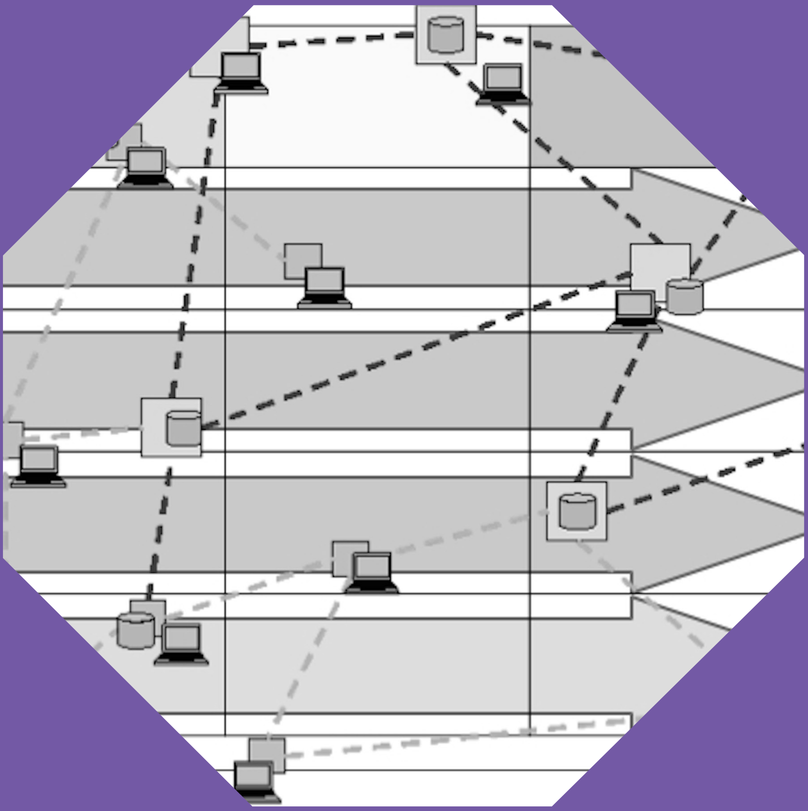
Department of Communications and Networking

Developing cyber security architecture for military networks using cognitive networking

Anssi Kärkkäinen



Aalto University

DOCTORAL DISSERTATIONS

Aalto University publication series
DOCTORAL DISSERTATIONS 170/2015

Developing cyber security architecture for military networks using cognitive networking

Anssi Kärkkäinen

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Electrical Engineering, at a public examination held at the lecture hall S5 of the school on 11 November 2015 at 12.

Aalto University
School of Electrical Engineering
Department of Communications and Networking

Supervising professor
Prof. Jukka Manner

Thesis advisor
Prof. Jukka Manner

Preliminary examiners
Prof. Hannu H. Kari, National Defence University, Finland
Prof. Mikko Siponen, University of Jyväskylä, Finland
Dr.ing. Konrad Wrona, NATO Communications and Information Agency, The Netherlands

Opponents
Prof. Timo T. Hämäläinen, University of Jyväskylä, Finland
Prof. Hannu H. Kari, National Defence University, Finland

Aalto University publication series
DOCTORAL DISSERTATIONS 170/2015

ISBN 978-952-60-6455-0 (printed)
ISBN 978-952-60-6454-3 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-60-6454-3

Unigrafia Oy
Helsinki 2015

Finland

NORDIC ECOLABEL
441 697
Printed matter

Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

Author
Anssi Kärkkäinen

Name of the doctoral dissertation
Developing cyber security architecture for military networks using cognitive networking

Publisher School of Electrical Engineering

Unit Department of Communications and Networking

Series Aalto University publication series DOCTORAL DISSERTATIONS 170/2015

Field of research Networking Technology

Manuscript submitted 8 June 2015 **Date of the defence** 11 November 2015

Permission to publish granted (date) 10 September 2015 **Language** English

☐ **Monograph** ☒ **Article dissertation (summary + original articles)**

Abstract

In recent years, the importance of cyber security has increased. Cyber security has not become a critical issue only for governmental or business actors, but also for armed forces that nowadays rely on national or even global networks in their daily activities. The Network Centric Warfare (NCW) paradigm has increased the significance of networking during last decades as it enables information superiority in which military combat power increased by networking the battlefield actors from perspective of processes, operations and information sharing. At tactical level, the ability to share information sets high requirements for data transport, and its security because the circumstances and needs of the operational activities are very challenging.

The development of military communication capabilities requires long term planning to ensure interoperability and maintain a life cycle support for even decades. Different network system architectures, including also cyber security, are an important tool to manage this long term development.

This thesis is focused on architectural cyber security aspects of military networks, and considers how security is improved by developing network cyber security architectures in line with military networking capability development. In the long term capability development, Cognitive Networks (CN) are seen as a promising solution for intelligent, self-learning and reliable networking. The phases of the NATO Network Enabled Capability (NEC) development require different types of architectural approaches for cyber security. In the short and mid-term, the development is based on the common security solutions and multilevel security. For the long term goal, the coherent networking requires a novel network cyber security architectural approach as networking will be based on the cognitive networks.

For the short and mid-term, the architectures for privacy protection, delay-tolerant networking, and multilevel security provide partial solutions for developing network cyber security. For the long term development, the thesis presents a novel cognitive network-based cyber security architecture that provides an overall design to build automated, self-configurable security management and control for future tactical military communications. The capabilities of the architecture ensure improved cyber threat management, and situational awareness. Cognitive behavior enables dynamic service configuration to protect services against cyber attacks.

The implementation of the architectures requires more research. The evaluation of architectures is a challenging task requiring simulations and practical implementations to measure the features designed in the architecture.

Keywords cyber security, cognitive network, military communications, security architecture

ISBN (printed) 978-952-60-6455-0 **ISBN (pdf)** 978-952-60-6454-3

ISSN-L 1799-4934 **ISSN (printed)** 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Helsinki **Location of printing** Helsinki **Year** 2015

Pages 176 **urn** http://urn.fi/URN:ISBN:978-952-60-6454-3

Aalto-yliopisto

Tiivistelmä

Aalto-yliopisto, PL 11000, 00076 Aalto www.aalto.fi

Tekijä
Anssi Kärkkäinen

Väitöskirjan nimi
Sotilastietoliikenneverkkojen kyberturvallisuusarkkitehtuurin kehittäminen kognitiivista verkkoa hyödyntäen

Julkaisija Sähkötekniikan korkeakoulu

Yksikkö Tietoliikenne- ja tietoverkkotekniikan laitos

Sarja Aalto University publication series DOCTORAL DISSERTATIONS 170/2015

Tutkimusala Tietoverkkotekniikka

Käsikirjoituksen pvm 08.06.2015 **Väitöspäivä** 11.11.2015

Julkaisuluvan myöntämispäivä 10.09.2015 **Kieli** Englanti

☐ **Monografia** ☒ **Yhdistelmäväitöskirja (yhteenveto-osa + erillisartikkelit)**

Tiivistelmä

Kyberturvallisuuden merkitys on kasvanut viime vuosina. Kyberturvallisuudesta ei ole tullut kriittinen kysymys vain valtiollisille tai yritysmaailman toimijoille vaan myös asevoimille, joiden päivittäinen ja erityisesti poikkeusolojen operointi riippuu kansallisista tai jopa globaaleista tietoverkoista. Verkostokeskeisen sodankäynnin paradigma on lisännyt verkottumisen merkitystä viime vuosikymmeninä, koska se mahdollistaa tietoylivoiman, jossa sotilaallinen voima kasvaa verkostoimalla taistelukentän toimijoiden prosessit, toiminnot ja tiedonjakaminen. Taktisella tasolla tiedonjakaminen asettaa korkeat vaatimukset tietoliikenteelle ja sen turvallisuudelle, koska olosuhteet ja operatiiviset tarpeet ovat haastavat.

Sotilastietoliikenteen kehittäminen vaatii pitkäjänteistä suunnittelua yhteentoimivuuden varmistamiseksi ja elinkaarituen ylläpitämiseksi jopa vuosikymmenien ajaksi. Erilaiset tietoliikennejärjestelmän arkkitehtuurit, mukaan lukien myös kyberturvallisuus, ovat tärkeä väline hallita pitkän aikavälin kehitystä.

Väitöskirja keskittyy sotilastietoliikenneverkkojen arkkitehtuuritason kyberturvallisuuteen ja tarkastelee, miten verkkojen turvallisuutta voidaan parantaa kehittämällä kyberturvallisuusarkkitehtuureja osana sotilastietoliikenneverkkojen kehitystä. Pitkän aikavälillä kognitiiviset verkot nähdään lupaavana ratkaisuna tuottaa älykäs, itseoppiva ja luotettava tietoliikenneverkko. Naton verkostokeskeisen suorituskyvyn kehittämisen vaiheet vaativat erilaisia arkkitehtuurillisia lähestymistapoja kybertietoturvallisuuteen. Lyhyellä ja keskipitkällä aikavälillä kehittäminen perustuu yhteisiin ratkaisuihin ja monikerrostietoturvaan. Pitkällä aikavälillä kognitiivisiin verkot vaativat uusia ratkaisuja kyberturvallisuusarkkitehtuuriin.

Lyhyellä ja keskipitkällä aikavälillä yksityisyyden suojan, viiveitä sietävän verkon ja monikerrostietoturvan arkkitehtuurit antavat osittaisia ratkaisuja tietoliikenteen kyberturvallisuuteen. Pitkän aikavälin kehitykseen väitöskirja esittelee uuden kognitiiviseen verkkoon pohjautuvan kyberturvallisuusarkkitehtuurin, joka tarjoaa kokonaisratkaisun automaattisen ja itsekonfiguroituvan tietoturvallisuuden ylläpidon, hallinnan ja valvonnan rakentamiseksi tulevaisuuden taktisiin sotilasverkkoihin. Arkkitehtuuri parantaa kyberuhkien hallintaa ja tilannetietoisuutta. Kognitiivinen toiminta mahdollistaa dynaamisen palvelukonfiguraation verkkohyökkäyksiltä suojautumiseksi.

Arkkitehtuurien implementointi vaatii vielä lisää tutkimusta. Arkkitehtuurien evaluointi on haastavaa, ja se edellyttää simulaatioita tai käytännön toteutuksen, jotta voidaan tarkasti todentaa arkkitehtuurin vaatimustenmukaisuus.

Avainsanat kyberturvallisuus, kognitiivinen verkko, sotilastietoliikenne, tietoturva-arkkitehtuuri

ISBN (painettu) 978-952-60-6455-0 **ISBN (pdf)** 978-952-60-6454-3

ISSN-L 1799-4934 **ISSN (painettu)** 1799-4934 **ISSN (pdf)** 1799-4942

Julkaisupaikka Helsinki **Painopaikka** Helsinki **Vuosi** 2015

Sivumäärä 176 **urn** http://urn.fi/URN:ISBN:978-952-60-6454-3

Acknowledgements

My journey lasted eight years. It is a long time with many ups and downs. Sometimes I felt the journey won't end or it ends only by leaving the whole idea of becoming D.Sc. (Tech.). But step by step, my academic trial became to this point; my dissertation is now published after eight memorable years. Now I realize how challenging this academic work is when you study besides of daily work. My studies would not have been possible without continuous support of important people. I would like to express my gratitude to the people who supported me to accomplish my studies.

