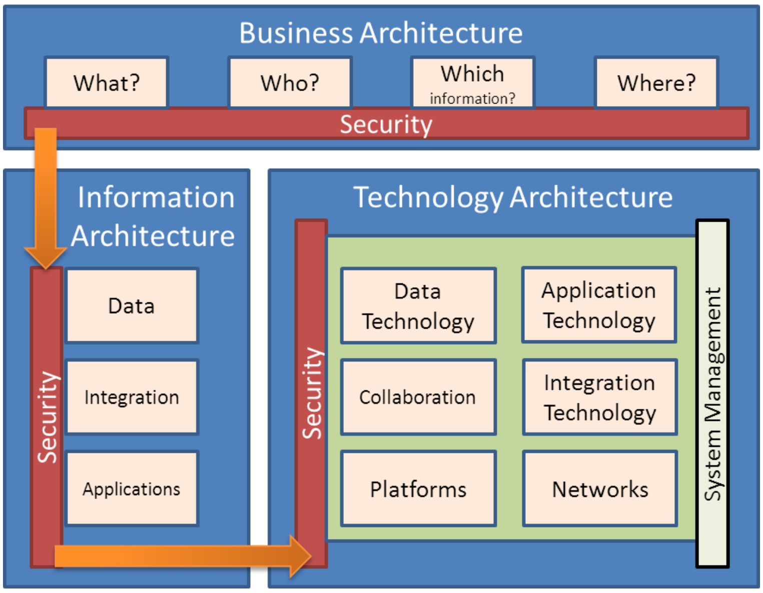


Figure 11: High-level conceptual security architecture framework.

iCode Security Architecture Framework [44] developed by iCode Information Security is one of the attempts to provide an architecture framework including all required security controls whether they were procedural or technical. The purpose of the framework is to help organizations prevent damages to assets by building security controls blocks and deliver a layered protection against the perceived cyber threats with a cost effective implementation.

The iCode framework covers the three fundamental tenets of information system security; confidentiality, integrity and availability. The framework also includes three information system dimensions that are the business, the information, and the technical dimensions. In the framework, standards play a significant role and provide guidance and interchange capabilities of elements within the architecture. [44]

iCode Enterprise Security Architecture Framework is illustrated in Figure 12. The technical viewpoint includes conceptual, logical and implementation levels. At the implementation level, the technical reference model sets boundary conditions for security functionality and technologies. Then, security controls are figured within three architectures: security infrastructure, security services and application security.

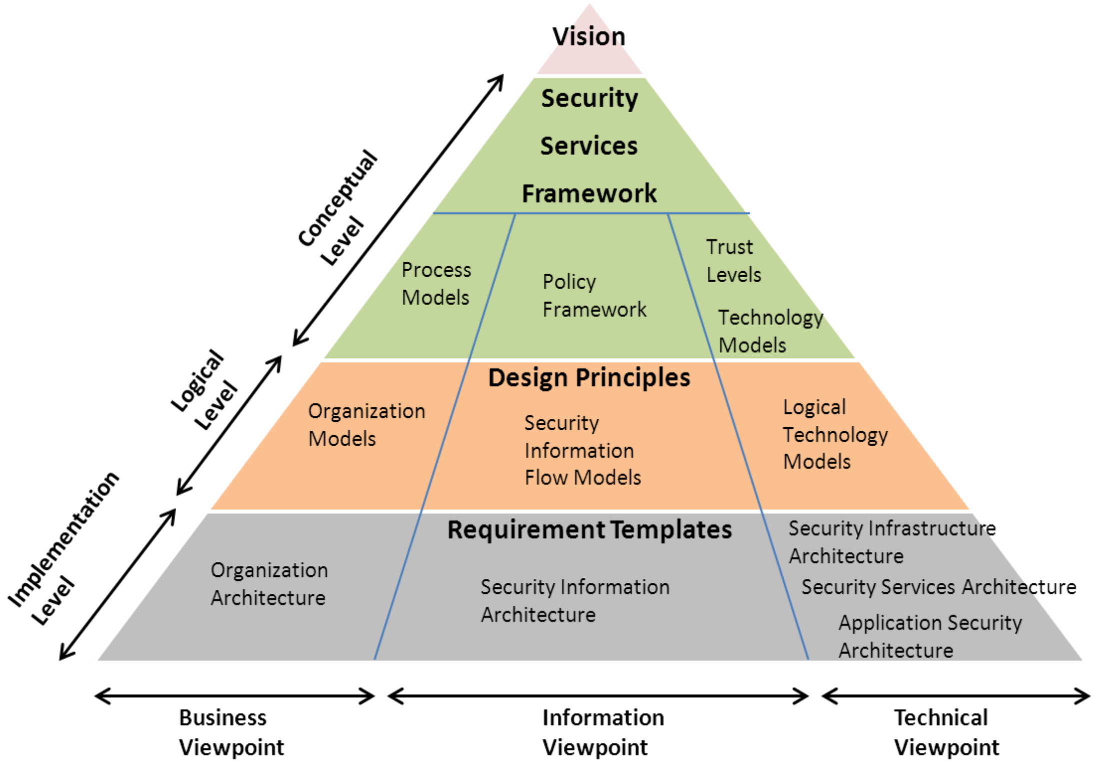

Vision
Security Services Framework
Conceptual Level
Process Models
Policy Framework
Trust Levels
Technology Models
Logical Level
Design Principles
Organization Models
Security Information Flow Models
Logical Technology Models
Implementation Level
Requirement Templates
Organization Architecture
Security Information Architecture
Security Infrastructure Architecture
Security Services Architecture
Application Security Architecture
Business Viewpoint
Information Viewpoint
Technical Viewpoint

Figure 12: iCode Enterprise Security Architecture Framework.

Sherwood Applied Business Security Architecture (SABSA) [86] is a model and a methodology for developing a risk-driven enterprise information security architecture. The goal of the architecture is to deliver security infrastructure solutions that support critical business initiatives. The main feature of the SABSA model is that all functionality must be derived from an analysis of the business requirements for security. Especially, the business areas in which security has an enabling function for new business opportunities.

The SABSA process analyzes the business requirements at the outset, and develops a chain of traceability through the strategy, design, implementation and lifecycle to ensure that the business opportunities are maintained. Practical experience is a basis for framework tools that further support the whole SABSA methodology. The SABSA model is generic and can be the starting point for any organization. By going through the process of analysis and decision-making implied by its structure, the architecture becomes more specific to the organization, and finally, the architecture is highly customized to a unique business model. [86]

The SABSA uses a layered model in which the top layer consists of the business requirements. On the way to the bottom layer, a new level of abstraction and detail is developed. The process goes through the definition of the conceptual architecture, logical services architecture, physical infrastructure architecture and finally at the lowest layer, component architecture with the selection of technologies and products. The service management architecture connects these five architectures as depicted in Figure 13. [86]

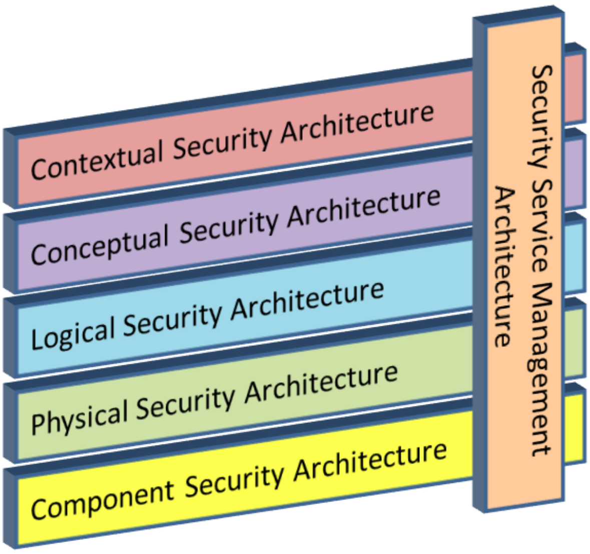

Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

Figure 13: The SABSA layered model for security architecture.

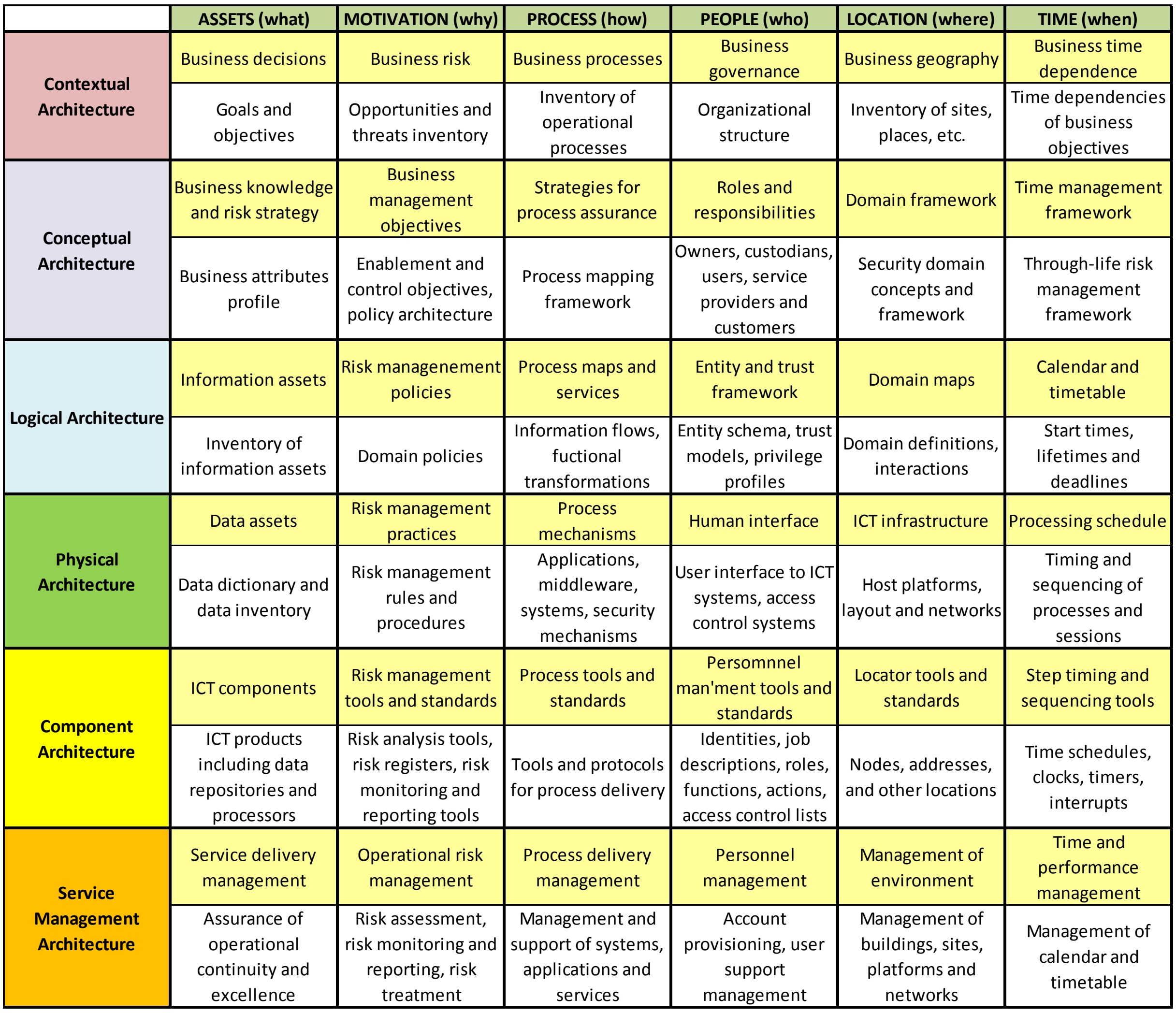
In the SABSA model, each horizontal architecture layers (illustrated in Figure 12) have also vertical cuts that answer the questions [86]:

- What are we trying to do at this layer? (protect assets, data, etc.)
- Why are we doing it? (motivation)
- How are we trying to do it? (processes and functions)
- Who is involved? (people and organizational aspects of security)

- Where are we doing it? (locations where to apply security)
- When are we doing it? (time-related aspects)

These six vertical architecture elements are combined with six horizontal architecture layers which create a six by six matrix of cells representing the whole model for the enterprise security architecture. The table is called the SABSA Matrix that in shown in Figure 14. The SABSA developing process is a process of describing all of these thirty-six cells of the table. The SABSA Matrix also provides two-way traceability. The matrix allows tracing every requirement through to the components that provide a solution when the fulfillment of the requirements is considered. On the other hand, the matrix can be used to check the relevance of each security component at the bottom layer. A single component requirement can be traced all the way back to the top layer of the business requirements that describe the specific solution.

We can also find a few defense related architecture frameworks such as MODAF (UK Ministry of Defence Architecture Framework) [61], DoDAF (US Department of Defense Architecture Framework) [29] and NAF (NATO C3 Systems Architecture Framework) [66]. These frameworks include little about security issues, and once security is taken account it is presented at a very high level. MODAF and DoDAF are discussed more in details in the following sections.



	ASSETS (what)	MOTIVATION (why)	PROCESS (how)	PEOPLE (who)	LOCATION (where)	TIME (when)
Contextual Architecture	Business decisions	Business risk	Business processes	Business governance	Business geography	Business time dependence
	Goals and objectives	Opportunities and threats inventory	Inventory of operational processes	Organizational structure	Inventory of sites, places, etc.	Time dependencies of business objectives
Conceptual Architecture	Business knowledge and risk strategy	Business management objectives	Strategies for process assurance	Roles and responsibilities	Domain framework	Time management framework
	Business attributes profile	Enablement and control objectives, policy architecture	Process mapping framework	Owners, custodians, users, service providers and customers	Security domain concepts and framework	Through-life risk management framework
Logical Architecture	Information assets	Risk managenement policies	Process maps and services	Entity and trust framework	Domain maps	Calendar and timetable
	Inventory of information assets	Domain policies	Information flows, fuctional transformations	Entity schema, trust models, privilege profiles	Domain definitions, interactions	Start times, lifetimes and deadlines
Physical Architecture	Data assets	Risk management practices	Process mechanisms	Human interface	ICT infrastructure	Processing schedule
	Data dictionary and data inventory	Risk management rules and procedures	Applications, middleware, systems, security mechanisms	User interface to ICT systems, access control systems	Host platforms, layout and networks	Timing and sequencing of processes and sessions
Component Architecture	ICT components	Risk management tools and standards	Process tools and standards	Persomnnel man'ment tools and standards	Locator tools and standards	Step timing and sequencing tools
	ICT products including data repositories and processors	Risk analysis tools, risk registers, risk monitoring and reporting tools	Tools and protocols for process delivery	Identities, job descriptions, roles, functions, actions, access control lists	Nodes, addresses, and other locations	Time schedules, clocks, timers, interrupts
Service Management Architecture	Service delivery management	Operational risk management	Process delivery management	Personnel management	Management of environment	Time and performance management
	Assurance of operational continuity and excellence	Risk assessment, risk monitoring and reporting, risk treatment	Management and support of systems, applications and services	Account provisioning, user support management	Management of buildings, sites, platforms and networks	Management of calendar and timetable

Figure 14: SABSA matrix (the whole model for the enterprise security architecture).

The Department of Defense Architecture Framework (DoDAF) [29] is an architecture framework for the United States Department of Defense that provides structure for a specific stakeholder concern through viewpoints organized by various views. These views act as mechanisms for visualizing, understanding, and assimilating the broad scope and complexities of an architecture description through tabular, structural, behavioral, ontological, pictorial, temporal or graphical means. The framework is especially suited to large systems with complex integration and interoperability challenges, and is apparently unique in its use of "operational views" detailing the external customer's operating domain in which the developing system will operate. The DoDAF viewpoints are presented in Figure 15.

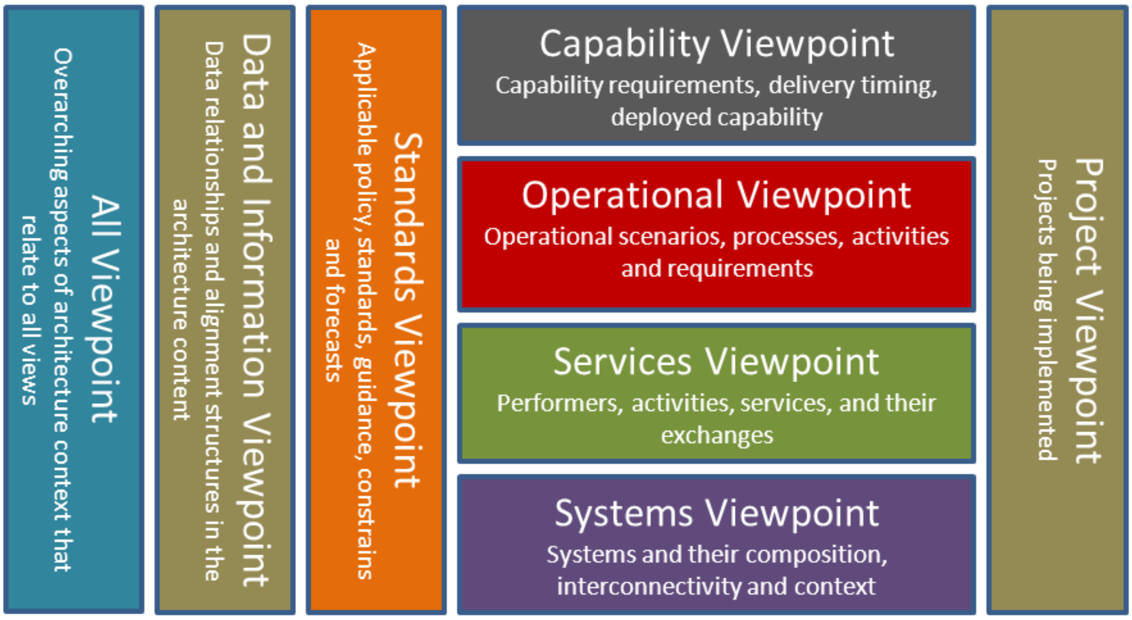

All Viewpoint
Overarching aspects of architecture context that relate to all views
Data and Information Viewpoint
Data relationships and alignment structures in the architecture content
Standards Viewpoint
Applicable policy, standards, guidance, constrains and forecasts
Capability Viewpoint
Capability requirements, delivery timing, deployed capability
Operational Viewpoint
Operational scenarios, processes, activities and requirements
Services Viewpoint
Performers, activities, services, and their exchanges
Systems Viewpoint
Systems and their composition, interconnectivity and context
Project Viewpoint
Projects being implemented

Figure 15: The DoDAF viewpoints.