First, I would like to thank my outstanding supervisor professor Jukka Manner for creating a convenient and supportive atmosphere that was required to find motivation to finalize my study. He also gave excellent guidance for the content and structure of this thesis. I also thank Lic.Sc. (Tech.) Marko Luoma for reviewing and commenting my thesis. His feedback had a great effort to glue the pieces of this research together.

I thank my employer Finnish Defence Forces, and especially the C4 Division of Defence Command for supporting my aspirations, and for funding some conference trips. Especially I thank Dr. Catharina Candolin who as my superior and co-author strongly encouraged me to conduct post graduate studies. I would also like to extend my gratitude towards my pre-examiners, professors Timo T. Hämäläinen, Hannu H. Kari and Mikko Siponen, whose comments guided me to make this thesis better.

Last but not least, I would like to express my greatest gratitude to my family. I thank my wife, Sanna, for continuous and varied support (such as babysitting) while I needed time to concentrate on writing and reading. I thank my children for enduring me when I was in the other world with my laptop. Thank you all, I would not have been able to pull this off without you.

Hausjärvi, 3 October 2015
Anssi Kärkkäinen

Contents

List of Abbreviations and Symbols

AACE	Application Access Control Element
AES	Advanced Encryption Standard
API	Application programming interface
AW	Awareness
BSP	Bundle Security Protocol
C2	Command and Control
CC	Common Criteria
CBIS	Content-Based Information Security
CIS	Communications and Information System
CE	Cryptography Element
CN	Cognitive Network
CNR	Combat Net Radio
COTS	Commercial off-the-shell
CSF	Cisco Security Framework
DDoS	Distributed Denial-of-Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoDAF	Department of Defense Architecture Framework
DoS	Denial-of-Service
DTN	Delay-Tolerant Networking
ED	Ease of Discovery
EE	Ease of Exploit
FMN	Federated Mission Network

FTP	File Transfer Protocol
HF	High frequency
HIP	Host Identity Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and communications technology
ID	Intrusion detection
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information technology
ITSEC	Information Technology Security Evaluation Criteria
ITU-T	ITU Telecommunication Standardization Sector
LA	Loss of Availability
LAC	Loss of Accountability
LC	Loss of Confidentiality
LI	Loss of Integrity
MAC	Media Access Control
MACE	Management Access Control Element
MLS	Multilevel security
MN	Mission Network
MODAF	Ministry of Defence Architecture Framework
NACE	Node Access Control Element
NAF	NATO C3 Systems Architecture Framework
NATO	North Atlantic Treaty Organization
NCW	Network Centric Warfare
NEC	Network Enabled Capability
NII	Network and Information Infrastructure
NNEC	NATO Network Enabled Capability

OODA	Observe-Orient-Decide-Act
OSI	Open Systems Interconnection model
OWASP	Open Web Application Security Project
PACE	Packet Access Control Element
PCN	Protected core networking
PCS	Protected-core segment
PLA	Packet Level Authentication
QoS	Quality of service
RF	Radio frequency
RSE	Routing Security Element
SA	Situational Awareness
SABSA	Sherwood Applied Business Security Architecture
SACE	Service Access Control Element
SCE	Security Control Elements
SOM	Self-Organizing Map
SOA	Service-Oriented Architecture
SLA	Service Level Agreement
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TMFE	Traffic Monitoring and Filtering Element
TSE	Traffic Shaping Element
TVM	Threat and Vulnerability Management
UDP	User Datagram Protocol
VHF	Very high frequency
VPN	Virtual Private Network

List of Latin Symbols

I_i	impact of the scenario i
I_{ir}	vulnerability index

L_i	likelihood of scenario i
LR_i	lack of security element resistance
LV	security risk vector
M_s	cyber security risk matrix
R_i	risk of scenario i
T	transpose
VF_i	average of the vulnerability factors for scenario i
w_a	weight of damage risk
W_{cai}	weight matrix
w_r	weight of cyber security risk,
w_l	weight of damage influence

List of Greek Symbols

α_j	improvement effect of control j

List of Publications

This doctoral dissertation consists of a summary and of the following publications which are referred to in the text by their numerals

1. A. P. Kärkkäinen and C. Candolin. Ensuring Privacy in a Network Centric Environment. In *Proceedings of 7th European Conference on Information Warfare and Security (ECIW)*, Plymouth, United Kingdom, pages 111-118, July 2008.

2. A. P. Kärkkäinen and C. Candolin. Multilevel Security in a Network-Centric Environment. In *Proceedings of 8th European Conference on Information Warfare and Security (ECIW)*, Braga, Portugal, pages 134-141, July 2009.

3. A. P. Kärkkäinen. Ensuring Communication Security in Delay-Tolerant Networks. In *Proceedings of 5th International Conference on Information Warfare and Security (ICIW)*, *Ohio, USA*, pages 193-201, April 2010.

4. A. P. Kärkkäinen. Improving Situation Awareness in Cognitive Networks Using the Self-Organizing Map. In *Proceedings of IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, Miami Beach, USA, pages 40-47, February 2011.

5. A. P. Kärkkäinen. Cyber Threat Management in Cognitive Networks. In *Proceedings of 11th European Conference on Information Warfare and Security (ECIW)*, Laval, France, pages 320-328, July 2012.

6. A. P. Kärkkäinen. Improving Cyber Defence of Tactical Networks by Using Cognitive Service Configuration. In *Proceedings of 12th European Conference on Cyber Warfare and Security* (ECCWS), Jyväskylä, Finland, pages 135-143, July 2013.

7. A. P. Kärkkäinen. A Cognitive Network-Based Network Security Architecture for Mission Critical Communications. *International Journal of Information & Network Security (IJINS)*, IAES, Vol 3, No 3, 2014. ISSN 2089-3299. DOI: 10.11591/ijins.v3i3.6146.

Author's Contribution

Publication 1: Ensuring Privacy in a Network Centric Environment

The Author wrote the background and the threat modelling in which the X.805 prefix was further developed to support military related threat scenarios. The author also contributed in writing the section of privacy architecture. The paper was written by Dr. C. Candolin and the author.

Publication 2: Multilevel Security in a Network-Centric Environment

The author designed the architectural concept for multilevel security. The author wrote the article almost completely and edited the article based on the comments of the second author.

Publication 3: Ensuring Communication Security in Delay-Tolerant Networks

The single-author paper presents a three-layer security architecture for delay-tolerant networking. The architecture was researched and developed by the author.

Publication 4: Improving Situation Awareness in Cognitive Networks Using the Self-Organizing Map

In this single-author paper, the author applies self-organized maps to build situational awareness in cognitive military networks. The publication demonstrates the performance of SOM in monitoring the status of networks.

Publication 5: Cyber Threat Management in Cognitive Networks

The single-author paper presents an architectural concept that was developed by the author.

Publication 6: Improving Cyber Defence of Tactical Networks by Using Cognitive Service Configuration

The author designed a new approach for cyber defence in which information services and networks are cognitively managed creating a target system much more challenging to an attacker. The work was conducted alone.

Publication 7: A Cognitive Network-Based Network Security Architecture for Mission Critical Communications

The journal article presents a novel cognitive network-based cyber security architecture for military networking. Research and writing was conducted by the author.

1. Introduction

Computer networks and services, as part of cyber domain, are revolutionizing our society worldwide by giving people, business and government more efficient ways to work and co-operate with one another. Cyber domain means a digital information processing domain, and it comprises of one or several information technology infrastructures with the all hardware and software deployed to process digital information (bits). Growing number of connections and devices expand cyberspace continuously. Also for armed forces, cyber domain has become a strategic domain where strategic or operational advantages of military business can be won or lost. The military's growing dependency on cyber domain means that its disruption will disturb or damage armed forces' ability to function effectively during a crisis. [101]

The security of the cyber domain, cyber security, has become a worldwide issue in recent years. The various players have expressed cyber security the most significant factor in the near future. Many countries have drawn up cyber security strategies. The Finnish cyber security strategy described cyber security as the desired end state in which the cyber domain is reliable and its functioning is ensured. In the desired end state, the cyber domain will not jeopardize, harm or disturb the functions dependent on digital information processing. [26]

Events in cyberspace may occur in milliseconds. Traditional responses may not be sufficient to protect critical services provided in cyberspace. Risks in cyberspace can be managed in several ways, but risk mitigation may turn out to be challenging due to this complex and dynamic environment and changing threat. 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. [101]

Simultaneously with growing cyber security threats, military troops are more dependent on networks and information services than ever. The Network Centric Warfare (NCW) paradigm [2] has increased the significance of military communication networks during last decades. NCW is an operational concept driving towards 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 [2]. NCW is primarily an operational model, but communication networks play an important role as an enabler of networking activities and information sharing. Ideally in NCW, all traditional military capability areas (weapon systems, targeting, logistics etc.) are interconnected via networks and the capabilities rely heavily on information technology and applications. NCW has brought new requirements for military networking which naturally reflects to the way network security is designed and implemented. New warfighting paradigms demand new approaches and innovations how network security is built in a military communications system.

Network cyber security as a subset of cyber security focuses on protecting communication networks, and it has become critical to armed forces as they operate using the national or even global networks. Legacy security architectures and controls were not designed to face the emerging cyber threats. Traditionally, military networks were totally isolated from the other networks, and access to them was very limited to both geographical areas and the number of authorized users. Physical security means played an enormous role in these systems. In the legacy systems, security controls are often built after the implementation without a holistic view on information and cyber security. [21]

For the future secure military network, a potential research area is Cognitive Networks (CN). These intelligent and self-learning cognitively behaving networks are believed to generate more performance to communications networking including 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 [60]. 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. CN is able to use network resources dynamically and effectively. Network administration and configuration is maintained without human operators [84].

In military context, the development of communications network and services is based on long term roadmaps such as introduced in the NATO Network Enabled Capability (NEC) [74] and Federated Mission Networking [73] concepts. The long term capability development requires the architectural level analysis which means also network cyber security is considered from a holistic view point, and the focus is moved from a single security protocol to the architectural and design model level. [39]*This thesis focuses on architectural aspects on cyber security of military networks. The main purpose of the thesis is to consider how cyber security is improved by developing overall network cyber security architectures in line with military networking capability development.* The thesis presents several architectures and frameworks to improve security capabilities in different phases of the development. Finally, the thesis introduces a cognitive network-based cyber security architecture, and describes its benefits for providing cyber security in military communications networks.

The thesis combines the research fields of cyber security and system architecture design. The purpose is to provide applied research results rather than new theoretical models in the context of military communications. An idea is to deliver practical guidance for system architects and development engineers with relation to state of the art technologies. The thesis proposes how the ideas and technologies of cognitive networking could be used to design security architecture for military communications.

1.1 Motivation

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. [77]

As it is known the life-cycle of military capability is long when compared to civilian systems [17]. Long life-cycles typically concern for example weapon systems such as main battle tank or artillery pieces, but also special communications systems such as tactical networks. In a military context, the long life-cycle means the systems are initially designed to be capable and operational for decades. Typically, the average life of a major weapon system often exceeds 20 years [17]. The long life-cycles require overall system of system design supporting modularity and flexibility. In a system of systems thinking, all interfaces between subsystems are standardized enabling varying lifecycles to the sub components [42].