The current version of the DoDAF treats security as any other requirement. The DoDAF does not contain any separated security-specific viewpoint. Security information can be presented on models using annotations and call-outs. The DoDAF model comprises the concepts, associations, and attributes for capturing and representing security characteristics in a consistent way between models. A formal processing of security features is important because many of the artifacts such as nodes, interfaces, systems have several security requirements. Some of the items decomposed in the architecture are actually security implementations (e.g. authentication). Also, some components cannot function without security.[29]

The DoDAF model is effective at mapping operational activities to systems, but capturing and modeling security threat and attacks or their countermeasures is not easy using the framework. Attempting to detach security features into other activities is challenging, especially when it appears that many of the activities themselves are enabled or protected by security mechanisms. For example, modeling confidentiality is difficult while it causes activities in almost every other activity. [26]

MODAF [61] is an internationally recognized enterprise architecture framework developed by the United Kingdom Ministry of Defence (MOD) to support defense planning and change management activities. Originally the purpose of MODAF was to provide an accurate structure to support the definition and integration of MOD equipment capability, particularly in support of Network Enabled Capability (NEC). MODAF was developed from the previously introduced DoDAF, but has been extended and modified to meet UK requirements by the addition of Strategic, Acquisition and Service Oriented Viewpoints. The MODAF viewpoints are quite similar to the DoDAF viewpoints. The viewpoints are [61]:

- Strategic Viewpoint (desired business outcome, required capabilities)
- Operational Viewpoint (processes, information and entities needed to fulfill the capability requirements)
- Service Orientated Viewpoint (services required to support the processes described in the operational views)
- Systems Viewpoint (physical implementation of the operational and service orientated views)
- Acquisition Viewpoint (dependencies and timelines of the projects that will of deliver the solution)
- Technical Viewpoint (standards that are to be applied to the solution)
- All Viewpoint (description and glossary of the contents of the architecture).

As in the DoDAF model, MODAF includes no security view. Security information can be shown on views using annotations and call-outs similarly to DoDAF. Furthermore, some add-ons have been developed to the framework to support security aspects. For instance, a model library provided with the MODAF Meta-Model underpins the representation of security characteristics in a consistent way between models [43].

The previous architecture frameworks architectures are created for an enterprise level use. A challenge is to find a framework that concentrates on technical security and gives guidelines and methods to design a technical network security architecture formally. On the other hand, many lower level security architectures consider technical security at a very detailed level.

Typically, the low level architectures address a certain security control or a single security control (e.g. cryptography, software code, and authentication). For example, Security Architecture for Survivability Mechanisms [18] presents a novel framework to facilitate software security against malicious execution environments, and describes the design, implementation, and analysis of an approach to the problem of software security in untrustworthy environments. Another example is a Mobile Ad Hoc Network Security Architecture [18] that is based on the use of an immune agent system. Immune agents are network nodes that either detect possible invaders or counterattack. When invasion is detected by a detection agent, it sends out directions to all neighbor nodes around the attacker to active counterattack agents, to surround and isolate the attacker node. The scope of the architecture is very limited, and it does not present any security controls in practice.

The Cisco Network Security Baseline [69] presents the fundamental network security elements that are critical to developing a strong network security baseline. The focus is primarily on securing the network infrastructure itself, as well as critical network services. The baseline utilizes the Cisco Security Framework (CSF) that is a security operational process model targeted at ensuring network, and service, availability and business continuity. The CSF is designed to identify current threat vectors, as well as track new and evolving threats due to an ever-moving target of cyber security threats.

The CSF is describes two fundamental objectives; total visibility and complete control. To gain the total visibility and complete control, the CSF uses multiple technologies and capabilities throughout the network to gain situational awareness into network activity, enforce network policy, and detect anomalous traffic. Figure 16 illustrates the Cisco Security Framework with six key elements (identification, monitoring, correlation, hardening, isolation, enforcement).

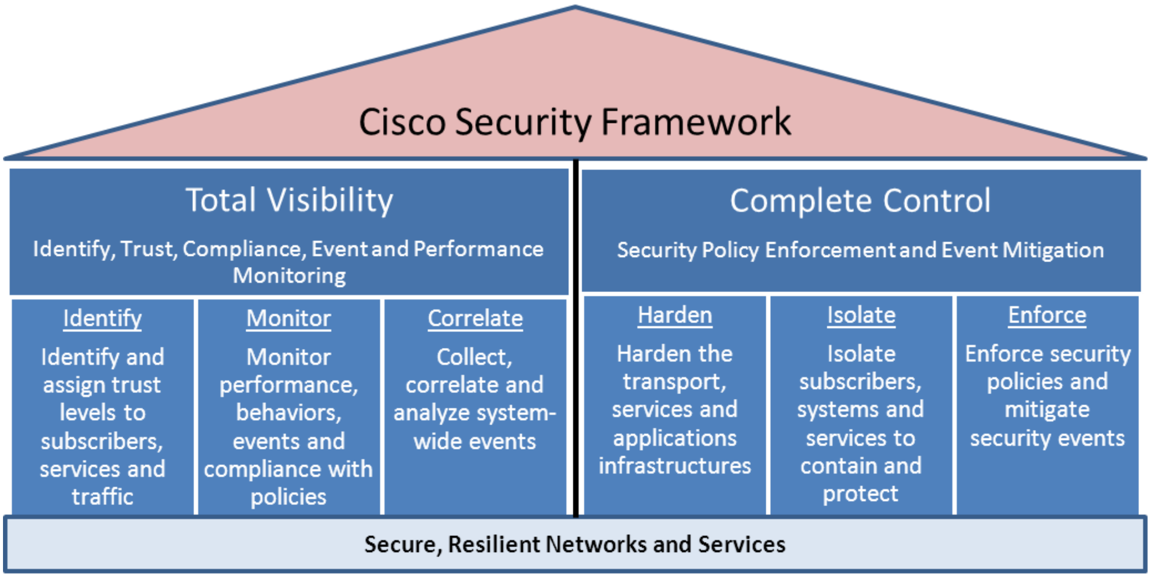

Cisco Security Framework
Total Visibility
Identify, Trust, Compliance, Event and Performance Monitoring
Complete Control
Security Policy Enforcement and Event Mitigation
Identify
Identify and assign trust levels to subscribers, services and traffic
Monitor
Monitor performance, behaviors, events and compliance with policies
Correlate
Collect, correlate and analyze system-wide events
Harden
Harden the transport, services and applications infrastructures
Isolate
Isolate subscribers, systems and services to contain and protect
Enforce
Enforce security policies and mitigate security events
Secure, Resilient Networks and Services

Figure 16: Cisco Security Framework overview.

The Cisco Network Security Baseline does not offer an effective architectural views or structures that would help to design new network security architectures. The baseline and the CSF are especially designed for configuring network devices and services. Thus, the baseline provides detailed guidance on how to implement each security control and best practice, along with plenty of configuration templates and examples [69]. Obviously, most of the security controls implemented in the Cisco systems are relevant and useful for the cognitive military networks.

The ITU Telecommunication Standardization Sector (ITU-T) has published several standards and recommendations for telecommunication systems security. ITU-T recommendations are created from a technical point of view, making them more interesting for this research. The ITU-T recommendations are not such architecture frameworks, but they still include systematic matters to build security in networking devices.

Recommendation X.805 (Security architecture for systems providing end-to-end communications) [55] defines the general security-related architectural elements that, when appropriately applied, can provide end-to-end network security. The recommendation addresses security concerns for the management, control and end-users through three layers; network infrastructure, services and applications. This approach is similar to one presented in the previous iCode security architecture framework. Figure 17 illustrates the X.805 security architecture.

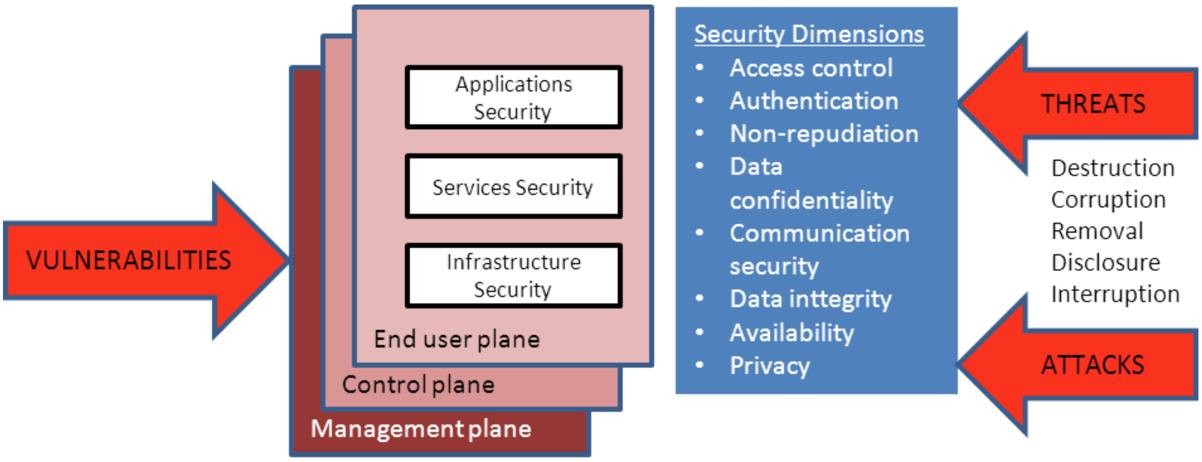


Figure 17: X.805 security architecture overview.

The older ITU-T recommendations X.800 [83], X.802 [45] and X.803 [58] consider security through the OSI layers defining the requirements for security and characterizing the approaches to satisfying these requirements. The recommendation X.800 describes the Reference Model including the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required.

Recommendation X.802 describes the cross layer aspects of the revision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link, Physical). It describes the architectural concepts common to these layers, the basis for interactions relating to security between layers and the placement of security protocols in the lower layers. X.803 Recommendation describes the selection, placement and use of security services and mechanisms in the upper layers (applications, presentation and session layers) of the OSI Reference Model. A common factor for these ITU-T recommendations is that they all use the security services (dimensions) described in Section 2.4.

From the review of the architecture frameworks and models, the following conclusions can be drawn:

1. Some of the models (MODAF, DoDAF) are high-level architecture frameworks, and they do not originally include any security related views. Typically they are specially designed for military organizations, but the focus is more on command and control applications than on communications networking.

2. The presented security architectures (SABSA, iCode) are overall security architectures, and they attempt to describe enterprise-level security management and controls. The architecture models are difficult to use for describing a cyber security architecture of military networks, because the models do not introduce any functional or component-level features.

3. Technical security architectures (e.g. Cisco Security Framework) are created to support the network devices of a certain manufacturer. These architectures typically define how to the devices are to configured to provide a desired security level. The architectures are independent and open, but they are based on certain technologies and devices.

4. ITU-T recommendations are more promising. They define technical security requirements and mechanisms in different scenarios. A challenge is that the ITU-T architecture documents only present the technical requirements at each system layer, but do not show how the architecture layers are built with smaller blocks and security elements.

5. None of the architecture models or frameworks introduces any cognitive processing. This is natural because the research area of the cognitive networks is quite new, and cognitive systems are still in a prototyping phase.

5.2. Overview of Cyber Security Architecture

Figure 18 presents the overview of cyber security architecture for the cognitive military networks. The architectural design is based on a block diagram that describes functional element at five functional layers. As it was stated in the end of the previous section, the reviewed architecture models were difficult to apply to the proposed architecture. Thus, this proposed architecture model is not based on any existing model or framework. However, the layered approach of the ITU-T X.805 recommendation is utilized in the architecture design. Also, the overall structure of the cognitive system framework presented in Figure 10 is exploited to create the cognitive layer to the cyber security architecture.

The functional layers of the architecture are Security Policy and Management Layer, Cognitive Layer, Application Security Layer, Service Security Layer, and Infrastructure Security Layer. The layers are implemented in each network node throughout the entire network. The nodes may be mobile or fixed, and man-packed or vehicle-mounted. Security controls and settings are controlled and optimized from three perspectives; a single network node, a network cluster, and an entire network.

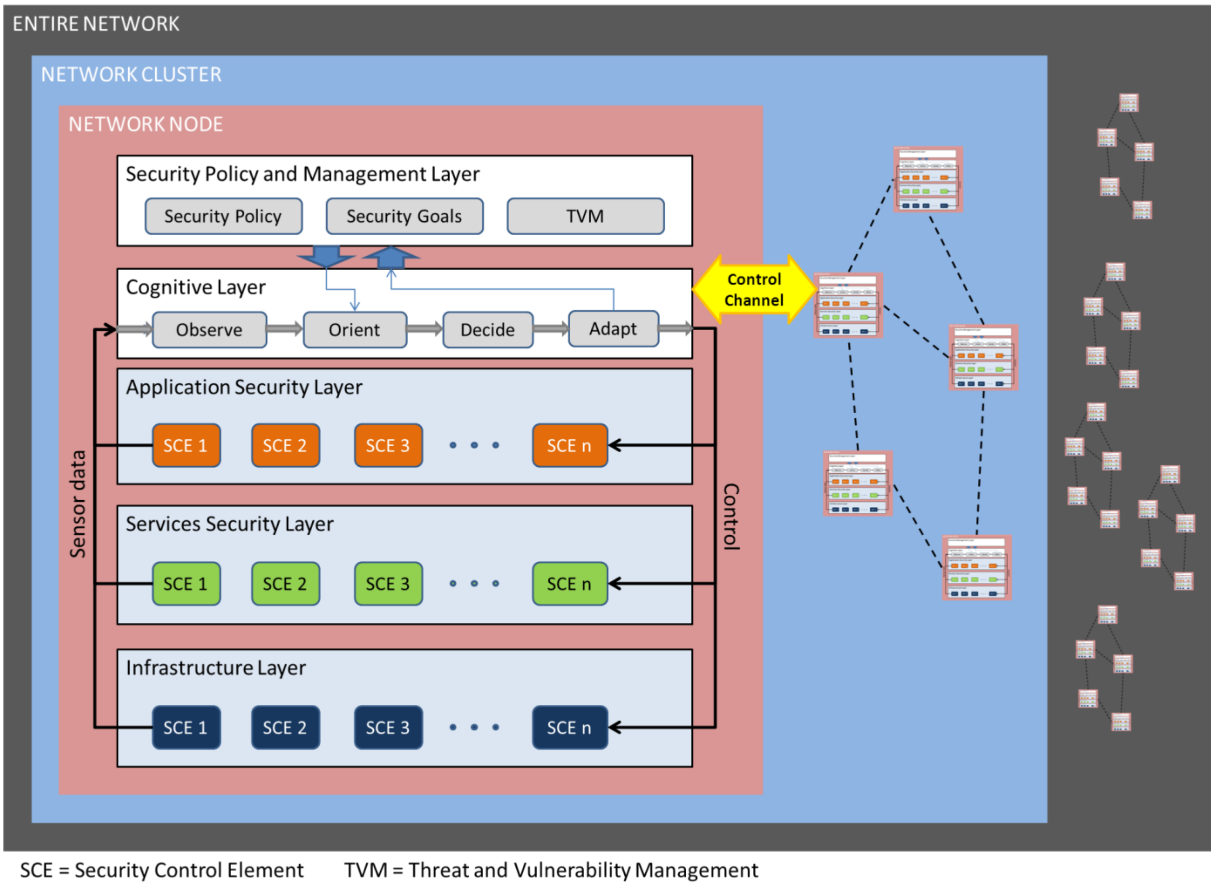


Figure 18: Overview of the cyber security architecture.

At the top of the architecture, security policies and goals are set and executed at the Security Policy and Management Layer which then guides and controls the Cognitive Layer. In addition to the Security Policy and Security Goals elements, the Security Management Layer also includes the Threat and Vulnerability Management (TVM) element that provides cyber security threat and vulnerability libraries to the Cognitive Layer. This input includes security goals for user access (e.g. authorization, authentication), data classification levels, cryptography algorithms, key patterns, security requirements for data transport, etc. The security policies and goals are manually set in an initiation phase of network deployment.

During the operational phase, some situations require that modifications to the goals and policies are conducted. The threat and vulnerability libraries are updated continuously during the operational phase of the network. The Security Management Layer also receives information from the Cognitive Layer. This information contains data about network adaptation decisions, current setup, and detected anomalies.

The main task of the Cognitive Layer is to provide a cognitive process for decision making and to execute the security adaptations in a network node. The process follows the previously introduced OODA loop with the observation, orientation, decision-making and acting phases. The layer is connected to the Application Security Layer, Service Security Layer, and Infrastructure Security Layer in two ways. Firstly, the Cognitive Layer controls and adjusts Security Control Elements (SCE) of these three layers according to the adjustment orders (based on the decisions), and secondly, the Cognitive layer monitors all the Security Control Elements and receives status data from them.

The security controls of the cognitive military network are implemented at three separated layers; Application Security Layer, Service Security Layer, and Infrastructure Security Layer. These layers are built in accordance with the ITU-T X.805 recommendation [85]. The layers are a series of enablers for securing networks; the infrastructure layer enables the services layer and the services layer enables the applications layer. According to the recommendation, each layer has different security vulnerabilities and offers the flexibility of countering the potential threats in a way most appropriate for a certain security layer.

The Infrastructure Security Layer includes the security controls of network transmission facilities, and individual networking elements. The infrastructure layer represents the most vital base when building blocks of networks, services and applications [85]. Network elements belonging to the infrastructure layer include individual routers, switches, servers, and the communication links (wireless and fixed) between these routers, switches and servers. In a context of the military tactical networks, the Infrastructure Security Layer mainly consists of mobile tactical network nodes that provide both networking and information service capabilities to the end-users.

The Services Security Layer addresses security of services that a network provides to the end-users. These services range from basic transport and connectivity to service enablers like those that are essential for providing service and network access (e.g. authentication/authorization services, dynamic host configuration services, domain name services, etc.) to value-added information services such as military C2 tools, location services, messaging, VPN connections, etc.

The Applications Security Layer concentrates on security of the network-based applications accessed by end-users from commanders to regular soldiers. The end-user applications are enabled by network services and infrastructure, and they consist of basic C2 applications, file transport/storage applications, voice messaging and email, video collaboration, etc. The applications may be provided using data centers or local servers.

Security Control Elements provide appropriate security controls at each of these three layers. The controls can be classified into three categories according to the timescale of an incident. Before the incident occurs, preventive controls are intended to prevent an incident from occurring by e.g. blocking unauthorized user access. Detective controls are design to act during the event, and they are planned to identify and characterize an incident in progress, and to alert other security controls (in automated systems) or network security personnel (manual incident handling). After the event, corrective controls are used to limit any damages caused by the incident e.g. by separating damaged network segments, filtering traffic, or recovering damaged services.

The Security Control Elements provided by the security architecture include the following components of security protection [107]:

- *Integrity protection components* generate and authenticate the digital signatures and authentication messages for the purpose of entity and data integrity.

- *Confidentiality protection components* encrypt and decrypt data (files, message, packets) to protect the confidentiality of data in all processing or transferring phases.

- *Vulnerability management components* automatically scan and update the system vulnerability of network nodes and patch the security holes.

- *Authentication components* provide authentication services for network nodes, and for example, negotiate the session key required by secure communication.

- *Access control components* receive and request access control lists and authenticate the access control requirements of network nodes.

- *Communication insulation components* configure and manage network communication connections and implement traffic monitoring and for example packet filtering.

- *Malware protection components* automatically scan and remove viruses and automatically update malware libraries.

- *Security audit components* automatically follow and record the operation logs of network infrastructure, services and applications.
- *Intrusion detection components* automatically detect and record hostile intrusion events and cyber attacks, and distribute warning information to related control components.

In addition to the cognitive layer and process, the implementation of cognitive security features requires the security controls to be fully software-controlled. This means that all the security elements are controlled by software. Another requirement for the security controls is an ability to collect status information from the security control elements.

5.3. Infrastructure Security Layer

The Infrastructure Security Layer architecture describes the security controls to prevent cyber attacks causing damages to data transition, communication links, and their supporting control capabilities such as routing, and network access. In a context of the military tactical networks, the Infrastructure Security Layer mainly consists of mobile tactical network nodes that provide both networking and information service capabilities to the end-users.

Securing the infrastructure layer consists of securing the control or signaling information (e.g. routing information) that resides in the network nodes as well as securing the receiving and transmission of control or signaling information by the cognitive military network node. Securing the infrastructure layer is also concerned with securing the operations, administration, maintenance, and provisioning of the individual network elements, wireless and fixed communication links, and mobile server platforms.

The Infrastructure Security Layer protects user data packets as they are transported through the network nodes, as well as, they are being transported across wireless and fixed communications links. Figure 19 presents the architecture of the Infrastructure Security Layer that contains six separated security elements to provide efficient security controls for management, control and end-user data at the infrastructure layer. The infrastructure layer is connected to the other layers as depicted in the overall architecture view in Figure 18. The features of each element are described in the following sections.

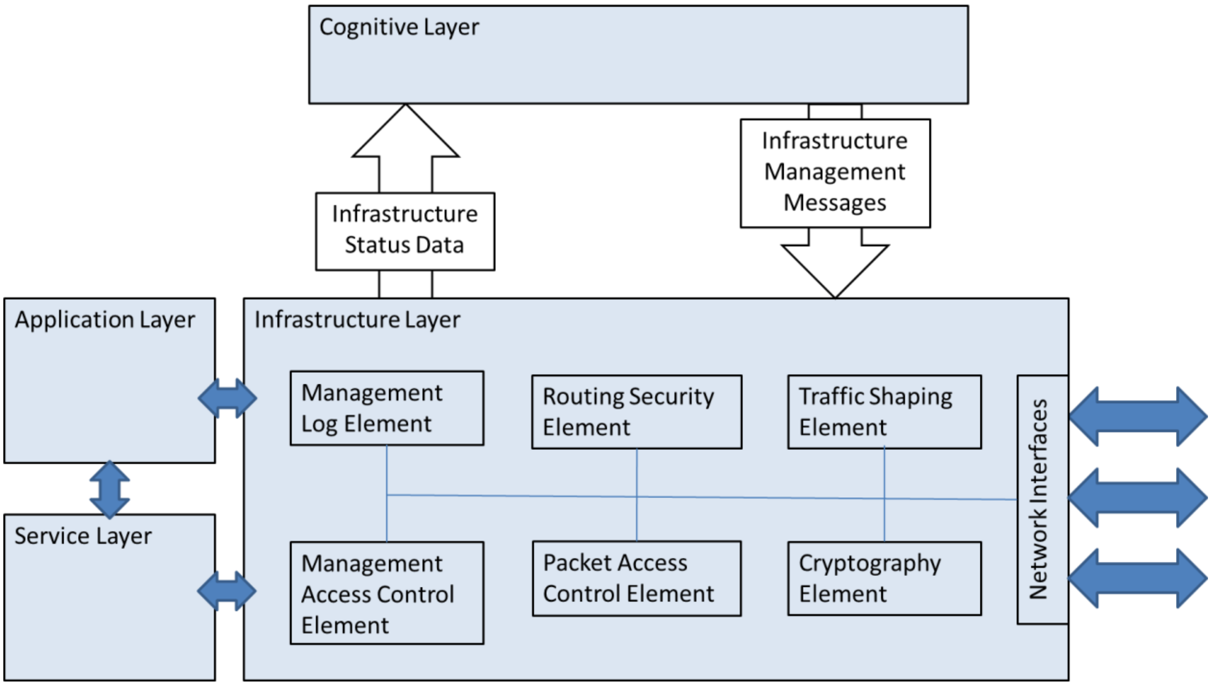


Figure 19: Overview of Infrastructure Security Layer.

Cryptography Element (CE)

The Cryptography Element provides cryptographic services to protect outgoing packets from losing confidentiality. At the infrastructure layer, the cryptography element encrypts the control and addressing data of outgoing packets, and decrypts the same data of incoming packets. The purpose of the element is to protect data packets against discovering control (e.g. routing, addressing, etc.) information. Table 9 illustrates the tasks and cognitive management of the element. The cognitive layer controls the element by setting up cryptographic algorithms and distributing keys. The third column of the table defines what information is collected to the cognitive process from the element.

Table 9: The tasks and management of the Cryptography Element.

Tasks	Cognitive control	Sensor data
Control message encryption (for routing, QoS, authentication, access, etc.)	Cryptographic algorithm selection Key distribution	Algorithms in use Current key
Control data decryption (for routing, QoS, authentication, access, etc.)	Cryptographic algorithm selection Key distribution	Algorithms in use Current key

Routing Security Element (RSE)

The main purpose of the Routing Security Element is to ensure that routing is secured and operational during network operations. The element guarantees that only valid routing updates are approved. The element also filters adverse or fake routing information. Table 10 illustrates the tasks and cognitive management of the Routing Security Element. The element authenticates and authorizes the sources of routing update information. Invalid sources are rejected. The status of accepted and blocked routing updates is collected by the cognitive layer.

Table 10: The tasks and management of the Routing Security Element.

Tasks	Cognitive control	Sensor data
Routing update authentication	Information of valid nodes	Authenticated network nodes
Routing update authorization	Information of permission to exchange routing data	Authorized network nodes
Filtering	List of accepted routing information sources	Blocked routing information sources

Packet Access Control Element (PACE)

The task of the Packet Access Control Element is to provide authentication, and authorization services for data packets. The access control element guarantees that only valid traffic packets enter into a network node. The element also adds authentication information on outgoing packets. The purpose of the element is to prevent that malicious packets arrive at the node.

Table 11 presents the tasks and cognitive management of the Packet Access Control Element. The cognitive layer controls the packet access control element by providing valid authentication and authorization information. The cognitive layer takes care of access lists and valid authentication keys so that correct packet sources are accepted and packets from unknown or hostile sources are dropped.

Table 11: The tasks and management of the Packet Access Control Element.

Tasks	Cognitive control	Sensor data
Identification of incoming packets	Authentication key distribution List of valid packet sources	Incoming packet sources
Authorization of incoming packets	Distribution of authorization information (access lists)	Authorized packet sources
Add authentication information to outgoing packets	Distribution of authentication information (keys)	Status of authentication information (keys, etc.)

Traffic Shaping Element (TSE)

The purpose of the Traffic Shaping Element is to generate and modify data traffic on each communication link so that traffic flow do not disclose communication behavior, and thus, command and force structures. This critical information can be observed by looking at the traffic flow instead of looking at the payload content of the packets. Traffic flow can often expose that there is communications, the volume, and who is communicating to whom. Traffic flow can be protected by padding of data such that the links are always fully utilized regardless of the end-user traffic volumes.

The task of the Traffic Shaping Element is to generate bulk traffic to communication links so that the traffic rate of a link is constant. By eavesdropping the link the enemy has a challenge to figure out if transmitted data is operational or just bulk. The cognitive layer controls the element by setting up the current traffic rates at each link. Status information collected by the cognitive process includes information of current link utilization.

Management Access Control Element (MACE)

Secure node management is important to prevent unauthorized configuring of a network node. Especially, when the cognitive process automatically controls and reconfigures system parameters, it is critical to have appropriate access control for node management. All management requests are authenticated. In an ideal system, a whole management is provided by the cognitive layer, but some manual configuration may also be required in certain situations. Although, all the management commands are mostly incoming from the node’s own cognitive process, in some cases the source of a management message may be somewhere else in the network. Thus, it is critical to have a full controlled access mechanism to management data.

Table 12 illustrates the tasks and cognitive management of the Management Access Control Element. The tasks are authentication and authorization of incoming management data. The cognitive layer updates access information about valid management sources and permissible services to be configured. As a feedback to the cognitive process, the element provides information about current management sources and managed services. Also, the element informs the cognitive layer about the blocked management source.

Table 12: The tasks and management of the Management Access Control Element.

Tasks	Cognitive control	Sensor data
Authentication of management data	Updating authentication information	Current management sources Blocked management sources
Authorization of management data	Updating authorization information	Currently reconfigured services

Management Log Element (MLE)

The main purpose of the Management Log Element is to provide a management audit trail for the network. The task is simply to store information of the management sessions into a log file. The cognitive layer sets up the requirements for information to be collected. Typically these include a source ID, date, time, and the changes that are made. The cognitive layer collects data of the status of the log file, and for example, cleans the files when they become too large.

5.4. Services Security Layer

Building security controls at the Service Security Layer may be complicated, because network services are often built-upon one another. For instance, in order to provide a secure email service, a cognitive military network has to provide a simple IP service that relies on enabling services such as DHCP, DNS, and authentication [85]. The network should also provide cryptography and QoS services to meet end-user’s quality and security requirements for the secure email service.

The Services Security Layer includes the security controls that protect data used by network services. Protecting the end-user data traffic of the network services means, for example, that the confidentiality of a user's conversation is protected in a VoIP service or a DNS service is secured to ensure the confidentiality of users. Securing the control or signaling information used by the network service concerns, for example, issues of securing the SIP protocol that is used for the VoIP sessions. Securing the management of the network services consists of the protection of the Operations, Administration, Maintenance & Provisioning (OAM&P) functions of the network services. This also includes securing the configuration of network services.

Figure 20 presents the architecture of the Service Security Layer that consists of six separated security elements to provide efficient security controls for management, control and end-user data. The layer has input and output connections to the cognitive layer allowing the cognitive layer to control the security elements, and to collect status data from the elements. The Cryptography Element, Management Log Element and Management Access Control Element provide the same functionalities as those at the infrastructure layer (see Figure 19), and they are described in the previous section. The features of the rest of the element are described in the following sections.

The purpose of the Cryptography Element is to secure all the messages concerning service controls. The Management Access Control guarantees that only allowed management messages are passed to control the service layer. The Management Log Element stores all the management sessions for the service layer.

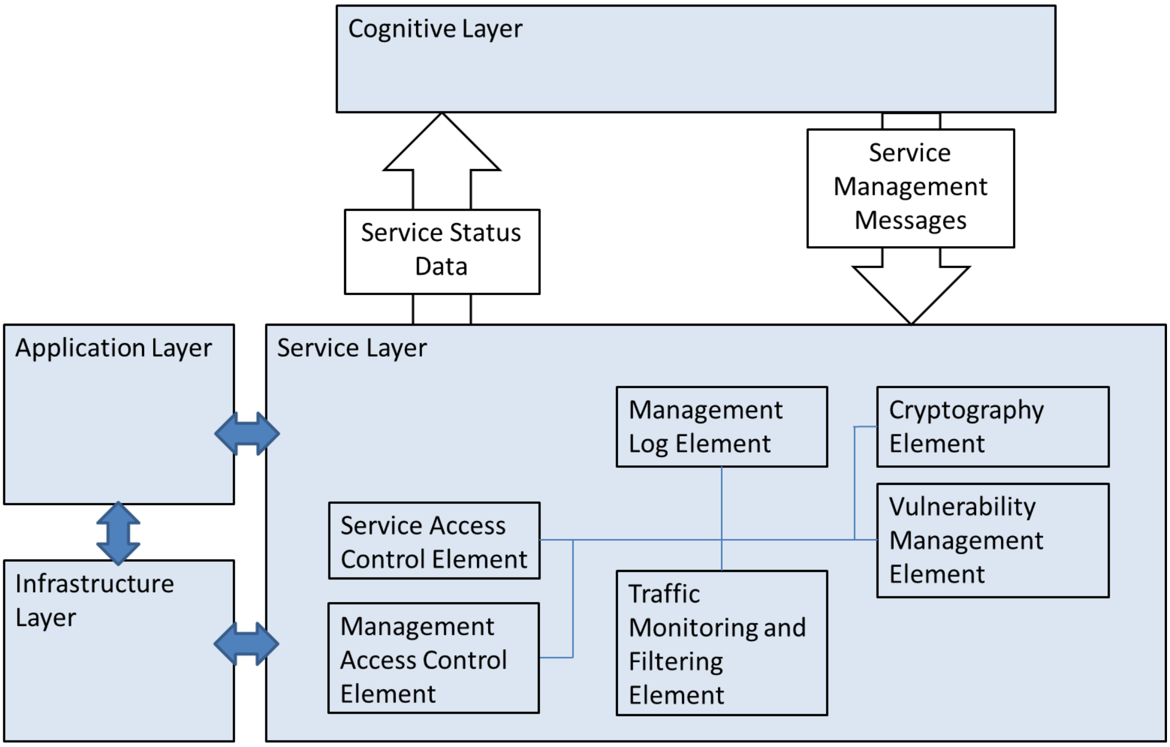

Cognitive Layer
Service Status Data
Service Management Messages
Application Layer
Service Layer
Management Log Element
Cryptography Element
Service Access Control Element
Vulnerability Management Element
Infrastructure Layer
Management Access Control Element
Traffic Monitoring and Filtering Element

Figure 20: Overview of Service Security Layer.

Service Access Control Element (SACE)

The purpose of the element is to control access to the network services. The element prevents access from unknown and hostile sources that may be both end-users and other services. The tasks of the element are equals to those shown in Table 11 except that authentication and authorization is provided to the service access messages instead of the packet source. The cognitive layer controls what services are accessible to different end-users and other services. The cognitive layer collects information about the current service usage status and dropped access requests.

Traffic Monitoring and Filtering Element (TMFE)

The main tasks of the Traffic Monitoring and Filtering Element are related to those provided traditionally by firewalls and anti-virus software. The Element monitors incoming and outgoing data traffic to prevent, detect and remove malware in all descriptions. The Element also provides the control of the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not. The element also monitors anomalies from network traffic

Table 13 shows the tasks and cognitive management of the element. Detecting malware from network traffic is based on information about anomalous traffic behavior and malware signatures. The cognitive layer updates signatures, filtering settings and distributes information about traffic behavior. The cognitive layer collects data about traffic statistics, incidents and other suspicious traffic.

Table 13: The tasks and management of the Traffic Monitoring and Filtering Element.

Tasks	Cognitive control	Sensor data
Detection of malware from incoming traffic	Distribution of signatures	Malware incidents
Detection of malware from outgoing traffic	Distribution of signatures	Malware incidents
Filtering incoming traffic from unpermitted sources	Filtering setup for incoming traffic	Dropped traffic
Filtering outgoing traffic to unpermitted destinations	Filtering setup for outgoing traffic	Dropped traffic
Anomalous traffic detection	Updating information about normal traffic baseline and anomalous behavior	Detected anomaliess

Vulnerability Management Element (VME)

The Vulnerability Management Element is a component that collects information about system vulnerabilities, and executes patching when a fixing piece of software is available. The purpose of the element is to keep the network nodes up-to-date as rapid as possible. Vulnerability information is based on information about software and firmware versions of system elements. The element also runs black box testing called fuzzing [79] in which services or components are provided with invalid, unexpected, or random input data.

Table 14 lists the tasks of the Vulnerability Management Element. The tasks consists of collecting vulnerability information, patching and fuzzing. The cognitive layer controls the element by setting data collection requirements (what information is collected concerning vulnerabilities), by distributing available security patches, and by guiding fuzzing (target services and systems, fuzzing settings, etc.). Sensor data to be gathered includes information about vulnerabilities and fuzzing results.

Table 14: The tasks and management of the Traffic Shaping Element.

Tasks	Cognitive control	Sensor data
Collecting vulnerability information	Setting data collection requirements	Vulnerable services, software and firmware
Vulnerability patching	Distributing available security patches	-
Fuzzing	Information about elements or services to be tested	Testing results

5.5. Application Security Layer

Securing the applications layer includes securing data generated by end-user applications. The applications may be locally installed or they may be network-based (server-client solutions). In the military environment, the applications have high requirements for processing, sharing and storing classified information to ensure operational security. For example, the confidentiality of force tracking data must be protected by a military C2 application. Securing the applications layer also includes the protection of the control or signaling information used by the network-based applications. An example of this is securing the email protocols (e.g. IMAP) used to control the delivery of email.

The OAM&P functions and the configurations of the applications must also be secured. For an email application, this means that, for instance, the provisioning and administration of user mailboxes is protected.

Figure 21 depicts the architecture of the Service Security Layer with five separated security elements to provide efficient security controls for management, control and end-user data at the application layer. The Cryptography Element, Management Log Element and Management Access Control Element provide the same functionalities as those at the infrastructure layer (see Figure 19), and they are described in the previous section. The features of the rest of the element (Node Access Control Element and Application Access Control Element) are described in the following sections.

The purpose of the Cryptography Element at the application layer is to encrypt and decrypt all application traffic. The Management Access Control protects the management of the applications allowing only authorized access to application management data. The Management Log Element stores all the management sessions for the applications.

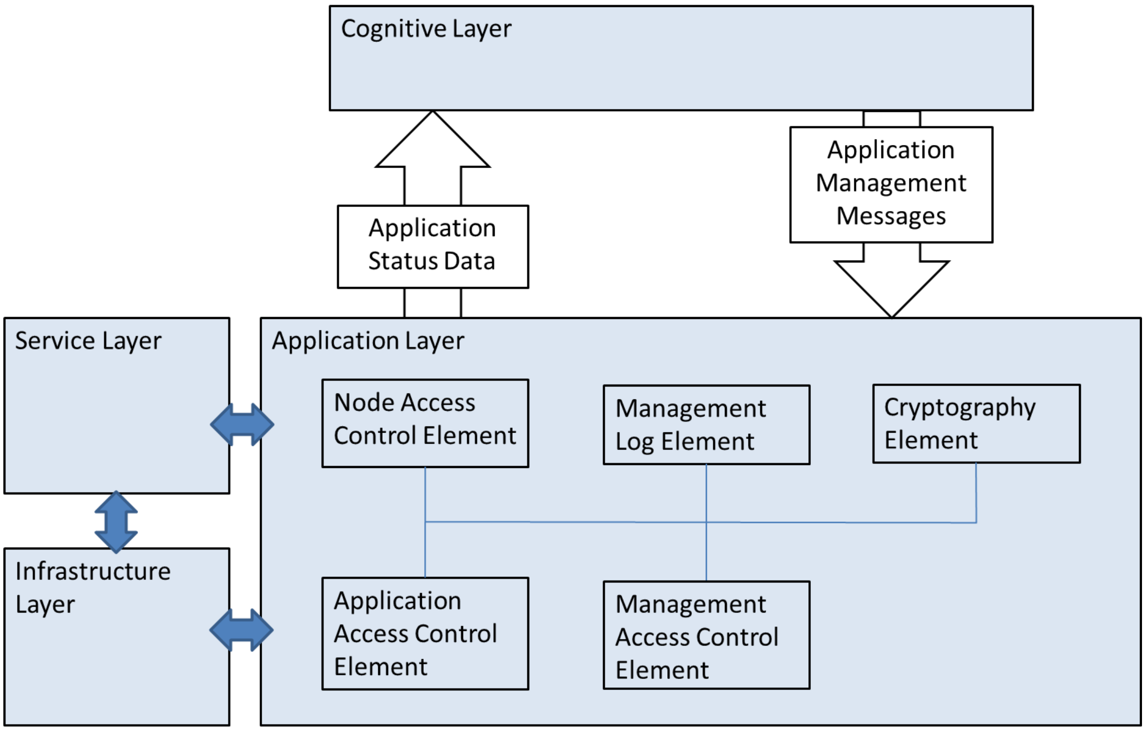


Figure 21: Overview of the Application Security Layer.