Successful long term support of systems, such as military communications systems, requires careful up-front planning, and a proper system architecture that supports a comprehensive long term life cycle management plan [35]. For military communications systems, software is becoming increasingly more important in long term sustainment as it continues to define more and more of the functionality of networking systems. Architectures must support software and hardware development and interoperability in a long term as the system of systems of a military network may consist of heterogeneous technologies and components in a certain time of life cycle.

If the architecture of the systems does not support flexible updates of security controls or components, it may be impossible to maintain desired cyber security level as the threat changes and grows. Changing the entire security architecture is much more challenging with the long-lifecycle systems. Experimenting new features is relevant at the protocol level, but not at the architectural level where experimenting requires large implementations. Thus, it is vital to develop cyber security architectures and design models to respond to the future threats and technologies.

Many complex systems have behaviors and properties that no subset of their elements have [16]. Architecture models and frameworks help designers to perceive overall nature of a large, complex system of systems, such as a military network system. A key function of architecture as a tool of the architect is to provide a framework within which complexity can be managed successfully [91].

Cyber threats are not only subject to military command and control (C2) systems, but also subject to all military systems that include software and hardware. Overall military capability with technical systems of systems form a complex ICT infrastructure with embedded commercial off-the-shell (COTS), military and civilian technologies. Managing cyber security in this challenging environment requires an architecture level design.

CN is a paradigm that has its potential in civilian business and networks [60], but it could also provide great benefits to the military communications. CN providing automated and self-learning features may help to meet the high requirements of especially tactical networking where dynamic and auto-configure capabilities are demanded. CN has also its potential to provide improved cyber security for military networking by controlling security controls dynamically. In theory, the cognitive process is aware of current situations of security controls and it is able to adjust security parameters according to environmental or other changes.

A security architecture is a basis for designing security services for networking system. The architecture is required to meet the needs of its users, system elements to implement the security services, and performance levels to mitigate cyber threats. Security must be integrated into the network design from the very beginning in order for the network to meet the needs of the users and for security to provide adequate protection. Thus, security must be considered also at the architectural level. [63]

Network cyber security is defined as the protection of networks and their services from unauthorized access, modification, destruction, or disclosure. Network security provides assurance that the network performs its critical functions correctly and that there are no harmful side effects. [63] The security architecture of a network system is an important tool to ensure that all the requirements are considered before implementation. Through architecture design, it is possible to find relationships and dependencies between the components providing services for integrity, confidentiality and availability.

A need for developing a new cyber security architecture for military tactical networking could be summarized with the following three points:

- *Life cycle management*. A security architecture ensures the technical solutions in different life cycle phases are interoperable, and different technologies are implemented with a managed manner.
- *Complexity management*. Military networks form a large system of systems in which technical security must be managed at all the layers. This requires an overarching security architecture to be developed.
- *Risk management*. Managing a risk in a complex system means that the system is considered as a whole. Concentrating only on the risk

level of a single element, means that overall risk is not analyzed. The overall risk may turn to be at a different level than the sum of partial risks [58].

- *Design guidance*. In a large organizations, such as armed forces, subsystems are developed by different actors. A security architecture describes how security must be implemented from a technical point of view, and guarantees that sub elements fulfil security requirements.

1.2 Scope and Objectives of the Thesis

The main objective of this thesis is to develop cyber security architectures for future military networks. The purpose is to research how cyber security architectures must be designed as part of the military communications capability development including the short, mid and long term improvements to fulfill the future operational requirements. The scope is not to develop the NATO NEC roadmap phases, but support these phases by architectural development.

The thesis focuses on the architecture level challenges and develops novel architecture approaches to overcome emerging cyber security challenges. The architecture level research inevitably leads to analysis that is conducted at the higher level of abstraction. The architectural design is considered from a technical viewpoint, and protocol level research and development is outside of the scope. The focus of this dissertation is to develop a technical architecture, and thus, architecture views of organization and processes are out of the scope of the thesis.

A large part of the research work specifically focuses on cognitive networking and how it could improve network security in military networking systems in a sense of communications security, privacy, automated risk assessment, dynamic security adaptation and service availability. Cognitive networks are a promising paradigm for managing network security in rough environments where a networking system is under continuous reshaping due to changing communications requirements. The thesis emphasizes the benefits of cognitive networking in development of security architectures for military networks.

The thesis also discusses the cyber security requirements of military networking, presents the paradigm of cognitive networks, and introduces a novel cognitive network-based cyber security architecture of military networks.

1.3 Research Contributions

The scientific results achieved in the thesis are related to the field of developing network security architectures in the context of military networking. The proposed architecture models represent improvements to the prior art and also present new approaches for solving existing problems in network security of military communications. A major contribution is to present the benefits of using the cognitive network paradigm to improve cyber security of military networking systems in the long term development. Figure 1 illustrates how the publications cover the phases of military networking development roadmap.

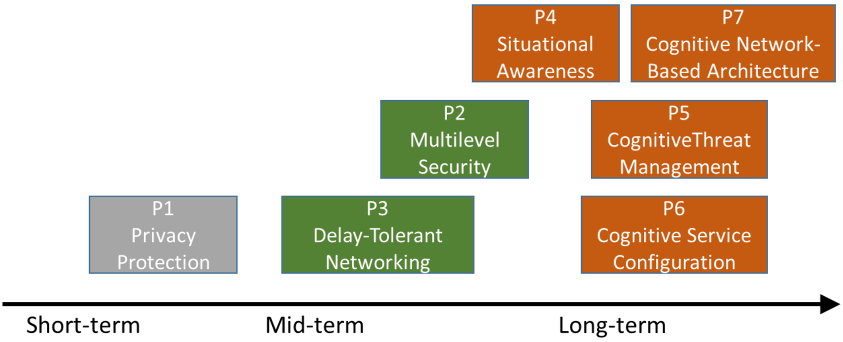

P4
Situational Awareness
P7
Cognitive Network-Based Architecture
P2
Multilevel Security
P5
CognitiveThreat Management
P1
Privacy Protection
P3
Delay-Tolerant Networking
P6
Cognitive Service Configuration
Short-term
Mid-term
Long-term

Figure 1. Publications covering the development roadmap.

The main contributions of this thesis are divided into three development phases:

The short term development. The architectural development concerns privacy protection (P1). An architectural framework model for ensuring privacy in a network centric environment was described to mitigate the threat of losing privacy by hostile intelligence. Privacy is considered through a layered model with content, communication and network levels. The model presents various protection schemes at each layer.

Related Research: Privacy is defined as the claim of individuals, groups, and institutions to determine for themselves, when, how, and to what extent information about them is communicated to others [113]. While privacy is not a new requirement, the networked world poses several challenges, as information may be efficiently gathered, processed, and distributed, also for illegitimate purposes or by illegitimate means. Privacy protection is researched in many studies (see Publication 1), but a privacy protection model including all the layers of a communications system has not been presented.

The mid-term development. The architectural development concentrates on multilevel security (P2) and delay-tolerant networking (P3). A concept of multilevel security (MLS) architecture framework for a network centric environment was defined and a solution for secure information sharing was proposed. Multilevel security was considered from three perspectives; content, communication and network security.

Related Research: The traditional view of multilevel security is to ensure that information at a high security classification cannot flow down to a lower security classification (see Publication 2). In a traditional MLS mechanism, users, computers and networks carry computer readable labels to indicate security levels. Publication 2 considers MLS within a larger perspective, not only limiting to information processing challenges in computer systems, but also expanding the problem to information sharing and network structures.

A security architecture for tactical delay-tolerant networking (DTN) was described to improve security in the battlefield conditions where delay-tolerance is one of the critical communications requirements. The functionality descriptions for each level were defined and implementation challenges of the architectural security solutions for low-bandwidth, high-delay tactical military networks were discussed.

Related Research: The IRTF Delay-Tolerant Networking Research Group (DTNRG) has developed an architecture (RFC4838) [10] for Delay-tolerant networking. The architecture defines an end-to-end message-oriented overlay called the "bundle layer" that exists at a layer above the transport (or other) layers of the networks on which it is hosted and below applications. Security architectures for DTN are defined in many papers (see Publication 3), but a common feature for these architectures is they all focus on a certain piece of security without overall aspects. Typically, these include trust models, authentication or key management, but an overall architecture is not defined.

<u>The long term development</u>. The architectural development in the long term focuses on the cognitive networks and its applications. Publications 4 – 6 utilize a cognitive process to improve network cyber security in a certain part of the area while Publication 7 introduces a new overall cyber security architecture for military networking.

Self-organizing map techniques (P4) were used to provide improved security situational awareness for cognitive networking. Self-organizing map was used to visualize multi-dimensional security status data to help decision-making in a cognitive network system. For testing the performance of SOM, a rough metric for network security was created.

Related Research: Routing performance and auto-configuration of tactical military networks are researched a lot in recent years, but building situational awareness, that is critical for cognitive networking, is studied only in a few research papers. This research includes, for example, the use of Dezert-Smarandache theory for trust evaluation and building situational awareness in mobile hostile environment [30, 31]. Applying the SOM for building situational awareness in a cognitive networking environment is unique.

A three-phase cyber threat management framework (P5) was developed to improve threat mitigation processes in a network system. A cognitive layer enables automated threat management required in a dynamic tactical networking environment. The framework presents a three-phase management process including threat identification, risk assessment, and mitigation tradeoff phases.

Related Research: Most of the research on security of cognitive networks concentrates on a certain piece of security in cyberspace, e. g. security threats and detection techniques or control channel security. Also, threat management is widely studied, but in the context of cognitive vetworking. These studies approach cyber threat at very high-level. The current research typically has a quite narrow scope without presenting an overall approach or framework for cyber threat management (see Publication 5).

A functional architecture with dynamic and cognitive service configuration (P6) was developed to protect military networks against evolving security threats. Cognitive service configuration continuously modifies service structure and configuration making a network system as a moving target to a potential attacker. Without static system configuration the attacker has a challenge to exploit found vulnerabilities as information is out of date immediately after the collection.

Related Research: Only a few research papers of cognitive information services have been published. Zheng et al [115] propose a new intelligent and cognitive Service Delivery Platform model integrated with the concept of cognitive networks. The new model helps the platform turn to an autonomous platform without unnecessary manual interventions. The model provides dynamic system configuration for easier service creation and maintenance. Kliazovich et al [51] propose a novel concept in cognitive network management and protocol configuration in which any protocol of the TCP/IP protocol reference model can be extended to dynamically tune its configuration parameters based on history performance. Jimenez-Molina and In-Young [44] present a novel cognitive engineering mechanism to optimize service functionality coordination. None of the research papers considers cognitive features to enhance cyber security.

A novel cognitive network-based cyber security architecture for mission critical communications (P7) was developed to improve overall cyber security at all layers of a networking system. The architecture includes a new cognitive layer that is responsible for learning and decision-making in accordance with the security requirements and environmental conditions.

Related Research: Several security or enterprise architectures exist, but none of them apply cognitive networking features when addressing security controls design in a communications network [96]. Security architecture frameworks in the context of cognitive networking provide only partial solutions to build a secure networking system. Several security architecture frameworks concern cognitive radios. These include a security framework of access control [61], a physical layer approaches to defense against security threats [37] and an unified layered security architecture with two security sub-layers; application layer and physical layer. [59]. None of the proposed frameworks present an overall architecture supporting cognitive networking systems.

1.4 Structure of the Thesis

The rest of the thesis is structured as follows. Chapter 2 presents the development roadmaps of the network enabled capabilities and the federated mission networking that are leading concepts towards future military communications. The chapter discusses how the security architecture development must be considered when developing networking capabilities according to the concepts.