Node Access Control Element (NACE)

The task of the End-User Access Control Element is to provide authentication, and authorization services for end-users accessing to a network node. The main purpose of the element is that only legitimate users are able to access and connect to the network node.

The tasks of the element simply consist of authentication and authorization processes to provide access to the node. The cognitive layer controls the element by providing valid authentication and authorization information. The cognitive layer takes care of distributing authentication authorization information (keys, certificates, access lists, etc.). The cognitive layer also provides the list of legitimate users. As sensor data, the cognitive layer collects information about current users of the node and rejected access requests.

Application Access Control Element (AACE)

The Application Access Control Element provides authentication, and authorization services for end-users accessing to the applications located in a local or remote node. The main purpose of the element is that only legitimate end-users are able to use applications. Hostile or unknown end-users are rejected by the element.

Generally, the tasks of the element are the same as those of the Node Access Control Element include authentication and authorization of an end-user. The cognitive layer controls element by providing valid authentication and authorization information for application access. The cognitive layer distributes authentication and authorization information, and updates the list of the legitimate users. The element provides information about current users, applications they use and rejected application accesses as input data to the cognitive layer.

5.6. Cognitive Layer

The cognitive layer presented in Figure 18 functions as “brains” for the network. The layer implements the cognitive process and previously introduced OODA loop with the phases of observation, orientation, decision-making and adaptation. The layer receives information from all the security elements at the infrastructure, service and application security layers. This information consists of data described in the previous sections where the security layers are presented in more details. At the same time, the cognitive layer controls the security elements according to the decisions made in the decision-making phase.

The cognitive layer is connected to the security policy and management layer in the orientation and acting phases. The security policy and management layer provides end-to-end security goals that are considered in the orientation phase in which current situational data, history data and the goals are fed into the decision-making process. On the other hand, the acting phase pushes overall situation information to the management layer.

The cognitive layer is distributed over the entire network trough the control channel presented in Figure 18. The control channel is a vital part of the system as it shares situational information between the network nodes. The control channel is important when network parameters are optimized over the network. Several algorithms can be applied for optimizing and decision-making [58], but researching algorithms is not in the scope of this study.

As it is seen in the overview figure, in a sense of parameter optimizing, the network is divided into three areas. The first area includes a single node, and optimizing is conducted within this single node. In this case no control channel is required, and the nope is able to make decisions with information collected from its own elements. The second optimizing area consists of a cluster of nodes. In that case, the network is divided in sub networks on which specific end-to-end targets are set. Optimizing is provided among the nodes inside the cluster. The third optimizing area involves all the nodes of the network, and optimizing is performed within the whole network. The cluster and entire network wide optimizing requires an effective control channel so that parameter values can be shared between the nodes. A weakness of the control channel is resource consumption. The distributed channel requires computational capacity, link capacity, channel protocols and obviously security protection.

The network performance depends on the amount of available network state information at the cognitive layer. In order to make beneficial and optimal decisions, the cognitive layer must receive and have the latest information from all software controlled network security elements. Obviously, decisions made by the cognitive layer are better than those made in ignorance. However, in complex systems such as tactical military networks, it is unlikely that the cognitive layer would know the complete system state. [97] The tactical networks are often challenging (e.g. weak links, connectivity problems, scarcity of bandwidth) when sharing status information between the network nodes, meaning the cognitive layer have to work with less than a full picture of the network and security status.

5.7. Security Policy and Management Layer

The security policy and management layer is located on the top of the cognitive layer (see Figure 18). The purpose of the layer is to manage and control the cognitive layer. The management layer consists of three management components that are Security Policy, Security Goals, and Threat and Vulnerability Management. In this section, these components are described in more details.

Security policies are the basis for all information security planning, design, and deployment. Policies direct implementers and end-users how issues should be addressed and technologies should be used. Typically, policies do not specify the proper operation of equipment or software, but it sets limitations how networks are operated and how information is processed in the networks. A policy is a plan or course of action that conveys instructions from an organization's security management to those who make decisions, take actions, and perform other duties. [102] In this case, these instructions are created for the cognitive layer.

A security policy may include the following issues:

- *Access control*. Access rules and rights for applications, databases, portals and services are defined through access control.
- *Configuration rules*. System configuration processes and limitations are defined in security policies.
- *Processing classified information*. The requirements for processing classified information are defined in policies.

It is important to ensure that the security policy is enforced by mechanisms that are strong enough. In the case of cognitive networking, the policy enforcement is provided by an automated process. Thus, the enforcement process does not include any manual enforcement by human network operators creating fewer possibilities that the policy is not followed.

The main task of the security goals management is to describe the end-to-end security goals for the network performance. The goals are sent to the cognitive process that optimizes network parameters to achieve the goals. The security goals include for example approved encryption algorithms, key lengths, access protocols and controls, overall security controls in each node, etc. The security goals should provide information for the cognitive process enough to set the optimized parameter values for all configurable security elements.

Threat and Vulnerability Management (TVM) has an important role in today's cyber threat environment. Using TVM the network is able to adjust its parameters to defend against cyber threats. The threat and vulnerability management component maintains the libraries of current threats and threat scenarios. The component also provides threat and vulnerability information for the risk assessment implemented at the cognitive layer.

5.8. Defense in Depth

In this section, the proposed architecture is considered from the Defense in Depth perspective. Defense in Depth is an information assurance (IA) concept in which multiple layers of security controls are placed throughout information systems and networks [27]. The purpose is to provide redundancy in the case a security control fails or vulnerability is exploited. The concept covers aspects of personnel, procedural, technical and physical security, but in this section we focus on the technical aspects.

The idea behind the defense in depth concept is to protect a system against any particular attack using several independent methods and protection layers. The placement of protection mechanisms, procedures and policies is intended to increase the reliability of an information system and network where multiple layers of defense prevent espionage and direct attacks against critical systems. In terms of computer network defense, defense in depth measures should not only prevent security breaches, but also buy an organization time to detect and respond to an attack, thereby reducing and mitigating the consequences of the attack. [10]

The Defense in Depth strategy introduces five technological approaches [27] to improve the network's ability to defend against cyber attacks. The approaches are considered from the cyber security architecture point of view in the following paragraphs.

Defense in Multiple Locations. Adversaries can attack a target from multiple locations using either insiders or outsiders. A network system needs to deploy protection mechanisms at multiple locations to resist different types of attacks. The proposed architecture implements security elements and controls in each network node. The protective mechanisms such as access control, encryption, traffic shaping, anomaly detection, traffic filtering and monitoring, are located multiple points throughout the entire network.

Layered Defenses. Even the best available security technology has inherent weaknesses and vulnerabilities that an adversary will find and exploit sooner or later. An effective countermeasure is to place multiple defense mechanisms between the edge of the network and a target service or information. Each of the security mechanisms must present a unique obstacle to the attacker. The mechanisms should include both "protection" and "detection" measures to help detecting the attacker at each layer of defense. The security architecture composes this layered defense by having several security elements to be passed before accessing to user data or services. These elements include encryption, traffic filtering and monitoring, and access controls at several layers.

Security robustness. The security robustness (strength and assurance) of each security component must be specified as a function of the value of what's it is protecting and the threat at the point of application. For instance, deploying stronger security mechanisms at the network boundaries is often more effective than deploying these mechanisms at the user desktop. The security robustness of the proposed architecture is carried out by the distributed implementation of the cognitive layer and security controls. The architecture includes no single point of failure. The security management is distributed so that each node can still operate locally without any connection to other nodes. However, without a control channel connections the node cannot adapt its security parameter optimally because vulnerability, threat and status information is not shared between the nodes.

Robust key management. Key management services and mechanisms should be implemented to support security technologies and to be highly resistant to cyber attacks. Key management infrastructures are lucrative targets for an attacker as we know that key management is one of the most critical issues in the networks. In the proposed architecture, key management is controlled by the cognitive layer which should be aware of key distribution situation throughout the network. The architecture does not describe key management mechanisms, but naturally key management is protected with all the available security elements.

Intrusion detection. Infrastructures should provide sufficient capabilities to detect and analyze intrusions, and to correlate the results and even react accordingly. The cyber security architecture present the Traffic Monitoring and Filtering Element to overcome detection challenges. Each network node is capable of detecting anomalous traffic and intrusions.

5.9. Conclusions

The purpose of the proposed cyber security architecture is to determine the structure of security controls and management of a military communication network from a functional perspective. For describing an architectural design method, several existing architecture models and frameworks were studied. The aim was to find a suitable architecture model for the cyber security architecture. The reviewed architectures included both military and enterprise related frameworks and models. The military architecture frameworks are originally designed for developing command and control (C2) applications, and do not typically include security perspectives. Some add-on security features are introduced, but these features are still at a very high level. However, some security specified architecture models are created for the enterprise level design. A problem is that they concentrate on overall security in an enterprise, and do not include methods to design architectural views for technical communication security.

The biggest challenge with applying the reviewed architecture models is that none of the architecture models has been developed to describe cyber security of communication networks from a technical point of view. Most of the models contain different views for describing business or organization-level functions from administrative issues to technical standards. The architectures related to technical information security are typically based on based on the practical implementation of the existing equipment and technologies. A good example is the Cisco Security Framework that describes how security issues are considered in Cisco devices. On the other hand, for example in ITU-T recommendations focus on describing the functional security requirements instead of specifying an exact security architecture or security controls.

The proposed architecture aims to meet the today's requirements for cyber security of military communications. As the existing architecture models were difficult to use, the presented architecture was described as a simple functional block diagram. The military communication network consists of three functional layers as introduced in the ITU-T X.805 recommendation. In addition to these layers, the architecture defines the cognitive and management layers that are based on the cognitive system framework.

Each layer is composed of functional security elements whose basic functions were defined. The main task of the security elements is to protect the information content and data packets so that the requirements described in the previous chapters can be fulfill. The elements were only defined at the functional level, and the practical implementation of the elements was not investigated. The implementation may show that the architecture must be modified, if the functionality of the elements cannot be reasonably implemented. A risk is that implementing the full functionality may result in lead to a very complex system.

The architecture design allows that the security elements are flexibly added, deleted, or modified. However, we must remember that the proposed architecture does not exactly define relationships between the elements, and how the elements are connected to each other. The layered approach provides depth in security protection. The Defense in Depth requirements are fulfilled by using several consecutive security controls, decentralized service structure, and wide network monitoring and incident detection. Reliability is increased by distributing security controls and services to all nodes in the network. A drawback is that the decentralization complicates the system structure, which may increase the vulnerability of the system and implementation difficulties.

Cognitive functionality may add value to the maintenance of security in the network. A smart, cognitive process enables automated risk management and updating systems in real-time. The cognitive process modifies system parameters so that protection is align with the current threat environment, and in a case of attacking, the network is able to start counter operations without a human network operator. The biggest challenges in the implementation of the cognitive layer are related to the development of decision-making algorithms, and a secure and resource-effective control channel. The control channel can significantly consume network resources that are scarce especially in tactical military networks (e.g. link capacity, processing power, power supplies).

The proposed architecture includes the management layer that is important in cognitive systems where the cognitive process requires the goals and objectives for parameter optimizing. In the cyber security architecture, the management layer sets end-to-end security goals for the network so that information processing and sharing is performed securely. The management layer also includes the threat and vulnerability library which is an important part of the management layer in the cognitive network. The library ensures the security elements are configured to protect against latest threats and attacking scenarios.

The functionality and compliance of the cyber security architecture is very essential and even critical. Thus it is important that the proposed architecture is evaluated against threat scenarios. The original architecture design could be improved according to evaluation results. The purpose of the evaluation is also to show that the architectural design is at a certain level after the detailed description of the elements could be started. The proposed cyber security architecture is evaluated in the following chapter.

6. EVALUATION

Evaluation is a key process to prove compliance of the proposed cyber security architecture. In this chapter, two separated methods are presented and used for the evaluation. The evaluation is carried out against the threat scenarios presented in Chapter 3. In the beginning of this chapter, a variety of different evaluation methods and criteria are reviewed. The purpose is to show how these existing methods inadequately support the evaluation of network security architecture. For this reason, the used evaluation methods must have been applied in a new way.

6.1. Evaluating Security Architectures - Methods and Criteria

It is clear that designing a network architecture with security functions will produce a more secure architectural design and eventually more secure networks, yet it is still not obvious how to evaluate and conduct this intuitive process. It is also clear that a good architectural design is one that performs certain tasks (i.e. functionalities) and exhibits certain properties (e.g. security) [81]. Evaluation of architectures and designs is important, and in a case of security it is critical.

The main problem about security assessments is that the security of a given architecture cannot be measured directly. No single value or component of the network can reliably tell us how secure a system really is. Actually, this is a general problem that security assessments have to face. Besides, a chance remains that an inherent vulnerability of a system has not yet been disclosed, that some kind of backdoor in a piece of software still is to be revealed. As a consequence, it is very difficult to develop security evaluation methods which provide reliable feedback about a system. [65]

We can find several different methods for evaluating and assigning assurance levels to information and communications systems. Two reasons for several assurance evaluation methods could be found; evaluating methods and ideologies have developed over time, and various groups of experts look at computer security differently and rate some aspects of security differently. The purpose of an evaluation program is to establish a trust between the customer and the product vendor. [65] Three most-known security evaluation criteria are explained in the following paragraphs.

Trusted Computer System Evaluation Criteria (TCSEC) [100] is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information. The TCSEC was initially issued in 1983 by the National Computer Security Center (NCSC), an arm of the National Security Agency, and then updated in 1985. TCSEC was replaced by the Common Criteria international standard originally published in 2005.

The Information Technology Security Evaluation Criteria (ITSEC) [100] is a structured set of criteria for evaluating computer security within products and systems. The ITSEC was first published in 1990. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the Commission of the European Communities for operational use within evaluation and certification schemes. Since the launch, a number of other European countries have agreed to recognize the validity of ITSEC evaluations. The ITSEC has been largely replaced by Common Criteria, which provides similarly-defined evaluation levels and implements the target of evaluation concept and the Security Target document.

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) [23] is an international standard for computer security certification. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. The CC offers a set of well understood security functional requirements that can be used to create trusted products reflecting the needs of the market. These security functional requirements are presented as the current state of the art in requirements specification and evaluation.

Some criticisms against these evaluation criteria have shown up [51]. Typically, evaluation focuses primarily on assessing the evaluation documentation, and not on the actual security, technical correctness or merits of the security product. Only the highest levels of the evaluation require deeper, full source code analysis. Evaluation using the criteria is also a costly process, and the evaluation does not make a product more secure.

The effort and time necessary to prepare evaluation evidence and other evaluation-related documentation is so large that the product under evaluation is generally superseded by the time the evaluation work is completed. Other concerns are the lack of control over the actual production of the products once they are certified, and the absence of a permanently staffed organization that monitors compliance.

The reviewed evaluation criteria are designed for security products. Thus, it is challenging to apply the criteria for evaluation of a cyber security architecture of cognitive networks without an existing product or prototype. For this reason, the TCSEC, ITSEC and CC are not reasonable for the evaluation of the security architecture, and thus, they are not used for evaluation. In this study, the proposed cyber security architecture is evaluated by comparing the new architecture to the legacy architecture of military networks. The comparison is made using two different approaches. The first approach is to apply the previously introduced SABSA matrix, and compare how different security controls and procedures are concerned at each layer against the threats of each scenario. The second approach uses a scenario based evaluation model that was originally developed for the evaluation of software architectures.

6.2. SABSA Based Evaluation

The purpose of the SABSA based evaluation is to use the traceability of the SABSA Matrix (presented in Section 5.1) to ensure that the security elements at the bottom level of the proposed cyber security architecture are relevant to the threat scenarios at the top level. Figure 22 illustrates the traceability of architectural design. For example, a component security solution must fit into the architectural design at the next layer (physical security) proceeding all the way to the contextual security layer.

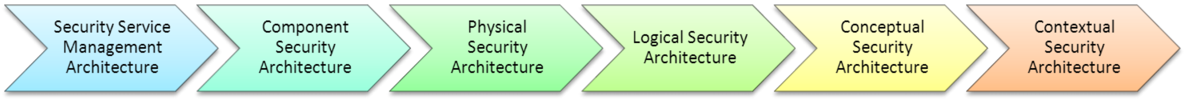

Security Service Management Architecture
Component Security Architecture
Physical Security Architecture
Logical Security Architecture
Conceptual Security Architecture
Contextual Security Architecture

Figure 22: The traceability of The SABSA Matrix.

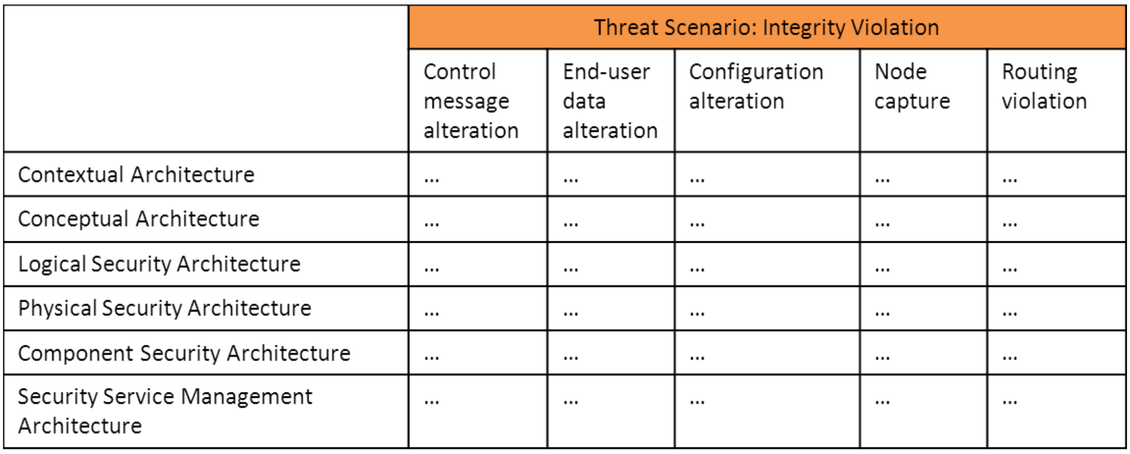
The SABSA Matrix was originally developed to cover overall security threats against business processes and actions [86]. Thus, it is challenging to modify the matrix and attributes to meet the technical cyber security requirements. The modification is started by describing the components and procedures of information system that are needed to be protected against cyber threats of the military environment. The objects to be protected are defined at all the layers of the SABSA Matrix. These objects are presented in Table 15.

The second phase is to modify the top row of the columns of the SABSA Matrix so that they include all the threats of the threat scenarios presented in Section 3.4. An example of that is depicted in Figure 23, in which the threats of the integrity violation threats scenario are added at the top row of the matrix.

Table 15: The protected objects at each SABSA Matrix layer in the context of military networking.

Layer	Objects to be protected
Contextual Architecture	Operational continuity Continuous command, control and communications capabilities
Conceptual Architecture	Availability of critical operational information Information sharing with strategic partners Recoverable networks and information services
Logical Security Architecture	Network topologies Command structures Communication profiles Information service structure Information sharing structures Network gateways
Physical Security Architecture	Critical data repositories Critical network nodes
Component Security Architecture	Network components: - Servers - Routers - Databases - Communication links
Security Service Management Architecture	Maintaining security service management: - Key management - Component management - Policy management - Access management

Finally, the protected objects are analyzed with each threat resulting an evaluation report that reveals the effectiveness of the elements of the architecture. The results will be more qualitative than quantitative. The SABSA Matrix does not output any checklists, or other metrics to follow. The matrix produces a holistic view how security controls are designed to protect against the threat scenarios. The SABSA matrix returns no absolute results of the security level. Thus, it is more reasonable to compare the results of both proposed and legacy cyber security architectures.



	Threat Scenario: Integrity Violation				
	Control message alteration	End-user data alteration	Configuration alteration	Node capture	Routing violation
Contextual Architecture	…	…	…	…	…
Conceptual Architecture	…	…	…	…	…
Logical Security Architecture	…	…	…	…	…
Physical Security Architecture	…	…	…	…	…
Component Security Architecture	…	…	…	…	…
Security Service Management Architecture	…	…	…	…	…

Figure 23: An example of addressing the threats of the integrity violation scenario when evaluating the layers of the SABSA Matrix.

6.3. Scenario Based Evaluation

Alkussayer and Allen [9] present a scenario-based framework for evaluating the security of a software architecture. Although, the framework is not originally developed for network security architecture, it is a promising approach to evaluate a high-level network security architecture. The inspiration for the scenario-based evaluation framework comes from recognition of the critical need for assessing the security of a system through its architectural design to disclose the underlying compliance of the architecture to the stakeholder's security needs. The proposed technique strengthens the security of a system architecture by combining three distinct factors seamlessly into a solid framework.

Evaluation Process

The evaluation process is based on a scenario-based architecture review. An architecture review is an efficient approach of ensuring design quality and addressing architectural concerns. The key goals of conducting an architecture review are to evaluate an architect’s ability to deliver a system that fulfills the security quality requirements and to identify potential security risks. The use of scenarios is maturing process and has proven to be a successful practice [22].

The scenario-based security evaluation both provides an assessment of quality attributes and explores the interactions and interdependencies of those quality attributes, highlighting trade-off mechanisms and opportunities between quality attributes [9]. Another factor is the combination of a risk analysis. The goal of identifying potential risks can be a normal part of the architecture review. The framework supplements the use of a well-known risk analysis model for application security called OWASP's Risk Rating Methodology [73].

Integrating security patterns to the framework enhances the quality of security components in the architecture. The framework includes security patterns not only for the risk analysis, but also as a core component of each security scenarios that contains the security profile. The scenario-based evaluation framework includes six phases that are defining the evaluation goal, generating security scenarios, creating the security profile, describing the architecture, evaluating scenarios and analyzing results. The evaluation process with these six phases is illustrated in Figure 24.

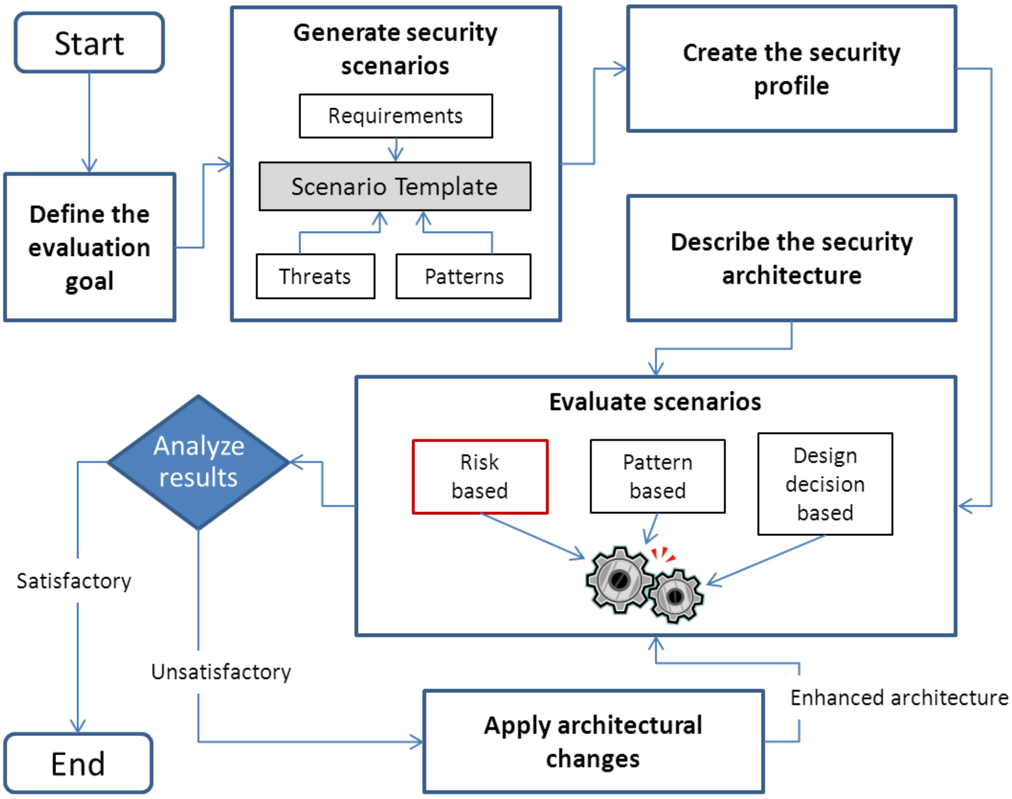


Figure 24: The security evaluation framework.

Defining the Evaluation Goal

The first phase is to determine the goal of the evaluation. This includes the declaration of the expected outcomes of this evaluation. Typically, the assessment process may have three types of goals; quantitative, qualitative or trade-off. In the quantitative assessment, the goal is to predict the level of security supported by the architecture. In many cases, a prediction is supposed to be an indicator rather than an absolute quantitative measure of security which may not even be feasible with all designs.

The goal with qualitative assessment is to compare two or more possible candidate architectures to decide which supports the best security. The trade-off assessment attempts to discover the right level of the security support with respect to other quality attributes of the target system.

Generating Security Scenarios

The second phase of the process is to create the security scenarios. A coherent and logical security scenario is a key for the relevant evaluation results. To generate a reasonable scenario, threat modeling and security requirements must be considered closely. Threats can be well defined and classified using several threat models [89]. However, it is not clear how the threat profiles could be used as an assessment instrument. Also, security requirements by themselves are not enough to build a security scenario. The security requirements describe a threat to the system in the context of functional requirements, but do not consider the threat profiles. Thus, a beneficial security scenario is a combination of security threats, requirements and patterns [9].

Alkussayer and Allen [9] propose a systematic approach to generate a coherent security scenario. The formal definition of the security scenario is as follows:

$$S = \{s_1, s_2, \dots s_n\}, \tag{7}$$

where S is the set of security scenarios such that s_i corresponds to the security scenario for the threat i, and n is the total number of identified threats. The scenario s_i is described as a tuple:

$$s_i = (r_i, t_i, p_i), \tag{8}$$

where $r_i \in R$, $t_i \in T$ and $p_i \in P$. R, T, and P represent security requirements, threats, and security patterns respectively. The template includes five elements that are requirement, threat, precondition, behavior, and patterns.

A *requirement* is the specific security requirement describing the desired security property of the target system. It is significant to be able to trace a security scenario back to its fundamental requirements because of understanding different trade-offs.

A *threat* is an act to elicit a negative response in the system. The threat may explicitly (directly) or implicitly (indirectly) violate the security requirement. The threat must be imported from the threat profile [89].

Precondition is the description of potential system constraints that may cause the security scenario to occur.

Behavior is the expected behavior of the system when a specific scenario is tested. It is important to focus exclusively on security and avoid defining the system behavior from other quality-attribute viewpoints (e.g. performance).

Patterns should to be combined in order to mitigate the corresponding threat and protect the required behavior.

Each threat scenario is linked to a specific security requirements, potential threats, and security pattern(s) that may be used to remediate that threat.

Creating Security Profile

The security scenario profile includes the identified security scenarios that are going to be used during the evaluation analysis of the security architecture. Two key factors that impact on the generation of the scenario profile are selection criteria and prioritization.

A complete selection includes all scenarios that may potentially occur. Although it is essential to include all identified scenarios into the profile, the complete selection is impossible to achieve because security is a moving target and new threats are developing all the time changing the threat landscape continuously. Thus, an appropriate method for selection of representative scenarios depends on the risk related to each scenario. The process of associating risk values with each scenario in the profile is described using the standard risk model [73]:

$$\textit{Risk} = \textit{Likelihood x Impact} \qquad (9)$$

The OWASP Risk Rating Methodology (RRM) proposes two factors to estimate the risk likelihood and two factors to estimate the risk impact. The risk likelihood is estimated using a threat agent factor or a vulnerability factor. The risk impact is evaluated using a technical factor or a business factor. Each of these four factors has a set of options which have rating from 0 to 9. In this study, the risk likelihood is based on the vulnerability factors, and the risk impact estimation is provided through the technical factors. The threat agent factor and the business impact factor have been omitted to maintain simplicity. In a military context, the business factor is not very relevant as the ultimate goal is to maintain the network operational in all conditions.

The OWASP Risk Rating Methodology uses the simple numerical values (0-9) during the estimation process to simplify the analysis process. The numerical values are replaced by the corresponding rating levels later in the process. The likelihood and impact levels of are:

$0 \leq 3$	Low
$3 \leq 6$	Medium
$6 – 9$	High.

The Full Scenario Table (FST) is used to extract scenarios from the security scenario profile. The output of the process is a simplified representation of the security scenario profile with a set of scenarios. During the process, all of the scenarios (*S*) developed in the previous phase are entered into the FST. The FST consists of four columns that are the scenario number, threat, patterns, and security objectives. The security objectives column is divided into sub-columns that represent the desired security objectives of the system.

It is normal to generate some scenarios without associated patterns because of two reasons. First, a pattern for newly emerged threats may not exist, and secondly, the cyber threat is to be mitigated by using an established best practice. In any case, it is vital to include the scenarios without patterns in the Full Scenario Table to assure that the security architecture has addressed all the threats and their countermeasures. An example of FST is presented in Figure 25.

Scenario #	Threat	Patterns	Security Objectives							Risk
			SO_1	SO_2	SO_3	SO_4	SO_5	SO_6	SO_7	
1	Denial-of-Service	α_1	5	5	9	1	2	2	4	High
1	SQL Injection	α_2, α_3	8	4	9	9	4	5	9	Medium
3	Data Storage Attack	-	3	4	8	9	9	3	8	Critical

Figure 25: An example of Full Scenario Table (FST).

Threats and patterns to protect against threat are located in the second and third column of the table. The following columns include the evaluation how a certain security objective is achieved. Finally, the risk value is calculated in the last column. The purpose of the prioritization of the profile is to highlight the scenarios that include more risks. The security scenarios are prioritized by using the risk level identified earlier in the FST.

Evaluating the Scenarios

Evaluating the cyber security architecture is provided by comparing the required security functionalities with the provided security capabilities. The scenarios in the Full Scenario Table indicate the required security functionalities of the system. The security scenarios profile generated earlier is used for the evaluation process in which the security architecture is analyzed for its support of each security scenario.

The security evaluation framework (see Figure 24) introduces three methods for scenario evaluation; pattern-based, risk-based and design decision-based evaluation. The pattern-based evaluation requires examining each scenario from the security profile and heuristically evaluating the architecture using the list of identified patterns in the scenario. A challenge with this method is that it requires expert-based identification of any security pattern that influences security in the system [9].

The design decision-based evaluation is based on analysis of the structural components of the system and their interrelationship. Every design decision that is identified is used to evaluate the security support for each security scenario. For each scenario in the security profile, the impact of the design decision is analyzed, and whether this decision has resulted in sufficient support for the scenario.

The risk-based evaluation is a process that estimates and associates risk weights to every scenario row in the Full Scenario Table. The evaluation is conducted by estimating the impact and likelihood of each scenario. The technical impact I_{s_i} of a scenario s_i in the Full Scenario Table is described as the average of the impacts I on corresponding security objectives SO_j when threat in the scenario is realized. The formalization of this calculation is defined by:

$$I_{s_i} = \frac{I(SO_1\ s_i\ )+I(SO_2\ s_i\ )+\cdots I(SO_j\ s_i\ )}{j\ _1} \qquad (10)$$

The vulnerability factor VF_{s_i} of the scenario s_i is estimated by averaging the vulnerability factors VF_j for each scenario s_i. The average is calculated by the following:

$$VF_{s_i} = \frac{VF_1\ s_i\ + VF_2\ s_i\ + \cdots VF_j(s_i)}{j\ \ 1} \tag{11}$$

If a scenario consists security patterns, their improvement effect ($\alpha_{s_{i_1}}$, $\alpha_{s_{i_2}}$,…, $\alpha_{s_{i_n}}$) is defined to reduce the likelihood estimation of the scenario. However, patterns vary in their expected resistance to attacks and hence the lack of pattern resistance *LPR* is determined. If multiple patterns are applied to a single scenario s_i, then $LPR_{s_i}$is as follows:

$$LPR_{s_i} = 1 - Min(\alpha_{s_i j}) \tag{12}$$

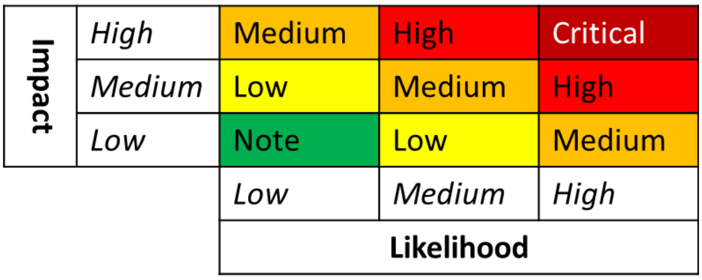
Finally, the likelihood of the scenario s_i is calculated by:

$$L_{s_i} = VF_{s_i} * LPR_{s_i} \tag{13}$$

The risk $R_{s_i}$of the scenario s_i could be then calculated by using the standard risk equation:

$$R_{s_i} = L_{s_i} * I_{s_i} \tag{14}$$

Figure 26 illustrates the RRM [11] severity levels. The overall risk severity level is achieved as a combination of the levels of impact and likelihood. For example, if the impact level is high and the likelihood level is medium, the final risk level is high. Focusing on severity levels to complete the risk evaluation may take a purer meaning and draw greater attention than numerical values. Thus, it is recommended to use the severity levels in the scenario based evaluation [9].



Impact	*High*	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	*Medium*	*High*
		Likelihood		

Figure 26: Risk severity levels.

In the end of the evaluation process, the results from the overall analysis of the architecture are summarized which may disclose some general security indicators. For example, the number of supported security scenarios can be compared with the number of scenarios not supported, or the total number of available security patterns (controls) can be compared with the number of patterns (controls) required by the profile.

Also, it is possible to synthesize risk values associated with each threat to the scenario template. As a result, an overall quantitative indicator of the evaluation can be determined. However, such a quantitative metric of the software design is outside the scope of this paper. During the evaluation process, the accumulated results must be documented. If the desired security level is not achieved, then some architectural modification must be applied to overcome the lack of security support.

6.4. Evaluation Results

The proposed cyber security architecture was evaluated by applying the previously presented evaluation methods. The architecture was valued against the four threat scenarios presented in Table 7. The scenarios describe typical threat scenarios concerning tactical military networks. An adversary launches attacks to achieve desired effects on an opponent’s networks. A primary target may often be classified information, but the enemy may also want to deny the availability of network services. Instead of launching cyber attacks through networks, the enemy can use kinetic power to destroy a critical node or databases. The tested scenarios are not complete as it was stated earlier, but they may cover most of the current cyber threats.

Results of SABSA Based Evaluation

The SABSA based evaluation was executed by analyzing the architecture with the SABSA matrix. The evaluation matrix was generated for each threat scenario as demonstrated in Figure 23. All the threats of each threat scenario are estimated through the layers of the SABSA matrix. The purpose is to analyze how the architectural design with the security elements and the cognitive functionalities overcome the requirements for security at each SABSA layer.

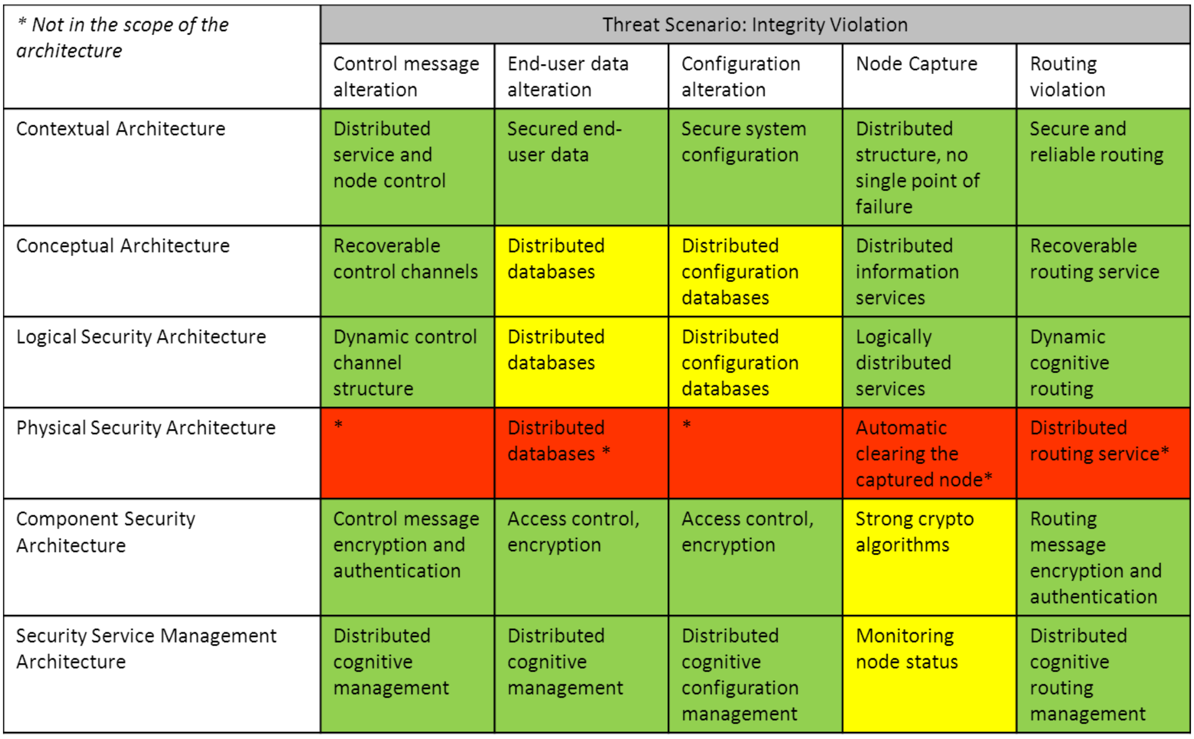
The analysis is provided by considering each threat and the security controls of the architecture against the objectives presented in Table 15. As a result, a matrix cell describes how the architecture mitigates the threat at each SABSA layer. For example, when analyzing the Conceptual Architecture layer, the targets of security include availability of critical operational information, information sharing with strategic partners, and recoverable networks and information services. By examining the overall architecture and the tasks of each security element and layer, it is possible to see if any mechanisms for protection exist.