In Chapter 3, the fundamentals of tactical military communications are presented. The chapter considers basic properties and security requirements for military networks and presents the major cyber threats on tactical networking. Chapter 4 presents the security architecture development in the short and mid-term as it proposes the security architectures to improve privacy, multi-level security (MLS) and network security in delay-tolerant networking.

Chapter 5 covers the paradigm of cognitive networking, and presents an overview of the paradigm and its benefits and promises in network security. The chapter illustrates how network security is developed by using the cognitive network-based approaches such as dynamic service configuration and cognitive threat management for improving the network security architecture. The chapter also presents a novel cognitive network-based security architecture for the long term development. Finally, Chapter 6 includes the discussion and conclusion statements of the thesis.

2. Developing Security Architecture for Military Communications

Network cyber security is one of the critical requirements for military communications [18], and thus cyber security must be considered in all system architectures and future development roadmaps. The purpose of this chapter is to explain how network cyber security is connected to the development of networking capabilities, and how security features be improved as part of the next generation federated Communications and Information System (CIS) [79] capabilities. The implementation of these cyber security architectures must provide an outcome that achieves desired design goals, and security requirements.

According to a definition given by the Open Group [106] an architecture framework is a tool which can be used for developing a wide range of architectures. It should include a method, a set of tools, a common vocabulary, recommended standards and compliant products. Existing defence related architecture frameworks are not fully compliant with the definition, but many of them such as MOD Architecture Framework (MODAF) [66], DoD Architecture Framework (DODAF) [20] and NATO Architecture Framework (NAF) [72] provide relevant assets and values [29]. However, the existing system architectures are very high-level architecture frameworks for security designing purposes. The frameworks do not originally include any security related views or assets. There also exist many architectural approaches addressing the design of secure system architectures but, in many cases, they have a low level of assistance for integrating security mechanisms in the initial system development stages [87], in which an overall security functionality of a communication system is designed.

The context of the capability development is NATO as Finland has chosen to build the future military capabilities in line with the NATO requirements. This decision is stated in the Finnish Government Program [83].

2.1 Cyber Security in Network Enabled Capability Development

Network Enabled Capability (NEC) is a NATO term for implementation of the network centric warfare tenets [79]. The purpose of NEC is to provide the timely exchange of secure information, and to utilize communication networks that are seamlessly interconnected, interoperable and robust. These networks must support the timely collection, fusion, analysis and sharing of coalition information.

The Nato NEC Framework consists of three components: human processes, information and network. The network component comprises a physical element of networking and information infrastructure (NII) that include communications, network, computer, and core services layers. In the framework, Service Level Agreements (SLAs) and network security are critical functions to effectively manage scarce system resources [79].

The NEC concept introduces five Command and Control (C2) maturity levels (phases) [67, 74]. From least capability to most capable these levels are: Conflicted, De-conflicted, Coordinated, Collaborative, and Coherent. The objectives associated with each of the levels is presented in Table 1. The phases provide a step-by-step approach for implementing C2 capabilities that provide operational benefits at each step along the way.

Figure 2 illustrates the idea of evolving operational needs, leading to assessments of architectural concepts and required technology needed to support the maturity levels. The evolution in operational needs is considered through several service components that are Functional Application Services, Information Integration Services, Communications Services, Information Assurance Services, System Management and Control (i.e. System and Network Management), and Policy, Processes and Architectures.

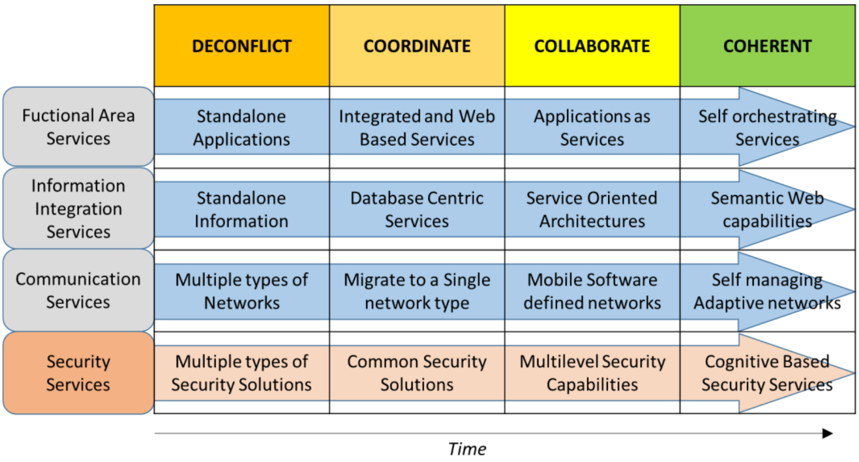
Table 1. The objectives of the NNEC maturity levels [67, 74].

Maturity level	Objective
Conflicted C2	None. C2 systems are implemented by the individual contributors over their own forces or organizations.
De-conflicted C2 – Functional "Stovepipes"	The avoidance of adverse cross-impacts between and among the actors by separating the problem space and the solution space.
Coordinated C2 – Communicate and Inform	Enhanced overall effectiveness by - seeking mutual support for intent - developing relationships and links between and among entity plans and actions to reinforce or enhance effects - pooling of non-organic resources - increased sharing of information to increase the quality of information.
Collaborative C2 – Collaboration and Planning	Developing significant synergies by - negotiating and establishing shared intent and a shared plan - establishing or reconfiguring roles, and coupling actions - rich sharing of non-organic resources - some pooling of organic resources - increasing interactions in the cognitive domain to increase shared awareness.
Coherent C2 – Sensing and Responding	To provide the enterprise with additional C2 approach options that involve entities working more closely together and with the ability to identify and implement the most appropriate approach to coalition C2.

Figure 2 highlights the impact of the development process on the Functional Application, Information and Integration, and Communications Services layers. Information Assurance, and System Management and Control Services function as a back plane and provide services to these higher level applications and services. Unlike in the diagram presented in NNEC Feasibility Study [74], cyber security is added as a new, separated layer to illustrate how cyber security technology and functionalities are to be developed during the NNEC transformation process. The references of the NEC and CIS development [74] do not provide exact phasing for each technology, architecture, or functionalities, but rather consider cyber security development using short, mid and long term approaches.

Cyber security mechanisms are embedded into every aspect of the overall NEC architecture to achieve the overall goal of protecting information and data whether at rest or in motion. The security mechanisms ensure that the right information can be delivered to the right actors at the right time, and that the information that they receive can be trusted. [74]

In the near term (De-conflicting Phase), IP encryption and key management infrastructures are the key enablers to meet the needs for secure communications. In the end of Coordination Phase, the transformation from separated encryption solutions to a common encryption is completed. However, the security solutions are still based on legacy technologies in that phase.



	DECONFLICT	COORDINATE	COLLABORATE	COHERENT
Fuctional Area Services	Standalone Applications	Integrated and Web Based Services	Applications as Services	Self orchestrating Services
Information Integration Services	Standalone Information	Database Centric Services	Service Oriented Architectures	Semantic Web capabilities
Communication Services	Multiple types of Networks	Migrate to a Single network type	Mobile Software defined networks	Self managing Adaptive networks
Security Services	Multiple types of Security Solutions	Common Security Solutions	Multilevel Security Capabilities	Cognitive Based Security Services

Figure 2. Evolving C3 Requirements and Technology Trends for NNEC [74].

In the mid-term (Coordination Phases), security architectures and capabilities are to enable the fielding of dynamic, role-based, policy-based, information access schemes [74]. The long term (Collaboration and Coherent Phases) ambitions include the concept of multilevel security (MLS) with object level encryption, where information is protected at the information object level and access is controlled based on a user identity and a user role within any certain operation [74]. In the Coherent Phase, NII is based on cognitive networking that requires a novel approach and even some major technology breakthroughs to meet the cyber security needs. Thus, it is rational that also the network cyber security capabilities are based and rely on a cognitive network based approach.

2.2 Cyber Security in Federated Networking

Military communications capabilities are developed towards federated networking to ensure more effective information sharing during operations [73]. An example of this capability development is NATO's Future Mission Networking (FMN) concept. The aim is to provide overarching guidance for establishing a federated mission network capability that enables information sharing among nations participating in coalition operations [73]. The FMN concept will be based on trust, willingness and commitment. FMN will enable command and control (C2) services in future NATO operations.

The FMN capability consists of three components that are Governance, FMN Framework and Mission Network (MN). The FMN Governance component is established to effectively manage both the FMN Framework and each MN. The FMN Framework offers a structure to provide processes, plans, templates, enterprise architectures, capability components and tools needed to prepare, develop, deploy, operate and evolve and terminate Mission Networks in dynamic, federated operation environments [73]. Each MN provides a capability of the Communication and Information Systems (CIS), management, processes and procedures.

From an architectural point of view, a goal of FMN is to provide a common, mission-wide information domain where there is open sharing of information underpinned by mutual trust and governed by a common rule set. The common information domain should include the fewest number of security classification levels required to meet the operational commander's requirement in order to reduce the need for complex gateways or manual processes, which would deter information sharing. A security classification level indicates how sensitive information is, and a governmental body sets a level on information that requires protection of confidentiality, integrity, or availability. The levels are typically public, restricted, confidential, secret and top secret [92]. Information in the common information domain should be managed at the lowest classification level permitted [73].

The strategic roadmap of FMN Mission Execution Environment includes three major phases. Figure 3 illustrates the strategic roadmap from cyber security architectural view.

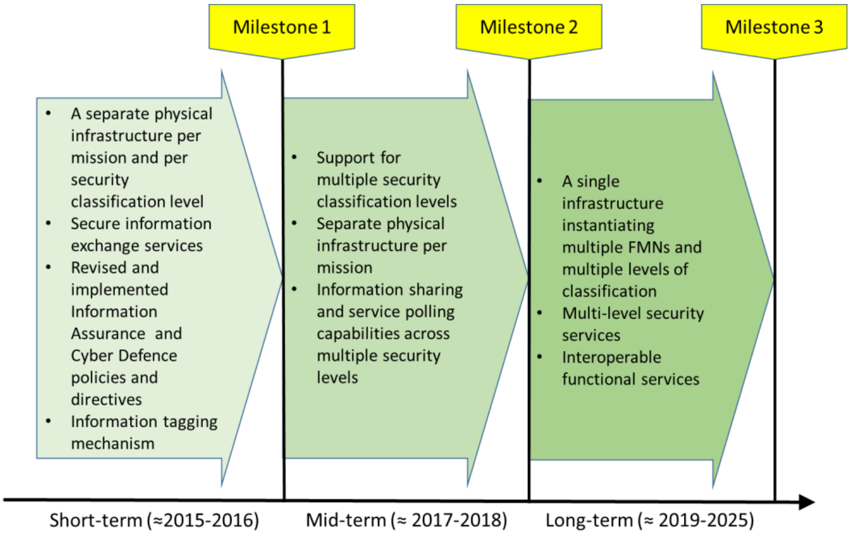

Milestone 1
Milestone 2
Milestone 3
• A separate physical infrastructure per mission and per security classification level
• Secure information exchange services
• Revised and implemented Information Assurance and Cyber Defence policies and directives
• Information tagging mechanism
• Support for multiple security classification levels
• Separate physical infrastructure per mission
• Information sharing and service polling capabilities across multiple security levels
• A single infrastructure instantiating multiple FMNs and multiple levels of classification
• Multi-level security services
• Interoperable functional services
Short-term (≈2015-2016)
Mid-term (≈ 2017-2018)
Long-term (≈ 2019-2025)

Figure 3. The FMN strategic roadmap from cyber security perspective [73].

Milestone 1 refers to a maturity level in which separate physical infrastructures of CIS exist per mission and per security classification level. The aim of Milestone 2 is to achieve support for multiple security classification levels within each mission, but still with separate physical infrastructure per mission. Finally, Milestone 3 aims to achieve a single common CIS infrastructure for all concurrently existing MNs and their multiple levels of security classification.

2.3 Implementing Cyber Security Architectures

A cyber security architecture for military communications must include all the functions that are required to meet design goals and desired security level. Architectures create a plan for high-level direction and guidance, and provide guidance on requirements capture, design, and evolution. The architectures will be implemented through a set of detailed design models [32].

The CIS cyber security architecture is part of an enterprise architecture. The CIS cyber security architecture is a plan that aligns the organization, the CIS, and the technology with high-level direction and guidance [32]. The focus of this dissertation is to develop a technical architecture, and thus, architecture views of organization and processes are out of scope.

NATO's security architecture called CIS Security Capability Breakdown [34] includes a number of high level capabilities from supply-chain management to education. Most of the capability areas concern security management rather than technical design. Implementing security capabilities defined in the CIS Security Capability Breakdown requires more detailed specifications as the level of technical design is not sufficient enough for building technical security functionality for future communication systems.

Military communication systems should be designed to provide battlefield networks that are highly automated, adaptive, interoperable, secure, and resilient to all types of attacks. The cyber security architecture should take care on its part that a military networking system achieves the following goals [28]:

1. *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.
2. *Robustness*. Robustness means a security function, mechanism, service, or solution, reflecting whether it is adequately strong to provide the defined information protection in all circumstances [71]. 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 the products with easily exploitable vulnerabilities reduces the number of attacks. Automated tools to detect and mitigate malicious codes should be developed.
3. *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 homogene-

ous, readily available systems. These two attributes must be addressed carefully. Another critical element that affects the ability to reconstruct destroyed systems, even partially, is system experts with unique knowledge or experience, especially with respect to integration issues.

4. *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. In practice, security up front means that security is considered from the very beginning of system design, and security aspect is basis for decision-making.

In security architecture design, comprehensive principles are needed to achieve an effective security outcome. The principles for guiding security architecture design may include the following [80]:

Defence in depth. In a military context, defensive controls are designed to form a layered model. The objective is to build separated security domains with different types of security controls between them. An attacker must penetrate through many layers to access the most critical information. The defence in depth concept also defines redundancy of security controls, where the failure of one layer is mitigated by the existence of other layers of controls.

Compartmentalization. Different assets and information with different classification levels should exist in physically or logically separated security domains. Attacks that try to access higher-security domains through lower-security domains are mitigated by using trust relationships between the compartments.

Least privilege. The idea originated in military and intelligence operations, is that if fewer people know about confident information, the risk of unauthorized access is reduced. In network cyber security, this means restrictive security policies that allow access to and from a security domain only for the required users, application, or network traffic. All other access is denied by default.

Weakest link. A network security system is as effective as its weakest link. A layered approach to security, with weaker or less protected assets residing in separated security domains, mitigates the necessary existence of these weakest links. Humans are often considered to be the weakest link in information security architectures.

Accountability and traceability. The principle involves the existence of risk and the ability to manage and mitigate it. Network security architectures should provide mechanisms to track activity of users, attackers, and even security administrators. An architectural design should include provisions for accountability and nonrepudiation.

The well-known secure dimensions, confidentiality, integrity and availability [21, 32] provide basic information protection requirements for tactical military information services and networking. Prioritizing the dimensions is challenging, but information confidentiality plays a critical role in military operations.

Classified information is protected by all means to keep operational intentions secret. Disclosing critical data may cause a loss of human lives.

Some balancing between the dimensions is also required [28]. It is possible to build a networking 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.

Security services of ensuring confidentiality, integrity and availability must be decentralized so that the network has no single point of failure. The coherency of a military network is often difficult to maintain as the network may split up into fragments during combat operations.

Multilevel security requirements have become more important as building separated infrastructures is not cost-effective and information exchange between different security domains has become critical in military operations. In many cases, information sharing between the domains is provided by using manual methods leaving a place for undesired behavior, and causing delay in information sharing. At the services and infrastructure layers, the separated systems require information exchange gateways which provide data packet authentication and content monitoring services.

Network security features must be implemented by using light weight protocols and methods that will not add much overhead to data packets. An additional requirement is an ability to reconfigure communication and security parameters after topology changes.

Security requirements for each functional layer are different. At the application layer, confidentiality, integrity and availability of user and application must be ensured. At the services layer, the aim is to protect all services and control traffic against denial of service, corruption and modifications. Security services must provide origin authentication and integrity verification for data packets. The infrastructure layer concerns the protection of the network infrastructure against unauthorized usage. The layer includes security services such as network access control and routing protection [90].

The military network is a subject for military intelligence. In commercial networks privacy is achieved by protecting information and content. In a military environment, protecting information content is less important than protecting communication, existence or time in many cases. Besides of information content, an adversary is also interested in who communicates, in which kind of networks and where network nodes are located. Thus, privacy requirements are defined to protect data content, communication behavior and network control from disclosure. Privacy protection consists of data, identity, location, existence, time, and transaction protection [9].

For delay-tolerant communications, security features must guarantee that [10] unauthorized data is not carried through or stored in a network node, and prevent authorized applications from sending bundles at a prohibited rate or class of service. Also, damaged or improperly modified bundles must be discarded, and compromised nodes must be promptly detected and de-authorized.

Limited power consumption and computation capabilities of mobile tactical devices make networks more vulnerable to attacks such as Denial of Service and incapable to process computation-heavy algorithms like public key algorithms. More chances for attacks are created by enforcing frequent networking reconfiguration of fast moving nodes. For example, it is difficult to decide between true and faked routing information. In a hostile environment, there is high probability for trusted node being compromised and then being used by enemy to launch cyber attacks or to exploit the node for other purposes. In other words, both insider attacks and outsider attacks need to be considered in challenging tactical networks, and probably these insider attacks are even more difficult to deal with. [111]

2.4 Summary

Network cyber security is one of the critical requirements for military communications, and it must be considered while networking capabilities are developed. Both the NEC and FMN concepts include a number of development phases with the design goals for functional area, information and communication services. The requirements for cyber security services are not described in details. However, both concepts identify some important areas of security. These requirements must be noticed in the security architecture development for each evolutionary phase.

The roadmaps of the military CIS capability development extend far into the future including the short, mid and long term development. The roadmap periods are typically longer than those designed for commercial technologies which is reasonable due to interoperability requirements and large investments for decades.

The target state is achieved through several phases. Thus, it is rational that network cyber security architectures are considered and designed to support the phases of the roadmap. While implementing cyber security capabilities, the security, reliability and endurance requirements must be considered. The networking systems must be developed to support operations in hostile and rough environments.

The purpose of the next chapter is to introduce the special characteristics of tactical military networking, and present the requirements for secure information services and networking for military communications.

3. Tactical Military Networking

A military networking environment, especially at the tactical level, is very challenging [95]. Simultaneously, the paradigm and doctrine of Network Centric Warfare (NCW) [2] increases demands on military communications and networking. 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 geographically distributed military forces.

Even though social networking and human's role has increased after the paradigm was introduced, information sharing and communications systems and technologies play a critical part of building situational awareness and information sharing capabilities to the actors of the battle space [114]. The effective linking means that distributed troops can generate synergy through which responsibilities and current tasks can be dynamically reallocated to adapt to changing situations. Effective information sharing requires the establishment of a robust, high-performance information service systems and networks that are able to provide all required services for warfighters across the whole armed forces. [114]

To achieve the full capability of network centric end user services, seamless networks with flexible information sharing are required. At the same time, the tasks of a military mission and battle space conditions set up high requirements for information security in these networks and services. Battle space conditions provide new demands for security solutions. Legacy and commercial standards, security architectures and techniques are often too complex, static and non-reliable for tactical military networking. Implementing commercial off-the-shell (COTS) security technology into military systems is often difficult or even impossible. [52]

This chapter concentrates on introducing of the special characteristics of tactical military networking, and presents the requirements for secure information services and networking.

3.1 Overview

Tactical military networks are designed and built for the tactical-level military operations to enable command and control, firing, intelligence and other operational warfighting services. Originally, these networks were implemented for voice communications, but today the main purpose is to transfer data for several applications and services. A part of the tactical networks operates under extreme circumstances while they are deployed in harsh environments where temperature, weather and other factors set high requirements for functioning. As the tactical networks support moving troops, wireless links are often an only realistic manner to connect troops.

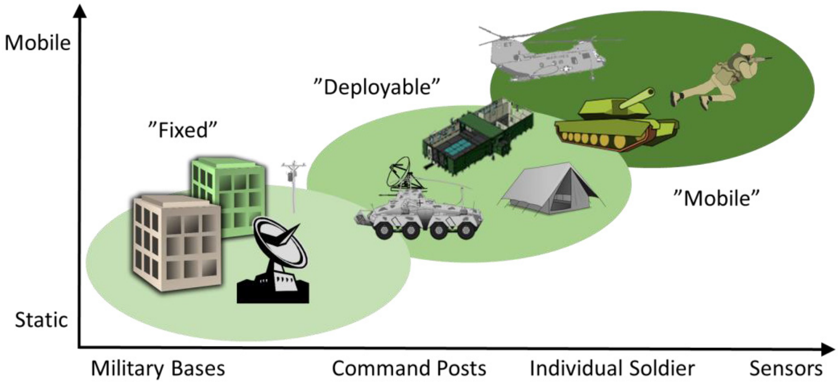


Figure 4. Heterogeneous nature of tactical networking environment.

Figure 4 illustrates the heterogeneous nature and structure of a tactical networking and communications system. At the highest level of tactical edge, the communications system is built to support operational commands, such as joint commands that are typically located in fixed locations (bottom left of Figure 4). Mobile services are not mandatory, but there may appear some needs inside of the headquarters' facilities. [19]

At the task force or brigade level, networking services are based on deployable communications system (center of Figure 4). Networking system is reconfigured according to the phases of the operations, but the services are not provided to support on the move features. At the individual soldier or warfighter level, the networking subsystem consists of the tactical networking services supporting a company or platoon level warfighting. This means that services are built to support command and control on the move.

3.2 Tactical Networking Environments

Roughly, a tactical networking system consists of network nodes and communication links between them. However, the operating environment is different at each level of warfighting. Tactical networking architecture may be decomposed into three information technology (IT) environments, each of which represents a unique category of mission functions [57]. These networking environments are the enterprise environment, the installation environment, and the operational environment.

Each networking environment are decomposed into mission environments, that represent the physical environments such as office environments, command posts, foxholes, etc. In general, each networking environment provides IT capabilities, but the requirements for these services are generated from the user needs focused on each type of mission environment [57].

The enterprise networking environment is the backbone for tactical communications. It enables interoperability, and connects all users operating throughout the network. Unlike the other networking environments, the enterprise networking environment has very few dedicated end-users. The environment is generally characterized by high-capacity and always-on transport, and by shared computing.