The evaluation results are presented in Tables 16 - 19. The colors in the matrices indicate the fulfillment of the requirements. The green color indicates that the architecture meets the security requirements for a threat. The yellow color shows that the architecture does not fully meet the requirements, and the functionality of the elements must be improved. The red color indicates that the design fails, and the architecture does not include the functions to protect information against a specific threat at a certain SABSA layer. It is important to notice that the physical protection is not in the scope of the architecture, and thus, the physical security layer results in the yellow color. However, some security features also protect against physical damages.

When examining the SABSA evaluation results it should be noted that the results presented in the tables are mostly based on the author's analysis and understanding of the functionality of the proposed architecture and its layers and security elements. The results could not have been directly calculated quantitatively using mathematical formulas. This is of course natural, since the architecture or its performance is not described mathematically, and the technical parameters of the architecture have not been determined precisely.

On the other hand, the attack patterns of the threats in each threat scenario are not specified or described. For example, the attacker’s cyber knowledge, tools and resources are unknown, and, the exact knowledge of used vulnerability or attack methods is missing. Therefore, these results should be interpreted carefully.

Table 16: Evaluation of the architecture against the scenario of integrity violation.



** Not in the scope of the architecture*	Threat Scenario: Integrity Violation				
	Control message alteration	End-user data alteration	Configuration alteration	Node Capture	Routing violation
Contextual Architecture	🟩 Distributed service and node control	🟩 Secured end-user data	🟩 Secure system configuration	🟩 Distributed structure, no single point of failure	🟩 Secure and reliable routing
Conceptual Architecture	🟩 Recoverable control channels	🟨 Distributed databases	🟨 Distributed configuration databases	🟩 Distributed information services	🟩 Recoverable routing service
Logical Security Architecture	🟩 Dynamic control channel structure	🟨 Distributed databases	🟨 Distributed configuration databases	🟩 Logically distributed services	🟩 Dynamic cognitive routing
Physical Security Architecture	🟥 *	🟥 Distributed databases *	🟥 *	🟥 Automatic clearing the captured node*	🟥 Distributed routing service*
Component Security Architecture	🟩 Control message encryption and authentication	🟩 Access control, encryption	🟩 Access control, encryption	🟨 Strong crypto algorithms	🟩 Routing message encryption and authentication
Security Service Management Architecture	🟩 Distributed cognitive management	🟩 Distributed cognitive management	🟩 Distributed cognitive configuration management	🟨 Monitoring node status	🟩 Distributed cognitive routing management

Table 16 presents the evaluation results in the threat scenario of integrity violation. As it is seen in the table, the purposed architecture seems to support the protection of integrity violation against each cyber threat. At the contextual layer, the architecture presents distributed services and controls and secured data services to prevent user data, routing and configuration alteration and violation. The main weaknesses in the scenario are in the protection against node capture. By monitoring nodes and using strong cryptographic algorithms it is possible to check that the nodes are under control and data stored in a node is secured. The strong algorithms are naturally more difficult to break but it is still just a matter of time when the most of cryptographic algorithms are to be broken [59].

Table 17 shows the evaluation results in the threat scenario of the prevention of availability. All the threats in the table have a goal of denying availability of network access and services. At the Contextual, Conceptual and Logical layers the cyber security architecture uses distributed and cognitive security services providing continuous in network and service operations as the network has no single point of service production. On the other hand, the cognitive process takes care of dynamic service reconfiguration so that blocked services is set up in a new location or/and with new parameters.

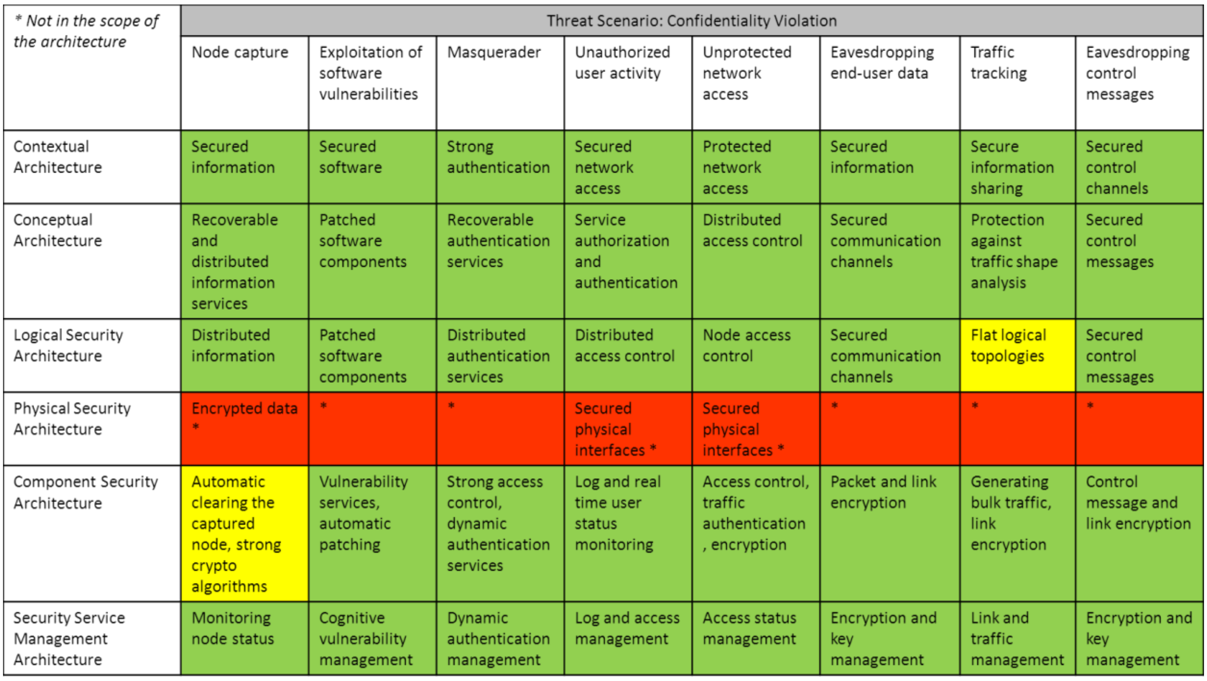
Table 17: Evaluation of the architecture against the scenario of the prevention of availability.

** Not in the scope of the architecture*	Threat Scenario: Prevention of Availability					
	Flooding	Node capture	Malformed control messages	Connection hijacking	Quality-of-Service abuse	Server impersonating
Contextual Architecture	Continuous services	Continuous services	Continuous services	Continuous services	Continuous services	Continuous services
Conceptual Architecture	Recoverable services	Recoverable services	Recoverable services	Recoverable connections	Recoverable services	Recoverable services
Logical Security Architecture	Distributed services	Distributed services	Secure control channels	Alternative connections	Secure control channels	Distributed information servers
Physical Security Architecture	*	*	*	*	*	Distributed information servers *
Component Security Architecture	Packet authentication, traffic filtering	Automatic clearing the captured node	Control message authentication	Packet encryption and authentication	QoS control message encryption and authentication	Server access control
Security Service Management Architecture	Monitoring connection availability and status	Monitoring node status, disconnecting captured nodes	Authentication management	Dynamic connection management	Secure QoS management	Access control management

At the Component Security layer, the architecture protects against availability prevention by having authentication, encryption and traffic filtering capabilities in each network node. At the security service management layer, traffic and status monitoring ensures that anomalous packets are dropped. The control message authentication prevents unauthorized control messages to cause denial of services.

Table 18 shows the evaluation results in the threat scenario of the confidentiality violation. At the highest layers of the SABSA matrix, the threat is defended by having secured information processing and sharing with strong authentication and encryption. At the Component level, the threats are minimized through the security elements of the architecture.

Table 18: Evaluation of the architecture against the scenario of confidentiality violation.

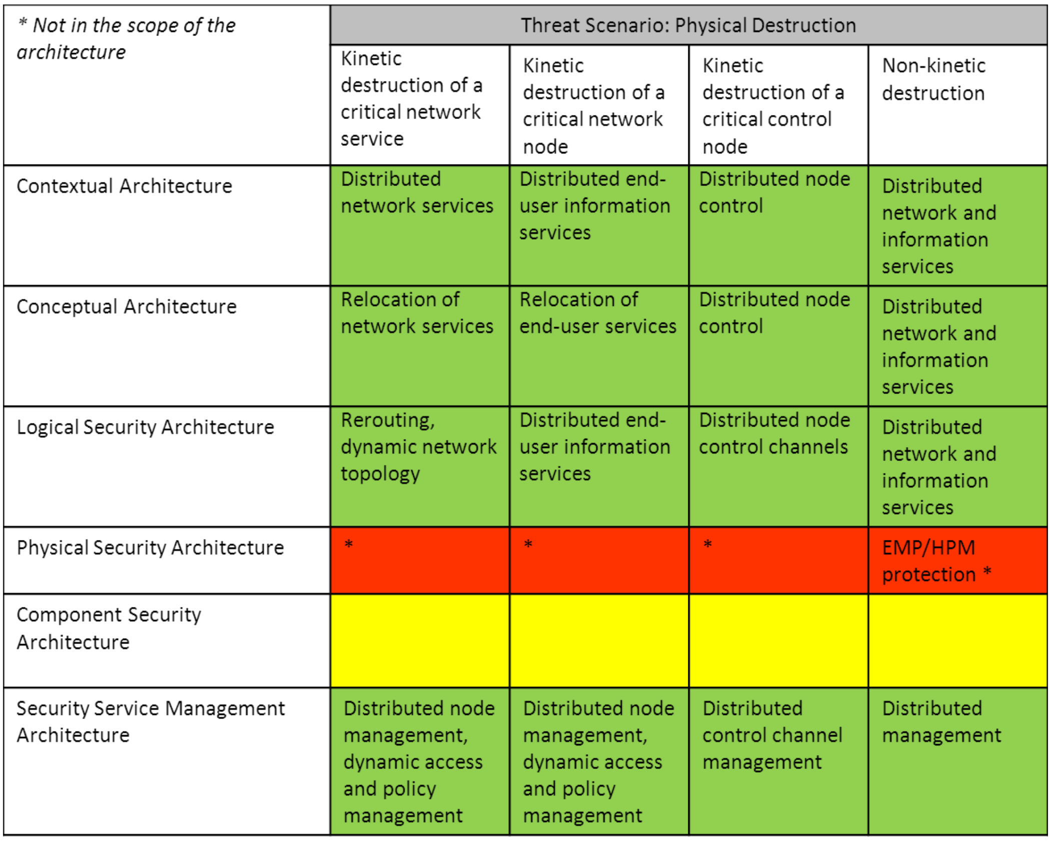


** Not in the scope of the architecture*	Threat Scenario: Confidentiality Violation							
	Node capture	Exploitation of software vulnerabilities	Masquerader	Unauthorized user activity	Unprotected network access	Eavesdropping end-user data	Traffic tracking	Eavesdropping control messages
Contextual Architecture	Secured information	Secured software	Strong authentication	Secured network access	Protected network access	Secured information	Secure information sharing	Secured control channels
Conceptual Architecture	Recoverable and distributed information services	Patched software components	Recoverable authentication services	Service authorization and authentication	Distributed access control	Secured communication channels	Protection against traffic shape analysis	Secured control messages
Logical Security Architecture	Distributed information	Patched software components	Distributed authentication services	Distributed access control	Node access control	Secured communication channels	Flat logical topologies	Secured control messages
Physical Security Architecture	Encrypted data *	*	*	Secured physical interfaces *	Secured physical interfaces *	*	*	*
Component Security Architecture	Automatic clearing the captured node, strong crypto algorithms	Vulnerability services, automatic patching	Strong access control, dynamic authentication services	Log and real time user status monitoring	Access control, traffic authentication , encryption	Packet and link encryption	Generating bulk traffic, link encryption	Control message and link encryption
Security Service Management Architecture	Monitoring node status	Cognitive vulnerability management	Dynamic authentication management	Log and access management	Access status management	Encryption and key management	Link and traffic management	Encryption and key management

The confidentiality violation threat through node capturing is difficult to counter as the captured node is open to an enemy to investigate databases and security control structure. With automated data clearing and strong cryptographic algorithms the threat is trying to be minimized. Other unsatisfied security implementations concern the unprotected network access and traffic tracking at the logical level. The proposed architecture does not propose any mechanism to provide the flat logical topology.

The evaluation results in the threat scenario of the physical destruction are presented in Table 19. At the three highest layers of the SABSA model, the physical destruction threat is mitigated by implementing distributed information services and node control in order to leaving no single point of failure in a case of physical influence.

Table 19: Evaluation of the architecture against the physical destruction scenario.



** Not in the scope of the architecture*	Threat Scenario: Physical Destruction			
	Kinetic destruction of a critical network service	Kinetic destruction of a critical network node	Kinetic destruction of a critical control node	Non-kinetic destruction
Contextual Architecture	Distributed network services	Distributed end-user information services	Distributed node control	Distributed network and information services
Conceptual Architecture	Relocation of network services	Relocation of end-user services	Distributed node control	Distributed network and information services
Logical Security Architecture	Rerouting, dynamic network topology	Distributed end-user information services	Distributed node control channels	Distributed network and information services
Physical Security Architecture	*	*	*	EMP/HPM protection *
Component Security Architecture	🟨	🟨	🟨	🟨
Security Service Management Architecture	Distributed node management, dynamic access and policy management	Distributed node management, dynamic access and policy management	Distributed control channel management	Distributed management

The proposed architecture does not include any physical protection at the component level which is seen as the yellow color in the matrix. However, the distributed and cognitive services fill the holes in physical protection in many cases. The system management is distributed among all the network nodes so that losing the network nodes does not disable the network management services.

Results of Scenario Based Evaluation

The first step in the scenario based evaluation is to determine the goal of the evaluation. In this evaluation, the goal was to evaluate the security risk of the proposed architecture design. In the second step, the threat scenarios presented in Table 6 were chosen for the evaluation. The scenarios include a total of 24 threats. The third step is to create the security scenario profile using the FST. Each threat was analyzed against specific security requirements, and security pattern(s) that are designed in the proposed architecture to remediate that threat.

For technical impact factors and vulnerability factors we use the values presented in Tables 20 and 21 are used. The factors are based on the OWASP Risk Rating Methodology [73]. The impact and vulnerability factors are derived from the security dimensions listed in Table 2. Finally the impact and vulnerability factors were calculated using Equations (10) - (13).

Table 20: Technical Impact Factors.

Impact Factor	Definition	Rating
Loss of Confidentiality (LC)	How much data could be disclosed and how sensitive it is.	2 = Minimal non-sensitive data disclosed 6 = Minimal critical data disclosed 6 = Extensive non-sensitive data disclosed 9 = Extensive critical data disclosed, all data disclosed
Loss of Integrity (LI)	How much data could be corrupted and how damaged it is.	1 = Minimal slightly corrupt data 3 = Minimal seriously corrupt data 5 = Extensive slightly corrupt data 7 = Extensive seriously corrupt data 9 = All data totally corrupt
Loss of Availability (LA)	How much service could be lost and how vital it is.	1 = Minimal secondary services interrupted 5 = Minimal primary services interrupted 5 = Extensive secondary services interrupted 7 = Extensive primary services interrupted 9 = All services completely lost
Loss of Accountability (LAC)	Actions by the attackers can be traced to an individual.	1 = Fully traceable 7 = Possibly traceable 9 = Completely anonymous

Table 21: Vulnerability Factors.

Impact Factor	Definition	Rating
Ease of discovery (ED)	How easy it is for attackers to discover the vulnerability.	1 = Practically impossible 3 = Difficult 7 = Easy 9 = Automated tools available
Ease of exploit (EE)	How easy it is for attackers to actually exploit the vulnerability.	1= Theoretical 3 = Difficult 5 = Easy 9 = Automated tools available
Awareness (AW)	How well known this vulnerability is to the attackers.	1 = Unknown 4 = Hidden 6 = Obvious 9 = Public knowledge
Intrusion detection (ID)	How likely an exploit is to be detected.	1 = Active detection in application 3 = Logged and reviewed 8 = Logged without review 9 = Not logged

The results are presented in Tables 22 - 25. A risk value (the last column in the tables) has been resulted by first calculating the average values of the impact factors (LC, LI, LA, LAC) and the vulnerability factors (ED, EE, AW, ID). Then, the influence of the security patterns (security controls and functionality of the architecture) is reduced from the averaged vulnerability factor by multiplying the vulnerability factor with the lack of pattern resistance defined by Equation (12). The security elements are denoted with the acronyms presented in Sections 5.3 - 5.5. The improvement effect α of the security elements gets the values from 0 to 1 where 1 equals to full mitigation (no vulnerability).

Finally, the numerical values are converted to the likelihood and impact levels (low $0 \leq 3$, medium $3 \leq 6$ and high $6 – 9$), and the final risk value is obtained by using the risk severity levels of the table presented in Figure 27. We must note that the assignment of technical impacts, vulnerability factors, and pattern resistance (improvement effect) is done based on the author's experience and literature review. Thus, the numerical values in the tables are not based on any mathematical analysis.

The Full Scenario Table of the integrity violation scenario is presented in Table 22. The column of Security Controls defines what controls in the architecture mitigate the threat at each line. A numerical value in brackets indicates an estimated value of the improvement effect. For example, in the case of End-user data alteration (#2) the average of the impact factors is 2.00. The average of the vulnerability factors (3.25) is multiplied by the lack of pattern resistance (LPR = 1 - 0.9) which leads to the likelihood value of 0.325. Thus, the both likelihood and impact factors are low, and the final risk severity level is note. The risk severity level of the other threats is calculated in the same way.