The installation networking environment encompasses the portion of networks that is physically located on fixed and temporary posts, camps, and stations. The environment is generally characterized by reliable transport and by mature and connected computing at all levels. It utilizes enterprise network services, provides local network services, and hosts mission-specific applications. [57].

The operational networking environment consists of physically deployable and mobile networking systems. It directly supports operational units whether they are based (at an installation), or deployed [57]. The environment is designed to operate in dynamic, less environmentally controllable, and mobile environments, without fixed IT infrastructure. The environment is generally characterized by disconnected, intermittent, or limited communications, frequency-based transport, and local computing and server capabilities. It consumes limited enterprise services and locally provides and hosts all required applications not otherwise available. Table 2 presents the attributes of each networking environment.

Table 2. Networking environments and their characteristics.

	Networking Environment		
Attribute	Fixed	Deployable	Mobile
Communication links	Fixed optical and copper lines, satellite links	High capacity links, optical and copper lines, satellite links.	HF/VHF (data) radios
Topology	Static	Dynamic	Ad hoc
Link capacity	Mbps - Gbps	Mbps	kbps
Latency	Milliseconds	Hundreds of milliseconds	Seconds
Connectivity	Assured	Disconnection may appear.	End-to-end disconnection may be more common than connection.
Queuing Times	Very short	The queuing time could seconds, and in message systems it could be minutes.	The queuing time could be extremely large (hours, perhaps days).
Interoperability	Commercial, civilian technology ensures good interoperability.	Mixture of military and civilian technologies, tolerable interoperability.	Many special protocols, not designed for interoperability.
Node Longevity	Nodes are mostly located in physically protected environments, great longevity.	Physical protection available in some situations.	Nodes are placed in hostile environments, nodes not be expected to last long due to environmental dangers or power exhaustion.
Duty Cycle Operations	Network devices backup powered, power infrastructure available.	Most critical devices backup powered, lacking power infrastructure.	Network devices often run off batteries when nodes are deployed in areas lacking power infrastructure.
Resources	Memory and processing capabilities of devices at a necessary level.	Memory and processing capabilities of devices at a necessary level.	Limited memory and processing capabilities are used.
Protocols	IP	IP/ Proprietary	Proprietary

Qualitatively, the tactical military networks are characterized by latency, bandwidth limitations, error probability, node longevity, or path stability, which are substantially worse than is typical of static networks as the Internet [23]. It is natural to use the performance of the Internet as a baseline due to its enormous scale and influence [23].

The tactical communication systems are expected to operate in hostile environments where mobile nodes, environmental factors, or intentional jamming may cause disconnection. The network topology at the warfighter level is ad hoc based, and the capacity of the combat net radios (CNR) is typically limited to 64 - 256 kbps. The capacity of the deployable radio relays varies from a few megabits up to hundreds of megabits. However, in the near future emerging technologies such as software-defined radios will provide higher capacity even to the mobile users with 1 – 100 megabit connections [68] depending on circumstances and distances.

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. The tactical systems may also have especially strong infrastructure protection requirements [23].

Based on the ITU-T X.805 standard [90], a tactical networking system can also be divided into three functional security layers: application security layer, services security layer, and infrastructure security layer [54]. The applications security layer focuses on security of the network-based applications accessed by end-users from a high commander to an individual soldier. 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 services security layer addresses the services the 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 to value-added information services such as military C2 tools, location services, messaging, and VPN connections.

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 the building blocks of networks, services and applications are created [90]. 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.

3.3 Cyber Security Threats on Tactical Military Networking

The emergency of large-scale cyber operations has moved network security attacks from the realm of hacktivists to criminal organizations and states what makes threat more dangerous with potential for great economic and political harm. At the same time, today's operations require military force, governmental and non-governmental organizations, and even supporting private sector to be globally networked which provides attackers new and even better opportunities to conduct cyber attacks. Military networks and communication services are always an interesting target for hostile parties. There are numbers of techniques and methods to attack in cyberspace, but the following attack methods [89] are most relevant in the context of tactical communications:

- *Cyber espionage* is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from enemies using exploitation methods on networks, software and or computers.
- *Gathering data* means that classified data that is not securely stored or handled is intercepted and even modified, making espionage possible from the other corner of the world.
- *Distributed denial-of-services* attacks are generated using a large number of computers controlled by an attacker launching a DoS attack against target systems. A huge amount of traffic prevents normal users to access the service.
- *Equipment disruption* may put soldiers and troops in high danger. In military operations communication equipment is vital. Orders and communications can be replaced or interrupted by using different exploitation methods.

Cyber attacks usually do not take place in one shot. Typically, the attacker first engages in mapping out the opponent's networks, resources, IP addresses, open or vulnerable services, and so on. This is called reconnaissance or cyber intelligence, and the attacker may try to get information that appears to be harmless if discovered, but may have some impact on cyber security later. The reconnaissance phase is followed by exploitation of vulnerabilities, information theft, taking over of hosts, feeding malicious information, etc.

Wireless military communication systems such as tactical networks provide a larger attack surface than fixed systems because of weaker physical protection and radio signal propagation. The tactical networks face the same cyber security threats as the fixed systems, but the wireless channels and interfaces cause some new threats. Table 3 lists some major cyber threats on the tactical wireless systems [93].

The *passive* methods include wiretapping and traffic analysis. In the tactical environment, wiretapping is a potential risk for losing confidential data, and it is almost impossible to avoid it. Traffic analysis is a consequence of succeeded wiretapping. Although all traffic is encrypted traffic analysis may provide critical information of communication profiles and command structures.

The *active* methods consist of packet replay, fraud counterfeiting, packet tampering, and denial of service. The purpose of packet retransmission is to cause malfunctioning in a target system. For example, a software defined radio may change transmit frequencies as a result of a fake packet. Fraud counterfeiting enables communication with unauthenticated network nodes as a node uses a fake identity. [93]

Table 3. Passive and active cyber threats on the military information service infrastructure.

Threat	Description	Security risks
Passive		
Wiretapping	Interception of transmitted data packets.	Access to confidential information. Disclosure of the structure of network or importance of various nodes.
Traffic analysis	Analysis of characteristics of packet frequency, length and etc.	Disclosure of the communications profiles and users.
Active		
Packet replay	A data packet is re-transmitted.	Undesired functions in the target system (malfunctioning).
Fraud counterfeiting	A network entity behaves as another entity to carry out network activities,	Communication with unauthenticated network entities.
Packet tampering	Data is modified, or deliberately delayed transmission, or a passive change in the order.	Integrity failure, delays, traffic fluctuation, network congestion. Injection of malicious code.
Denial of service	An authorized entity cannot access to the services	Service availability failure. Critical systems and services are not available when required.

The purpose of the packet tampering is to modify packets or packet transmission between network nodes. This could be used to corrupt messages or act as a relay that corrupts selected frames. By modifying data packets malware could be injected into the system. The enemy also attempts to cause blackouts to the opposite's communications systems. Denial of service attacks is an efficient method in which services are overloaded to deny service availability. A challenge with tactical networks is that these networks are not always connected to the global internet, and thus this attack requires other means to gain connection to the tactical ICT servers [93].

3.4 Summary

Military operations require reliable and secure communications networks also at the tactical level. At the tactical level, communication systems consist of several subsystems with certain capabilities depending on deployment scenarios. Thus, the communications infrastructure in the tactical environment is very heterogeneous. The infrastructure includes several technologies supporting both fixed and mobile users.

Managing cyber security of the heterogeneous system of systems is challenging due to variety of technologies and protocols, movement of the network nodes, changes in topology, and loss of connectivity and at worst, network nodes. The tactical networks are subject to a wide spectrum of cyber threats. Commercial solutions used in military systems provide the adversaries many benefits when searching vulnerabilities and creating exploits. Both the passive and active methods are used to disturb and damage communication networks, or to steal or modify data.

The next chapter presents three approaches to improve network cyber security prior to the coherent phase of the NEC roadmap (see Figure 2).

4. Developing Security Architectures Prior to the Coherent Phase

This section focuses on architectural development before the coherent phase networking (see Figure 2). During these previous phases (coordination and collaboration), security improvements are provided by developing legacy architectures without changing the fundamentals of a cyber security architecture.

In the coordination phase, the interoperability of security functions is achieved by implementing common security solutions. Interoperability is reached through the agreements of using similar security controls and protocols. For the coordination phase, the chapter introduces a security architecture for privacy protection (P1).

As previously described, one of the important goals of the collaboration phase in the NEC development process is to implement multilevel security capabilities. The chapter presents an architectural framework for multilevel security (P2), but it also introduces an architecture for secure delay-tolerant networking (P3) as an example of adding new functional layers into the legacy security architectures. The chapter presents the essential results of Publications 1 - 3, while the papers themselves provide further details.

4.1 A Security Architecture for Privacy Protection

As it was stated in the previous section, privacy is one of the key functions during warfighting. Disclosing critical data may cause deaths and operational failings. Threat against privacy includes all means of military intelligence such as signal, open source and human intelligence. Tactical networks have become more wireless, which makes the usage of electronic warfare capabilities easier. Wireless nodes could be located by tracking radio frequency (RF) signals and recording them.

Privacy in this study is understood as unauthorized data exposition, and thus the level of privacy is not mathematically defined or measured. There are many well-known measures for privacy such as k-anonymity [97] and ε-differential privacy [22]. k-anonymity seeks to hide individuals within groups of indistinguishable records. A release of data is said to have the k-anonymity property if the information for each entity contained in the data set cannot be distinguished from at least k-1 individuals whose information also appear in the same set. ε -differential privacy, based on confidentiality, seeks to limit the knowledge gain provided by the output data. ε-differential privacy uses a randomized algorithm to guarantee that presence or absence of an individual will not affect the final output of the query significantly. These measures could be used for evaluating and developing the technical security mechanisms presented in the proposed architecture.

Figure 5 illustrates a security architecture (presented in P1) with privacy protecting mechanism at each layer of a networking system. The architecture includes the layers according to the IP stack with two additions that are the host layer and the packet layer. In the architecture, the infrastructure layer is protected using physical connections such as optical and copper cables, or in a case of wireless communications, methods such as frequency hopping or spread spectrum techniques. Protection of the MAC protocol is provided with link encryption and link authentication whenever required. At the packet layer, privacy is ensured by using packet level authentication (PLA) in which data packets is authenticated using digital signatures and forwarded only through valid routes, and to some extent on the network level, for example, using IP Security Protocol (IPSec).

The IP level at the services layer is protected by using with IPSec together with the IKE protocol for key exchange. The host layer, originally from the HIP [76] architecture, adds a cryptographic namespace to the IP stack, thus enabling authentication, mobility, multi-homing, and easier IPv4/IPv6 transition in a sound way [76]. The transport layer provides similar services as IPSec, and these are data origin authentication, confidentiality, and integrity verification. On the transport layer, protocols such as TLS/SSL and SSH [12] are applied. Whether to deploy network or transport layer security depends on the situation.

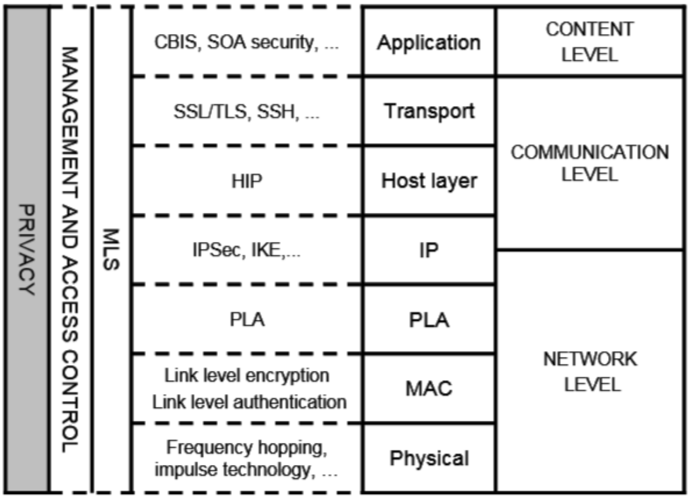


Figure 5. A security architecture for privacy protection (P1).

The protection of the application layer includes Content-Based Information Security (CBIS) [8], end-to-end encryption and Service-Oriented Architecture

(SOA) [55] techniques. Management and access control, and future multilevel security capabilities concern all the layers to ensure overall management and to provide the ability to process information belonging to the different security domains.

The presented architecture ensures privacy with many means at each layer of the network system. At the application layer, content privacy can be ensured by encryption and access control. Furthermore, functional measures such as avoiding the usage of identity or role information, especially in clear text, should be enforced. Location privacy needs to be ensured by measures at the infrastructure layer. Existence privacy can be enforced, for example, by steganography in which a file, message, image or video is concealed within another file, message, image or video [45].

The services layer comprises the transport, host, and IP layers of the protocol stack. The content of the communication can be protected by encryption. Identity of nodes can be enforced by not using IP addresses as an identifier, but only as a location identifier, and to ensure that cryptographic identities can be protected by anonymity schemes or multiple certified cryptographic keys. Location privacy may be ensured by various packaging means [24]. Existence privacy of identities may need to be enforced on lower levels, however, user behavior through sufficient training typically reduces the amount of traffic in the network and therefore ensures better protection with respect to location and existence. Transaction privacy can be enforced by encryption of the IP packet together with scrambling to protect the length of the IP packet which may give away the type of signalling.

The infrastructure layer comprises the IP, packet, MAC, and the physical layer of the protocol stack. At this layer, privacy can be enforced by network design (placing of nodes, usage of dummy transmitters), networking procedures (mobility, radio silence, trafficking patterns), radio technology (spread spectrum, frequency hopping), transmission power and direction, and access control to network resources.

4.2 Multilevel Security Framework

Multilevel security (MLS) capabilities are a key to improve data processing and sharing between several stakeholders on the battlefield. Publication 2 presents a MLS architectural framework depicted in Figure 6. The framework represents MLS as an entity which has functional elements and areas. Implementing the MLS capability is based on a common policy which covers all the authorities, and includes all the classification levels and domains. To guarantee interoperability between content, communication and network elements, a Service Level Agreement (SLA) is provided. SLA includes an agreement of supported capabilities between the content, communication and network elements.

On the content level, multilevel security is executed by implementing Content-Based Information Security (CBIS) capabilities. Basically, all classified information is processed in a same physical infrastructure and operating system. In a CBIS system, the security domains are created on the content level, instead of the system level. On the communication level, MLS is supported using the "edge" device (the boxes with letter E in Figure 6) with security capabilities.

The network layer consists of protected core networking (PCN) [34] elements. PCN is a concept to be used to implement a flexible transport infrastructure that supports future military operations based on NEC. PCN is based on creating a loose coupling between CBIS domains and the transport infrastructure meaning that the CBIS domains are allowed to move to another location and reconnect to the PCN core without any manual configuration. PCN focuses on the provision of high service availability, also in high-threat environments. The PCN network includes a set of security features to support information transportation in the sense of MLS. Security services provided on each layer are presented in the following chapters. Publication 2 explains the services in more detail.

CBIS provides a single physical and virtual IT infrastructure environment that interconnects different information domains for command and control, information sharing, and situational awareness dissemination, while enforcing and maintaining security and privacy concerns. CBIS distributes the access control information to the content or documents [49].

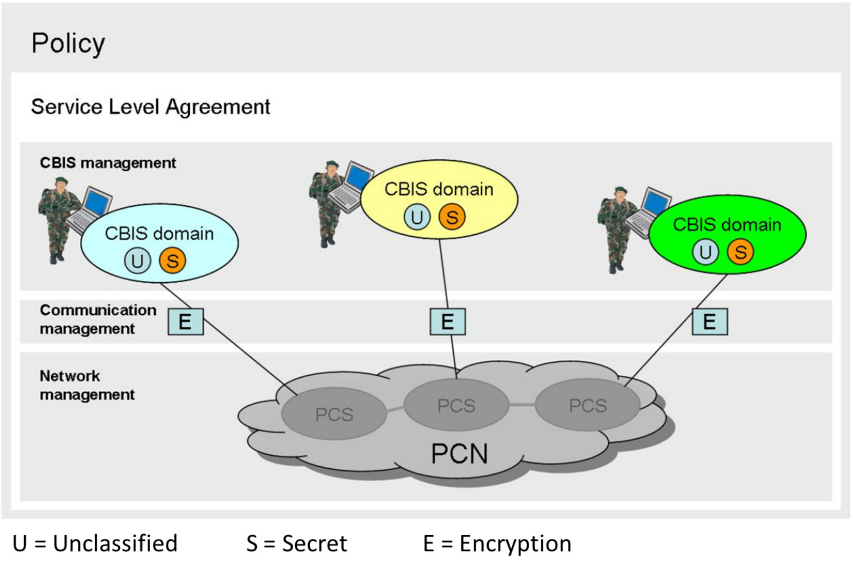


Figure 6. A concept of MLS framework.

CBIS considers the issue of sharing information in such a way that the content, while placed in a shared domain or transmitted cross domains, is protected end-to-end, and only authorized users may gain access to that information. CBIS is also characterized by multiple independent, yet co-operating security domains, which need to interchange content as well as access control information with each other. CBIS encrypts and signs all of the content and related metadata. Most of the CBIS requirements rely on proper selection and expressiveness of the underlying cryptographic schemes to be used for the key management.

At the communication level, MLS defines the capabilities needed to connect CBIS domains into the PCN network segment. The main services produced by the communication level element are:

- Fixed transmission Rates (to prevent critical information to be discovered)
- Flow control (Quality of Service for critical information)
- Peer discovery (enables to set up connections between two different CBIS domains without pre-knowledge)
- Multicast group mapping (functionality to allow mapping of multicast groups between CBIS domains)
- Seamless relocation of CBIS domains

The PCN trusted network provides following basic services and characteristics [34] at the network infrastructure layer:

- Authentication (supporting seamless connectivity, connection between PCSs)
- Risk level feedback (requires superior knowledge and dynamic real-time risk assessment)
- Traffic flow confidentiality
- Trust-based routing
- Dynamic accreditation of a PCS (a method to accredit (or reject accreditation of) the systems even in the presence of frequent changes)
- Federated security management (ability to exchange management information (related to the risk level, security policies, and key management) between PCSs.

The features of PCN bring many benefits to both network users and operators. Traffic flow confidentiality is guaranteed because the protected core knows which paths in the network offer confidentiality. The purpose of traffic flow confidentiality is to hide communication structures and hierarchies. PCN supports seamless mobility of security domains by offering dynamic set-up of secure connections. The PCN supports transporting information from different classification (CBIS) domains in the same physical infrastructure. Traditional cryptographic separation is used between information security domains.

Traditional ad hoc management does not provide the means to respond to changes in the network environment in an automated fashion. In PCN, the management agents that enforce the security policy are network nodes. The nodes have to communicate with the management system constantly in order to receive policy updates or report back their status with respect to the enforcement of the current security policy. In order to provide a trusted path through the network, a standard requirement in the network element security policy is for each node to authenticate the link that it monitors. As a result, all links in the element are authenticated.

In order to ensure proper MLS services, a Service Level Agreement (SLA) must be negotiated. The SLA must cover available security and communications services including necessary parameters such as bandwidth, delay, cryptographic schemes, authentication protocols, and priority. The SLA enables service predictability for the CBIS domains, and gives the PCN network the ability to differentiate services according to policy (e.g., ensuring that CBIS domains with critical data are not prevented from receiving service).

Understandable policy is the key to manage MLS in the whole information and communication system supporting the network-centric warfare. Policy should state explicitly what the system must do. Policy explains very clearly how classified information is processed and shared, and how clearance levels of users and classification of information are provided.

Publication 2 presents some challenges of implementation but an important research area will be integration of CBIS and PCN mechanisms. Integration issues concern for example key management, identification and service access capabilities, and cross-layer functionalities.

4.3 Delay-Tolerant Networking

Several security architectures for DTN are presented, but a common thing for all the architectures is that they only focus on a certain part of network security such as trust models, authentication and key management. In Figure 7, a security architecture for tactical DTN is presented. The architecture is inspired by the architectures presented by Candolin [9] and Wang [111].

In the proposed architecture (P3), the content level handles "end-user products", such as information or services. The communication level takes care of the distribution of the content as well as protocol signaling. The network level comprises the physical network infrastructure. The architecture also includes policy and management segments. The architecture is described in more detail in Publication 3.

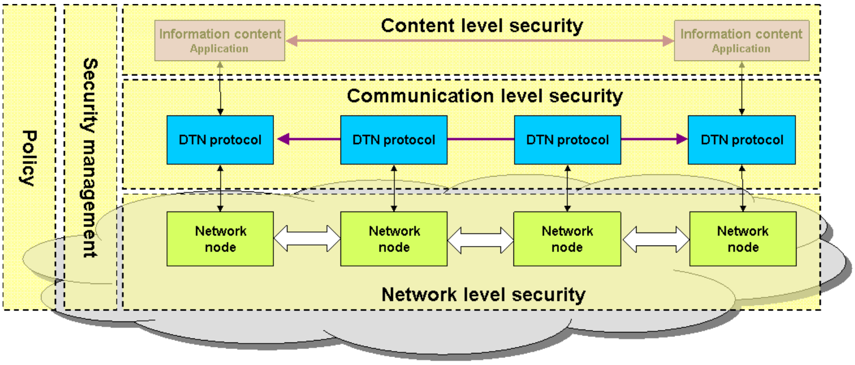


Figure 7. A security architecture for tactical DTN.

Security on the content level ensures confidentiality, integrity, availability, and trustworthiness of the content as well as verifiability of the source. On the communication level, security is ensured end-to-end between communicating nodes, and protocol signaling is protected. Communication level security services include data origin authentication, confidentiality and integrity verification. The network security level is concerned with protecting the network infrastructure and includes services such as network access control and Denial-of Service (DoS) protection.

To ensure confidentiality, availability and trustworthiness at the content level, the concept uses the previously introduced CBIS. The communication level ensures secure information transport between endpoints. The layer consists of the DTN protocols (the bundle protocol and convergence layer). Bundle Security Protocol (BSP) [99] has developed to improve security capability of the original bundle protocol. BSP provides data authentication, integrity and confidentiality services. BSP provides separate capabilities to protect the bundle payload and additional data that may be included within the bundle.

The network level provides the capabilities to protect physical transport and provide network access control for tactical DTN. The network level includes the physical, link and bundle transport layers. In the tactical networks, physical security is provided for example using frequency hopping and spread spectrum techniques in wireless systems or using optical cables between the communication nodes. Physical security is also increased by utilizing specific network tactics (movement, radio silence, trafficking patterns) and using robust network design (placing of nodes, usage of dummy transmitters).