Table 22: The Full Scenario Table for the integrity violation scenario.

#	Threat	Security Controls (α)	Impact Factors				Vulnerability Factors				Risk
			LC	LI	LA	LAC	ED	EE	AW	ID	
1	Control message alteration	CE, PACE (0.8)	1	1	6	-	3	2	4	1	Note
2	End-user data alteration	CE, PACE, AACE (0.9)	2	3	1	-	3	3	5	2	Note
3	Configuration alteration	CE, PACE, MACE (0.9)	2	3	5	-	3	5	6	2	Medium
4	Node capture (I)	CE, TMFE (0.3)	4	3	1	4	5	6	8	2	Medium
5	Routing violation	CE, RSE (0.7)	1	2	3	-	3	2	3	1	Note

The Full Scenario Table of the prevention of availability scenario is presented in Table 23. In the prevention of availability scenario, the threat of corrupting critical data is small compared to the impact on service and data availability. The main security controls against the threats are packet authentication, distributed services, cryptography, and traffic monitoring. The table shows that the availability prevention threat is mainly low with the security elements and functions proposed in the architecture. The risk level of availability prevention in the node capture threat is medium indicating that it is difficult to protect data and services in a captured node.

Table 23: The Full Scenario Table for the prevention of availability scenario.

#	Threat	Security Controls (α)	Impact Factors				Vulnerability Factors				Risk
			LC	LI	LA	LAC	ED	EE	AW	ID	
6	Flooding	PACE, TMFE, RSE (0.8)	1	1	7	8	9	8	8	1	Low
7	Node capture (A)	Distributed services, Cognitive service management (0.2)	6	1	9	7	7	7	8	2	Medium
8	Malformed control messages	CE, PACE (0.6)	1	1	7	8	8	8	6	2	Low
9	Connection hijacking	TMFE, RSE, cognitive link management (0.8)	1	1	3	6	3	5	8	3	Low
10	Quality-of-Service abuse	CE, PACE (0.6)	1	1	5	8	5	3	7	2	Low
11	Server impersonating	MACE, PACE, CE, TMFE (0.9)	1	1	9	8	6	5	8	2	Low

Table 24 presents the Full Scenario Table of the confidentiality violation scenario. The table shows the highest risk caused by masqueraders, which is obvious because it is very difficult to detect a illegitimate user with a valid ID. Node capture, software vulnerabilities and unauthorized activities are a medium risk. All the others provide low or very low risks. Losing confidentiality and integrity are valued high with the most of the threats because in this threat scenario the initial purpose is to discover data. However, the vulnerability factors are estimated quite low and the security controls lower the likelihood value even more.

Table 24: The Full Scenario Table for the confidentiality violation scenario.

#	Threat	Security Controls (α)	Impact Factors				Vulnerability Factors				Risk
			LC	LI	LA	LAC	ED	EE	AW	ID	
12	Node capture (C)	CE (0.7)	9	9	6	3	6	5	8	2	Medium
13	Exploitation of software vulnerabilities	VME (0.7)	9	9	7	6	4	6	7	5	Medium
14	Masqueraders	SACE, AACE (0.2)	9	8	4	9	8	3	9	7	High
15	Unauthorized user activity	SACE, AACE (0.8)	8	7	7	8	3	4	5	1	Medium
16	Unprotected network access	NACE (0.9)	9	3	3	5	3	6	2	2	Low
17	Unprotected data links	CE (0.7)	7	4	2	7	6	3	2	2	Low
18	Eavesdropping end-user data	CE (0.7)	9	2	2	8	7	3	5	8	Low
19	Traffic tracking	TSE, CE (0.8)	1	1	1	9	8	7	6	7	Note
20	Eavesdropping control messages	CE (0.7)	7	2	1	8	7	3	5	8	Low

The Full Scenario Table of the physical destruction scenario is presented in Table 25. Loss of Accountability is estimated to be at the level of 5 meaning that the attacker is possibly traceable. Also, The Ease of discovery factor is set to 5 as locating a single network node is possible but not always very easy. The Awareness and the Ease of exploit factors have very high values because physical destruction is easy to conduct when a target is located. The intrusion detection factor is set to 1 as it is quite easy to notice when a node is damaged by physical means. The proposed architecture present distributed services and management as well as cognitive rerouting which occurs as a high value of the improvement effect (0.9).

Table 25: The Full Scenario Table for the physical destruction scenario.

#	Threat	Security Controls (*α*)	Impact Factors				Vulnerability Factors				Risk
			LC	LI	LA	LAC	ED	EE	AW	ID	
21	Kinetic destruction of a critical network service	Distributed services (0.9)	1	6	9	5	5	9	9	1	Low
22	Kinetic destruction of a critical network node	Cognitive packet rerouting (0.9)	1	3	1	5	5	9	9	1	Note
23	Kinetic destruction of a critical control node	Distributed management (0.9)	1	3	5	5	5	9	9	1	Note
24	Non-kinetic destruction	EMP/HPM protection (-)	1	7	8	5	5	9	9	1	High

The table indicates that the risk of losing data or services by physical destruction is low or very low in a distributed system. The high risk severity level presented in the table concerns non-kinetic destruction (EMP/HPM) for which the proposed architecture contains no countermeasures as the EMP and HPM protection is out of the scope of the cyber security architecture. However, implementing military networking devices the HPM/EMP protection is one of primary requirements.

6.5. Conclusions

Evaluating a cyber security architecture is a very challenging issue. Although several different evaluation criteria and methods exist, using these methods for technical cyber security is not so straightforward. A problem is that different evaluation criteria are created for auditing existing devices. They are not designed for evaluating a high level security architecture with functional properties. The reviewed criteria such as Common Criteria are relevant for checking a product fulfills its security requirements. The criteria do not set, for example, threat scenarios which the security features are tested against.

Because of the challenge with the existing evaluation methods, two different approaches were chosen to carry out the evaluation of the proposed cyber security architecture. The first approach was to use the SABSA framework not for security design but for evaluation. The framework contains a broad 360 degree view on enterprise level security. Thus, it was interesting to see how the SABSA framework applies to evaluation tasks. The second approach uses a scenario based evaluation presented in an academic research paper in 2010. The paper describes a framework for calculating risk severity levels of each threat on computer software. The framework designed for evaluating software security also looked promising for evaluating security of a communication network.

The chosen evaluation methods were applied to all four threat scenarios with the specific threats. Both the methods provided four tables of the evaluation results. The tables show that the proposed architecture with the security elements and cognitive capabilities is able to mitigate the most of the threats, at least at the high level. As we see in the SABSA evaluation matrices, the architecture has functional solutions to mitigate the threats at almost all the SABSA layers. The major weaknesses are at the physical layer, but this is natural as physical security is not in the scope of the proposed architecture.

Another weakness concerns the highest layers of the SABSA matrix as those layers deal with very high level organizational and business issues that are not discussed and defined in the proposed architecture. The cyber security architecture only includes technical functionalities for architectural components. However, the cognitive capabilities are able to meet the high level challenges in many cases through the end-to-end goals.

Also, the results of the scenario based evaluation show that the proposed architecture mitigates the most of the threats. The risk level with most of the threats is low or very low (note). Cryptography, access control and traffic monitoring are key enablers to mitigate the threats. The high risk results in the full scenario tables concern masqueraders and non-kinetic weapons. Masqueraders (using stolen IDs) are difficult to detect, and it is problematic to prevent them to access services and data even if a network has strong security controls. The architecture does not contain any protection against non-kinetic weapons, and thus the threat causes a high risk.

In practice, the evaluation using the chosen methods was very challenging to process, and the results must be considered very critically. In the scenario based evaluation both the values of the impact and vulnerability factors, and the improvement effects were based on the author's estimations. With certain threats it was hard to estimate for example the level of vulnerability or loss of accountability. Similarly, the improvement effect of each security element was challenging to exactly estimate, because the evaluation methods included no mathematical analysis for calculating the level of protection of a single security element.

Due to the difficulties with the evaluation methods, the evaluation results must be seen more as examples or a demonstration than exact and correct results. The evaluation methods as they were applied do not give proper answers to the question of how secure a network is when the proposed cyber security architecture is used. In addition to the problem of quantifying security, a problem of quantifying the threat is also present. Now, the architecture was evaluated against a limited set of threats. In real life, cyber domain sets no limits for attacking techniques.

Adversaries are continuously seeking new vulnerabilities and attacking methods to penetrate target systems. When a security control is implemented, the threat may already be changed. The proposed cognitive features are ideal for this kind of dynamic threat environments as the cognitive process is able to reconfigure the network system to also mitigate the newest threats.

Although, the evaluation of the cyber security architecture did not produce the most reliable results, the results may roughly show that the designed security controls have added value to the military network. The results also showed that the evaluation methods and process must be developed.

7. CONCLUSIONS

In this chapter, the main research results of the thesis are presented. The chapter also discusses on reliability and validity of the study, and defines issues for the future work. The aim is to summarize the research results, and to evaluate the quality of the thesis and the research process.

7.1. Research Results

The main problem of this research was to describe how the cyber security architecture for tactical military networking should be designed using the attributes of the cognitive networks. The main purpose was to develop an architecture that meets the security requirements and utilizes cognitive networking features. An important part of the study was the evaluation of the proposed architecture to verify that the architectural solutions are relevant and they provide the desired security capabilities.

As concluded in Chapter 2, the military networking environment is difficult for networking. The networks should be mobile, reliable and secure at the same time. NCW requires that the networks and information services have enough data processing and sharing capacity, and the network is able to maintain continuous connections between the network nodes. To gain information superiority a commander and other decision-makers must have relevant information services and sources available during a military operation. The military information systems must be secured so that information confidentiality, integrity and availability are sustained. The systems must support processing information at different classification levels (from public to top secret information).

Cyberspace, cyber warfare and cyber threats, discussed in Chapter 3, are the hot topics of media in today’s networked world. Cyberspace extends everywhere with integrated circuits and computers. It seems like our physical world does not function without the capabilities of cyberspace. Dependency on networks and the Internet also concerns armed forces and their operational information systems. This dependency creates new cyber threats to the military networks and information systems. Cyberspace is easy to access and operate, and it has also become a new playground of nation actors that furiously develop new cyber weapons and doctrines to utilize cyberspace.

The cyber threat is complex and dynamic. Target systems could be attacked in several ways, and the modern attacking methods are very advanced to bypass defensive security controls and boundaries. The development of cyber exploits is cost-effective and only requires a deep knowledge of computer software and hardware. Cyber warfare requires no massive investments to armaments. Also, the mass of potential hostile actors is a huge. Protecting military networks demands new innovative approaches in both offensive (proactive) and defensive (reactive) manners.

The challenge with the legacy military networks is that they are often based technologies invented and implemented already decades ago. Defensive security measures are later added on causing a risk of unmanageable system configurations. The systems suffer the lack of overall security management, dynamic security configuration and threat assessment. The static configurations and system structures are easier targets to the enemy’s intelligence. It would be more benefit to build new information services dynamically so that the systems become a moving target to the adversary.

The cognitive networks, introduced in Chapter 4, are a promising research field to provide smart, dynamic, and self-learning networking capabilities. The cognitive process could help operating military networks and make them even more secure as the error-sensitive manual configuration of the networks is removed. Adaptive and automated network management also helps to maintain systems updated and configured to protect the systems against the rapidly changing cyber threat.

Due to the weaknesses of the existing security architecture models and frameworks, a five-layer cyber security architecture model was presented. The architecture includes the infrastructure, service and application security layers consisting of several security elements. Each of the elements has its own tasks to provide security controls and protection to provide data confidentiality, integrity and availability. The cognitive layer is located upon these three layers, and it acts as “brains” for the communication network. The layer controls all the security elements, and adapts system parameters dynamically. The fifth layer is a management layer at which end-to-end goals are set according to security policies and cyber threats.

The proposed architecture uses the separated cognitive layer to collect status data and to control software defined security elements. The layer runs a cognitive process that improves the overall management of security controls and parameters. The cognitive layer also builds situational awareness of system security, and the layer is a key element to provide Defense in Depth capabilities. The cognitive layer ensures that the network system has continuously several protective layers to be passed by an attacker, and countermeasures and offensive actions are started immediately during a cyber attack.

In theory, the architecture solves most of the problem with the legacy military networks. The proposed wit the cognitive process enables dynamic network and security configurations. The security controls and mechanisms built-in at each network node provide a distributed and reliable security services. The cognitive layer is able to provide the overall management of the security parameters and configurations including key distribution, encryption algorithms, and authentication. The proposed architecture does not define security protocols, hence the lack of light-weight security protocols is not removed with the architecture.

The evaluation of a security architecture is necessary, but also difficult. It is critical to verify that the architecture fulfills its requirements. The existing information security criteria proved to be impossible to be applied for evaluating a high-level cyber security architecture. Available evaluation methods are typically designed for implemented security devices and software, and evaluation methods created especially for security architectures could not be found. Thus, the proposed architecture was evaluated using two uncommon methods; the SABSA matrix and the scenario based evaluation method. The evaluation became very challenging, because mathematical analysis could not be applied to the architecture without performance parameters or values.

The both evaluation methods only produced rough evaluation results that must be considered very critically. The quality of the architectural design cannot be fully verified basing on the results. However, the results show that the proposed architecture includes elements that may mitigate the cyber threats with a high probability, but some of the threats such as the masqueraders and node capture are still difficult to counter.

Quantifying the functionality and performance of the security elements would help analyzing the overall quality of a cyber security architecture. Now, the analysis was mostly based on the author’s estimation of the capability (improvement effect) of each security element. Similarly, the threat impact and vulnerability factors were just roughly estimated without a deeper knowledge or mathematical analysis. However, the scenario based evaluation method is promising as it uses a mathematical approach for calculating a risk severity level of the architecture.

Finally, the main conclusions of this thesis can be summarized as follows:

1. Cyber threat is rapidly growing and changing which means that new approaches to build secure military networking systems are required.

2. The features of the cognitive networks will improve networking capabilities including overall network security and threat management.

3. This study proposes a five-layer cyber security architecture with cognitive control that provides appropriate security features and protection for a military network system.

4. Evaluation a cyber security architecture is not trivial because of lacking relevant evaluation methods. The evaluation results are only indicative, and the evaluation processes should be considered as examples.

7.2. Discussion

The original idea and process of building a new security architecture for tactical military networks was quite moderately simple; first, the definition of the cyber threats and security requirements, then designing the architecture, and finally the evaluation of the presented architecture. However, this straightforward research process proved to be very problematic, especially in the evaluation phase. Two major weaknesses of the research method concern the evaluation method and architecture modeling. Because of these fragilities, the research results are not as high quality as it was thought in the beginning of the study, but the quality of the results does not make this research unnecessary. It must be remembered that this kind of research of building and evaluation a technical security architecture could not be found in literature or academic research.

In Chapter 2, the thesis tried to draw a picture how modern military information systems require a lot of communication and networking resources. Command and control systems are continuously developed to support commanders' leadership and management activities. A challenge is that the developers of information systems often forget security issues typically in a brainstorming phase. It is almost impossible to add reliable security features to the system after it is already implemented. One small purpose of this study was to focus on security issues from the beginning of the network design and implementation.

The design goals and security dimensions were set as the requirements for cyber security in the military networks. However, the design goals may vary a lot at the different levels of warfighting, and their relevance could be repudiated. Also, using the security dimensions as the designing requirements could be considered critically. Now, all the dimensions had an equal weight for designing and evaluating the architecture. We may critically ask for example, are availability and confidentiality equally important in all situations at the battlefield? Data and communication privacy demands may be much higher than e.g. availability in a case that discovered data will cause the loss of human life.

In Chapter 3, the thesis represents the cyber threats concerning the military communication networks, and the challenges of the legacy military networking systems. The chapter describes the phenomena of cyberspace, cyber warfare and cyber threats to show how challenging the cyber domain is. One of the purposes was to describe security threat scenarios that are used in the architecture evaluation phase. The scenarios were based on the idea of that the enemy has always a certain reason for attacking. This resulted in four scenarios with a number of threats: integrity violation, prevention of availability, confidentiality violation and physical destruction. The dynamic nature of cyber threats causes problems to the scenario based approach. The list of threats in each scenario is difficult to maintain up-to-date. Another weakness is that the scenarios do not define an attacking process or phases in details. Thus, in the evaluation phase, it is challenging to show how the threats are defended in practice.

The current cyber threats and the challenges of implementing security controls into the military information systems and networks are relevant reasons for designing a cyber security architecture. A problem was that the existing frameworks and models are not created for this kind of use, and thus a layered block diagram was used to illustrate the overall security architecture. It can be criticized if it is even possible to describe a technical cyber security architecture in this way. At least, the evaluation showed that the functionality of the security elements and the cognitive and management layers must be described more precisely. The thesis does not also specify connections and relationships between the architectural elements.

Building and implementing security in networking devices and systems is a demanding work. A dilemma is that the more we add new features to build a system without security holes the more complex and vulnerable the networking systems become. Therefore, network security must be considered through risk management which is actually one of the key areas where the cognitive networks may be benefit. With the features of the cognitive networks the security elements could be controlled dynamically using intelligent and self-learning processes. Obviously, the cognitive functionality reduces the need of human network operators that sensitive to make errors. The proposed cyber security architecture provides lots of benefits, and it seems to solve the problems with the current military networks, but the implementation of the architecture may turn to be impossible in a sense of complexity.

Are the cognitive networks only alternative, and is it even possible to implement the cognitive feature? The cognitive networks may not be the only choices, but it is sure that new security devices and software becomes more and more sophisticated every day. Automated functionality of cyber security systems is already normal today, and the automated features will increase in the future. Currently, firewalls and IDS/IPS devices have lots of automated features in virus scanning and traffic monitoring. The cognitive networks are just an overall approach to provide cognitive processing at all the layers of networking systems. It is hard to see that future security features are developed without any self-learning or automated functionalities.

The structure of the security controls at each architectural layer can also be criticized. The study does not present a sub process for designing the proposed security elements. The design of the block diagram is just based on the requirement of different types of tasks needed to protect data against violations. A progressive thing is that the elements can easily be removed, modified and added to fulfill the requirements. Anyhow, the implementation of the architecture will likely be the case for major modifications to the architecture.

The thesis introduces the new features and benefits provided by the cognitive networks. Drawbacks are not analyzed systematically, although it is clear that the implementation of cognitive processes is not an easy task. The complexity of the system increases enormously. Every single security control must be software-programmable which causes a lot of new software code to be run, and new potential targets to be vulnerable. Securing the cognitive process itself will be an interesting issue. Violating the process the entire network may collapse.

What are the controls that protect the cognitive process? This thesis does not attempt to answer the question. Security controls that protect the cognitive process must be less vulnerable than those the process controls. This may require totally new operating systems and applications.

The evaluation of a cyber security architecture is significant, but a question is how the evaluation process and results can be enhanced. This thesis proves that the evaluation of this type of architecture is challenging. The evaluation process was clear but lots of values were based on estimation, not on measured performance values. Next versions of the architecture should describe performance values, algorithms and protocols that could be tested against the threat scenarios that include attack phases and methods. The benefits of the evaluation of the security architecture may be small without simulations or prototyping. It could also be wise to implement and evaluate a part of the architecture at the time or to simulate the system layer by layer.

As the evaluation results are not very high-quality, and also the evaluation process and the architecture design requires more research, this thesis could be seen as a process description how to build security architectures. The results could be seen as examples of verifying the architectural properties. The developed architecture modeling and evaluation can be utilized in real life development projects under certain boundary conditions.

Although the results of the thesis are not fully satisfactory, it is very important to seek new approaches to overcome the modern cyber threat. We can be sure we will need all our technological knowledge and research to develop military networks that are reliable and resistance against cyber attacks. It is hard to see that an enemy would stop seeking vulnerabilities and developing new methods or weapons for cyber warfare.

7.3. Future Work

The results of this study cause a lots of needs for further research work. Future work can roughly be divided into four categories. The first is to improve the proposed architecture which includes both the functionalities and more precise definitions etc. The presented architectural design describes only high level functionalities hath are difficult to evaluate. Thus it is more than necessary to plan and design more detailed functionality for each security element. The future work should include the development of formalized (mathematical) description for these functions. Also, the relationship between the security elements and architecture layer would be interesting to study and define.

The second is the development of the evaluation processes. The development could include either the improvement of the applied methods or the introduction of new methods. With the SABSA method, the development needs concern the objects of the layers and the overall demand to use all the layers for evaluation. Developing the scenario based evaluation could include more research about the vulnerability and impact factors and how those are valued against each threat. Also, the estimation of improvement effect of each security element requires more research. For new evaluation methods, the common criteria could be studied and developed more so that the modified CC could be applied for the cyber security architecture evaluation.

The third category for the future work is the cognitive layer and its capabilities. Many features of the presented cyber security architecture rely on the cognitive process. The further research should focus on decision-making algorithms, input and output data of the process and the control channel problematic. Algorithm research could focus on optimization methods and algorithms. Input and output data is critical for the decision making algorithms, and are also important to describe what information and how fast it is necessary to collect when talking about security of the military networking. Data collection uses network resources, but lack of data impairs the ability of decision-making.

The fourth category contains the work that develops the threat scenarios. The chosen scenarios were rough and simple, and they did not include any detailed information about attack phases, methods and tools. Developing the scenarios would improve the evaluation results and their reliability. More detailed threat scenarios would better illustrate real life situations of cyberspace and cyber warfare.

Future work also includes simulations and prototyping that are important when the maturity of the technology is evaluated. The simulations can be conducted using a step-by-step approach in which a security element is simulated and tested at a time. Prototyping can reveal implementation issues that cannot be found in the simulations.

REFERENCES

[1] *A Conceptual Model of Architecture Description*, Systems and software engineering - Architecture description ISO/IEC/IEEE 42010, http://www.iso-architecture.org/42010/cm/. [cited 20.2.2013]

[2] Agarwal A. K. and Wenye Wang, *Measuring performance impact of security protocols in wireless local area networks*, Proceedings of 2nd International Conference on Broadband Networks, Vol. 1, pages 581 - 590, 2005.

[3] Ahmad M., Taj S., Mustafa T. and Asri M., *Performance analysis of wireless network with the impact of security mechanisms*, Proceedings of International Conference on Emerging Technologies (ICET), pages 1 - 6, 2012.

[4] Alberts D. S. and Hayes R. E., *Planning, Complex Endeavors*, CCRP publication series, USA, 2007.

[5] Alberts D. S. and Hayes R. E., *Power to the Edge, Command and Control in the Information Age,* 3rd Printing, CCRP publication series, USA, 2003.

[6] Alberts D. S. and Hayes R. E., *Understanding Command and Control,* CCRP publication series, USA, 2006.

[7] Alberts D. S., Garstka J. J. and Stein F. P., *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd Edition (Revised), CCRP publication series, USA, 2000.

[8] Alberts D. S., Garstka J. J., Hayes R. E. and Signori D. A., *Understanding Information Age Warfare,* CCRP publication series, USA, 2001.

[9] Alkussayer A. and Allen W. H., *A scenario-based framework for the security evaluation of software architecture*, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.

[10] Andress J. and Winterfeld S., *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Elsevier Inc, 2011.

[11] Bechler M., Hof H.-J., Kraft D., Pählke F. and Wolf L., *A Cluster-Based Security Architecture for Ad Hoc Networks*, Proceedings of Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 4, pp. 2393 – 2403, 2003.

[12] Bidgoli H., *Handbook of Information Security - Information Warfare, Social, Legal, and International Issues and Security Foundations*, Volume 2, John Wiley & Sons, 2006.

[13] Boyd J., *The Essence of Winning and Losing*, a five slide set, June 1995.

[14] Burbank J. L., *Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security*, IEEE 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), 2008.

[15] Burbank J., *Security in cognitive radio networks: the required evolution in approaches to wireless network security*, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp 1- 7, 2008.

[16] Carr J., *Inside Cyber Warfare*, Second Edition, O'Reilly Media Inc, 2012.

[17] Chaczko Z., Wickramasooriya R., Klempous R., and Nikodem J., *Security threats in cognitive radio applications*, 14th International Conference on Intelligent Engineering Systems (INES), pp 209 – 214, 2010.

[18] Chenxi Wang, *A Security Architecture for Survivability Mechanisms*, Doctoral Dissertation, University of Virginia, 2000.

[19] Ci S. and Sonnenberg J., *A Cognitive Cross-Layer Architecture for Next-Generation Tactical Networks*, In Proceedings of IEEE Military Communications Conference, 2007.

[20] Clancy T. C., and Goergen N., *Security in cognitive radio networks: threats and mitigation*, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp 1 – 8, 2008.

[21] Clarke R.A. and Knake R., *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins, 2010.

[22] Clements P., Kazman R. and Klein M., *Evaluating Software Architectures: Methods and Case Studies*, Addison-Wesley, 2002.

[23] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, Version 3.1, Revision 3, July 2009.

[24] *Cyber Operations and Cyber Terrorism,* DCSINT Handbook No. 1.02, US Army TRADOC, Version 3.0, 2005.

[25] *Cybersecurity: Threats Impacting the Nation*, Statement of Gregory C. Wilshusen, Director Information Security Issues, United States Government Accountability Office, April 24, 2012.

[26] Dalton G., Colombi J. and Mills B., *Modeling Security Architectures for the Enterprise*, Proceedings of 11th International Command and Control Research and Technology Symposium (ICCRTS), Cambridge, UK, 2006.

[27] *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments*, Report, National Security Agency, 2001. (http://www.nsa.gov/ia/_files/support/defenseindepth.pdf)

[28] *Department of Defense Strategy for Operating in Cyberspace*, US DoD, July 2011.

[29] *DoD Architecture Framework Version 2.0, Volume 2: Architectural Data and Models, Architect's Guide*, US DoD, 28 May 2009.

[30] Douligeris C. and Serpanos D. N., *Network Security: Current Status and Future Directions*, John Wiley & Sons, 2007

[31] *Emerging Cyber Threats Report 2013*, Georgia Tech Cyber Security Summit 2012 (GTCSS), November 14, 2012.

[32] *Enterprise information security architecture*, http://en.wikipedia.org/wiki/Enterprise_information_security_architecture [cited 20.2.2013].

[33] *Facts about National Defence*, Public Information Division of the Defence Command, First Edition, ISBN 978-951-25-1955-2, Edita Prima Oy, 2008.

[34] Fall K., *A Delay-Tolerant Network Architecture for Challenged Internets*, Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, pp 27-34, 2003.

[35] Foreman P., *Vulnerability Management*, Taylor & Francis Group, 2010.

[36] Fragkiadakis A., Alexandros G., Tragos E. and Ioannis G., *A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks*, IEEE Communications Surveys & Tutorials, Volume 15 , Issue 1, pp. 428 – 445, 2013.

[37] Gansler J. S. and Binnendijk H. (ed.), *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*, U.S. Government, General Books, 2011.

[38] Garstka J. and Alberts D., *Network Centric Operations Conceptual Framework,* Version 2.0, U.S. Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration, 2004.

[39] Geers K., *Strategic Cyber Security,* NATO Cooperative Cyber Defence Centre of Excellence, June 2011.

[40] Gonzales D., Johnson M., McEver J., Leedom D., Kingston G. and Tseng M., *Network-Centric Operations Case Study: The Stryker Brigade Combat Team*, RAND, 2005.

[41] Graham J., Howard R. and Olson R. (ed.), *Cyber Security Essentials*, Taylor and Francis Group, 2011.

[42] Hallingstad G. and Oudkerk S., *Protected core networking: an architectural approach to secure and flexible communications,* IEEE Communications Magazine, Volume 46, Issue 11, pp. 35 - 41, 2008.

[43] *How does MODAF represent security?* , Report, UK MOD, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/36751/20090521_MODAF_1_2_FAQs_How_MODAF_Can_Reflect_Security_Concerns_V1_0_U.pdf [cited 20.2.2013].

[44] *iCode Enterprise Security Architecture Framework*, iCode Information Security, http://www.icodesecurity.com/architecture.html [cited 20.2.2013].

[45] *Information technology – Lower layers security model*, ITU-T Recommendation X.802, ITU-T Study Group 17, 1995.

[46] *Information technology – Open Systems Interconnection – Upper layers security model*, ITU-T Recommendation X.803, ITU-T Study Group 17, 1994.

[47] *Information Technology Security Evaluation Criteria (ITSEC),* Provisional Harmonised Criteria, ECSC-EEC-EAEC, Brussels, June 1991.

[48] Jajodia S., Liu P., Swarup V. and Wang C. (ed.), *Cyber Situational Awareness: Issues and Research*, Volume 46, Springer, 2010.

[49] Janczewski L. J. and Colarik A. M., *Cyber Warfare and Cyber Terrorism*, Idea Group Inc, 2008.

[50] Joshi J., *Network Security: Know It All*, Morgan Kaufmann, 2008.

[51] Kallberg J., *Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal*, Selected Papers in Security Studies: Volume 9, Technical Report UTDCS-

13-12, Department of Computer Science, The University of Texas at Dallas, August 2012.

[52] Kar D. C. and Syed M. R., *Network Security, Administration, and Management: Advancing Technology and Practice*, Idea Group Inc (IGI), 2011.

[53] Kim S., Seo S. and Lee I., *Essential Characteristics of Cyberspace and Analysis of Cyber Educational Institutions*, Proceedings of The third Asia-Pacific International Conference on computational Methods in Engineering (ICOME2009), 2009.

[54] Kizza J. M., *Guide to Computer Network Security*, Springer, 2009.

[55] Koponen T., *A Data-Oriented Network Architecture*, Doctoral Dissertation, Department of Computer Science and Engineering, Helsinki University of Technology, 2008.

[56] Kuptsov D., Garcia O., Wehrle K. and Gurtov A., *On Applications of Cooperative Security in Distributed Networks*, Proceedings of 4th International Conference on Trust Management, 2010.

[57] Luker M. A. and Petersen R. J., *Computer and network security in higher education*, Jossey-Bass, 2003.

[58] Mahmoud Q. H. (ed.), *Cognitive Networks: Towards Self-Aware Networks*, John Wiley & Sons, Ltd, 2007.

[59] Martin K. M., *Everyday Cryptography: Fundamental Principles and Applications*, Oxford University Press, 2012.

[60] *Military communications*, Wikipedia, http://en.wikipedia.org/wiki/Military_communications [cited 23.5.2013]

[61] *MOD Architecture Framework*, https://www.gov.uk/mod-architecture-framework [cited 20.2.2013].

[62] Mody A. N., Reddy R., Kiernan T. and Brown T. X., *Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard*, IEEE Military Communications Conference (MILCOM), pp 1 – 7, 2009.

[63] Mohapatra P. and Krishnamurthy S., *Ad hoc networks: technologies and protocols*, Springer, 2005.

[64] *Multilayer Traffic Normalization and Data Stream Based Inspection: Essential Design Principles of the Stonesoft IPS (Protection against Advanced Evasion Techniques in Stonesoft IPS)*, Whitepaper, Stonesoft Corporate, February 2012.

[65] Mű̈ter M., *Model-Based Security Evaluation of Vehicular Networking Archite*ctures, IEEE Ninth International Conference on Networks (ICN), 2010.

[66] *NATO Architecture Framework*, Version 3, NATO Consultation, Command and Control Board, 2007.

[67] Neelakantan S., Ampatt P., Muraleedharan N., Korimilli S.C.B., Parmar A., Kumar M. and Roy A., *An Architecture for self-configuration of network for QoS and Security*, Proceedings of First International Communication Systems and Networks and Workshops, pages 1 – 5, 2009.

[68] *Network Centric Warfare: Background and Oversight Issues for Congress*, CRS Report for Congress, USA, June 2, 2004.

[69] *Network Security Baseline*, Cisco Systems Inc, 2008, http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securbase.pdf [cited 4.4.2013]

[70] Onwubiko C. and Owens T., S*ituational Awareness in Computer Network Defense: Principles, Methods and Applications*, IGI Global Snippet, 2012.

[71] *Open Security Architecture*, www.opensecurityarchitecture.org [cited 14.2.2013].

[72] *Overview of cybersecurity*, Series X: Data Networks and Open System Communications and Security, ITU-T Recommendation X.1205, ITU-T Study Group, April 2008.

[73] *OWASP Testing Guide*, The Open Web Application Security Project (OWASP) Foundation, V3.0, 2008.

[74] Perry W., Gordon J., Boito M. and Kingston G., *Network-Based Operations for the Swedish Defence Forces: An Assessment Methodology*, Technical Report, RAND Europe, June 2004.

[75] Peterson G., *Don't Trust. And Verify: A Security Architecture Stack for the Cloud*, IEEE Security & Privacy, Volume 8, Number 5, pp. 83-86, 2010.

[76] Pfleeger C. P., and Pfleeger S. L.: *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*, Prentice Hall Professional, 2011.

[77] Prasad N., *Secure cognitive networks*, European Conference on Wireless Technology, pp 107 – 110, 2008

[78] Qingqi Pei, Rui Liang and Hongning Li, *A Trust Management Model in Centralized Cognitive Radio Networks*, IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 491 – 496, 2011.

[79] Rathaus N. and Evron G., *Open Source Fuzzing Tools*, Syngress, 2011.

[80] Reveron D. S., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, UPCC book collections on Project MUSE, Georgetown University Press, 2012.

[81] Rozanski N. and Woods E., *Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives*, Addison-Wesley, 2005.

[82] Safdar G. and O'Neill M., *Common Control Channel Security Framework for Cognitive Radio Networks*, IEEE 69th Vehicular Technology Conference, 2009.

[83] Security architecture for Open Systems Interconnection for CCITT applications, ITU-T Recommendation X.800, ITU-T Study Group 17, 1991.

[84] *Security architecture for systems providing end-to-end communications*, ITU-T Recommendation X.805, 10/2003.

[85] *Security architecture for systems providing end-to-end communications*, Series X: Data Networks and Open System Communications and Security, ITU-T Recommendation X.805, ITU-T Study Group, October 2003.

[86] Sherwood J., Clark A. and Lynas D., *Enterprise Security Architecture: A Business-Driven Approach*, CMP Books, 2005.

[87] Shoemaker D. and Conklin W. A., *Cybersecurity: The Essential Body of Knowledge*, Cengage Learning, 2011.

[88] *Survey of Architecture Frameworks, Systems and software engineering — Architecture description*, ISO/IEC/IEEE 42010, http://www.iso-architecture.org/42010/afs/frameworks-table.html [cited 20.2.2013].

[89] Swiderski F. and Snyder W., *Threat Modeling*, Microsoft Press, 2004.

[90] *The National Military Strategy for Cyberspace Operations*, Chairman of the Joint Chiefs of Staff, Washington, D.C., December 2006.

[91] *The National Strategy to Secure Cyberspace*, The White House, Washington D.C., USA, February 2003.

[92] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, Cabinet Office, November 2011.

[93] *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, US Army TRADOC Pamphlet 525-7-8, 22 February 2010.

[94] Thomas R. W., *Cognitive Networks*, dissertation, Virginia Polytechnic Institute and State University, June 15, 2007.

[95] Thomas R. W., DaSilva L. A. and MacKenzie A. B., *Cognitive Networks*, In Proceedings of First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2005.

[96] Thomas R. W., DaSilva L. A., Marathe M. V. and Wood K. N., *Critical Design Decisions for Cognitive Networks*, In Proceedings of IEEE ICC 2007, pp. 3993-3998, June 2007.

[97] Thomas R. W., Friend D. H., DaSilva L. A. and MacKenzie A. B., *Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives*, IEEE Communication Magazine, vol. 44, pp. 51-57, Dec. 2006.

[98] Thorn A., Christen T., Grubera B., Portman R. and Ruf L., *What is a Security Architecture?*, White paper, Security architecture Working Group, ISSS Information Security Society Switzerland, 2008.

[99] Troell L., Hartpence B. and Simons S., *Comparative Performance of Layer 2 and IPSec Encryption on Ethernet Networks*, Research Report, Security and Systems Administration Department, Rochester Institute of Technology Networking, October 2006.

[100] *Trusted Computer System Evaluation Criteria (TCSEC)*, Department of Defense Standard, The US Department of Defense, December 26, 1985.

[101] *UN terms*, United Nations, http://unterm.un.org/dgaacs/unterm.nsf/375b4cb457d6e2cc85 256b260070ed33/$searchForm?SearchView [accessed 17.05.2013].

[102] Whitman M. E. and Mattord H. J., *Principles of Information Security*, Cengage Learning, 2011.

[103] Whitman M. E. and Mattord H. J., *Principles of Information Security*, Cengage Learning, 2011.

[104] Wilson C., *Network Centric Operations: Background and Oversight Issues for Congress*, Congressional Research Service Report for Congress, Updated March 15, 2007.

[105] Wyglinski A. M., Nekovee M. and Hou Y. T., *Cognitive radio communications and networks: principles and practice*, Academic Press, 2010.

[106] Yi Peng, Fenghong Xiang, Hua Long and Jie Peng, *The Research of Cross-layer Architecture Design and Security for Cognitive Radio Network*, IEEE International Symposium on Information Engineering and Electronic Commerce, 2009.

[107] Yu Wang, Jun Lu and Zhongwang Wu and Yu Lu, *Component Based Security Control for Information Network*, Proceedings of Multiconference on Computational Engineering in Systems Applications (IMACS), Vol. 2, pp. 1357 – 1360, 2006.

[108] Yuan Zhang, Gaochao Xu and Xiaozhong Geng, *Security Threats in Cognitive Radio Networks*, 10th IEEE International Conference on High Performance Computing and Communications, pp. 1036 – 1041, 2008.

[109] Zhao Y., Mao S., Neel J. O. and Reed J. H., *Performance Evaluation of Cognitive Radios: Metrics, Utility Functions, and Methodology*, Proceedings of the IEEE, Vol. 97, No. 4, April 2009.