As with Publication 2, practical integration of BSP and CBIS requires further research. Cross-technology transactions and communication remains open. For example, how key management for CBIS is implemented to guarantee a reliable key exchange in a delay-tolerant networking system where communication links are not continuously maintained.

4.4 Summary

Before the coherent phase development, the security improvements include common security solutions and multilevel security. The proposed security architecture for privacy protection includes many security protocols that could be used as the common solutions for military operations. The architecture includes various protocols to be used at the different layers of a CIS system.

Multilayer security capabilities are key requirements for the collaboration phase. The presented architecture is based on the PCN core and CBIS domains that are allowed to move around the core transport system. The CBIS domain enables processing and sharing data from all classification levels in a same physical infrastructure. The DTN cyber security architecture integrates CBIS and BSP to provide delay-tolerant networking system.

A main challenge with the all architecture is how to manage complexity of the systems in the tactical warfighting environment. The layered approaches require some cross-layer communication. The key management for CBIS may appear challenging as all data elements are separated by a specific key.

To support cognitive networking in the NNEC coherent phase, and to provide a holistic approach for network cyber security, a new approach is required. The next chapter introduces a cognitive networking paradigm, and presents how cognitive features are used to improve network cyber security. The chapter also proposes a novel network cyber security architecture with cognitive layer.

5. Developing Security Architectures for the Coherent Phase

In the Coherent Phase of the NEC development (Figure 2, page 13), the networking and information infrastructure is based on cognitive systems and behaviour. Military communications networks must be self-aware to govern themselves and provide resilient communications capabilities for applications and services. Self-awareness is a prerequisite for learning that is a critical element to reduce human involvement. Although, some existing breakthroughs such as machine learning, reasoning techniques and biologically inspired computing may be used for building cognitive behavior into military networks, more innovations are demanded. [60]

Cognitive networks are a promising paradigm and the future of military communications. Cognitive networks are simply needed because they enable network operators to focus on other important issues instead of manual network configuration and management [60]. Especially in a military tactical environment, soldiers should not concentrate on managing military networks, but conduct their main warfighting tasks. Manual configuration provides a higher risk for misconfiguration and causes delays when redeploying the network systems during military operations.

Cognitive networks [60, 103, 105] can dynamically adapt its operational parameters in response to user and service needs or changing environmental conditions. The networks can learn from these adaptations and exploit knowledge to make future decisions. The applications of cognitive networks enable the vision of pervasive computing, seamless mobility, ad-hoc networks, and dynamic spectrum allocation, among others.

This chapter introduces the cognitive networks, and presents the main features of these networks. The chapter also discusses on the promises of cognitive capabilities for military networking, and presents three conceptual applications (P4 - P6) to improve network cyber security. The aim is to show how cognitive capabilities enhance security in military communications networks. The chapter presents a cognitive-network based cyber security architecture for tactical military communications (P7).

5.1 Cognitive Networks

The cognitive networks provides a smart communication platform which could observe its internal and external environment, plan, decide and adjust its parameters as a result of this process. The adjustment is done according to the desired goal, which could be set by users, applications or other services depending on situation. Because of this automated functioning, the hostile environment and dynamically changing goals, overall security of the network is challenging to obtain, although the cognitive layer is in theory able to take care of all the security requirements.

The basic functions of the cognitive networks include observation, learning, decision-making, self-management, and automatic configuration [60]. Thomas et al [102, 105] 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.

5.1.1 Cognitive Process

An important element of the cognitive network is a cognitive engine or process that includes all learning and decision-making features needed to reach service level goals. The cognitive process could be regarded as the commonly known OODA loop [6], in which the network observes, orients, decides and acts. The cognitive process attempts to exactly perceive the current network situation and plan and decide to meet the end-to-end goals in an entire network aspect. Figure 8 presents the phases of the OODA loop in context of networking.

First, in the observation phase, the network collects status information from all relevant sources. The phase is critical as the effect of a cognitive network's decisions on the network performance depends on how much correct network status information is available. If the cognitive network has all knowledge of the entire network's state, cognitive decisions should be more "correct" than those made in ignorance. For a complex and heterogeneous system such as military tactical networks, it is unlikely that the cognitive network would know the exact system state. Transferring status information through all network elements may be high costly, meaning CN is required to work with less than a complete picture of the network resource and performance status.[102]

The observation phase is followed by the orientation phase in which all observed information and previous knowledge are added together and analyzed. For learning capabilities, an appropriate amount of history data has to be available to the cognitive process. Learning is an important part of the orientation phase as it may prevent the recurrence of past mistakes in future decisions. Various methods such as filters and weighting may be used in the orientation phase. During the decision phase, the best decision for the desired end-to-end goal is made.

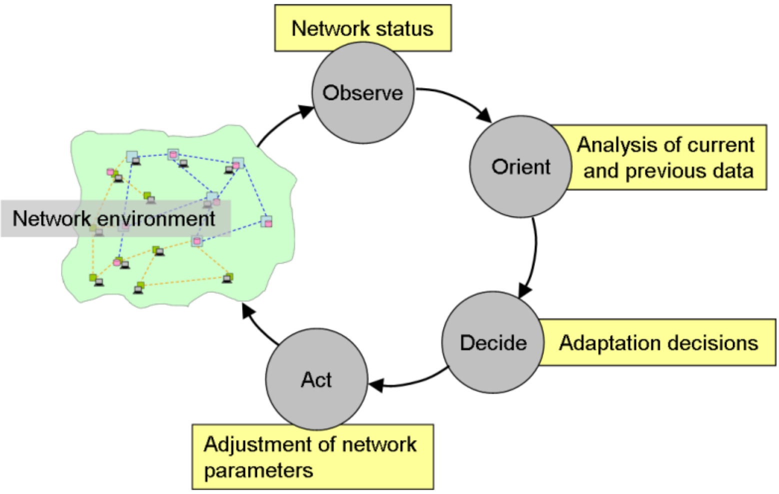


Figure 8. The OODA loop in context of cognitive networking.

Finally, a network adjustment is provided through the acting phase. The adjustment includes modifications and reconfiguration of cognitive network elements. The network nodes 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 accomplished actions have a 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.

5.1.2 Cognitive System Framework

Figure 9 illustrates a cognitive system framework [105] including 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 that are 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.

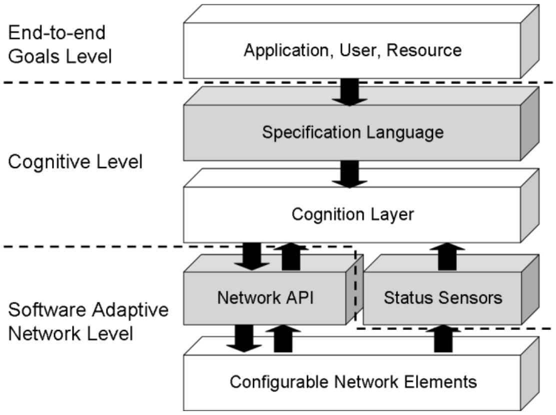


Figure 9. A cognitive system framework.

For connecting the top level requirements to the cognitive level, an interface layer must exist. Information about the goal must not be globally known by network nodes, but needs to be communicated between the source of the requirements and the local cognitive processes. Other requirements for the specification language include for example a support for distributed or centralized operations with the information sharing between multiple cognition layers. The specification language does not actually provide cognitive processes, but the language layer is required to translate application level requirements for the cognitive layer.

The cognitive process of the network can be either centralized or distributed. In a 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 such as neural networks, genetic algorithms, artificial intelligence, Kalman filters and learning automata algorithms [102].

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.

5.1.3 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 [104]. 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 [60]. 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.

5.2 Benefits of Cognitive Networking for Network Security

The cognitive networks present a novel, motivating approach for the development of the future military communications systems. In theory, the cognitive networks will offer better networking and security capabilities to meet the high requirements of battlefield communications. From a network performance point of view, the following value-added factors can be highlighted:

- Speed of adaptation
- Interoperability
- Usage of network resources
- Security

Cognitive, self-adaptive networks are able to respond quickly to the changing service level and performance requirements, primarily caused by developing operational needs. This may require updates for example in network topology, resource allocation, and security levels. Cognitive networking reduces 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.

Achieving the maximum effectiveness of network centric operations, full interoperability between the actors’ networking systems, interfaces and protocols is required. Interoperability is a key for modern warfighting and especially for joint operations where military services and branches conduct operations side by side supporting each other. Cognitive, software-programmable network devices enable complete adaptation of network protocols and parameters [25]. For example, the waveforms in tactical radio networks 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 the reachability of network nodes. The more nodes are compatible, the wider area of network coverage can be obtained. Gateways between cognitive network elements are transparent enabling open information flow between the network elements, and thus the quality of information can be maintained at the high level as this information flow remains unmodified while it passes the nodes.

In tactical military networking, the efficient usage of the network resources particularly means the efficient utilization of electromagnetic radio spectrum. Legacy radio technology only supports partial utilization of the frequency spectrum. The cognitive radio network is able to identify and utilize idle parts of the spectrum [25]. In the future, dynamic spectrum usage will be a mandatory capability as the number of wireless devices keeps growing. The effective use of network resources is not only limited to the efficient use of spectrum as the cognitive network is also 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 is the most interesting factor. In theory, a cognitive system is able to observe and adjust all the security parameters 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 the network security policies. The network is able to adapt 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.

As the previously described cognitive process controls all the elements of a communications network, a CN based network enables a holistic and dynamic approach for managing security parameters, building situational awareness and protecting mission critical networking. Through automated adaptation all the security parameters and controls can be continuously adjusted to provide the best available protection against current threats. The optimization of security parameters is provided through the entire network and all the layers which means that all conditional events are considered during the adaptation process.

In a networking system, privacy must be ensured at all the layers and entities. There are many methods, such as packet level authentication (PLA) [9] or data encryption, to build privacy and confidentiality, but guaranteeing that the privacy requirements are met through all the layers and network elements demands a common and distributed process such as a cognitive process.

The cognitive layer may also provide secure data processing in and between different security domains (e.g. confidential, secret, and restricted) as new efficient security controls such as flow control (domain access, information sharing between different domains), risk level feedback and trust-based routing are implemented within a cognitive system (see Section 4.2).

A cognitive network is a promising approach when concerning network robustness and resilience. In military networking, the environmental conditions vary a lot, and a hostile adversary is always present. Network nodes may lose their connectivity causing a need for delay tolerant capabilities and disaster recovery. The cognitive process may bring some advantages when delay-tolerant (P3) and distributed operational capabilities are required for military missions.

Situational awareness (SA) is a key functionality to build overall understanding of network security including cyber threat evaluation, risk assessment, and the knowledge of the network state and performance. SA plays a critical role when a network is adjusted during operations. With incomplete decisions the situation may lead to the conditions where the network is not operational anymore. Through the cognitive process, SA could be established automatically and preciously. Several methods could be applied for building SA. The Self-Organizing Map is an example of these methods (P4).

Cognitive networking also provides a support to dynamic information service configuration. Static configurations are attractive to attackers as a configuration do not change between intelligence and attacking phases. Instead of having a static network configuration, dynamic service configuration makes a military network a moving target for the adversary (P6). The cognitive network may change its information service configuration randomly or with a certain rule so that the attacker's intelligence information expires before the attack will influence.

The cognitive process enables an automated cyber threat management. The cognitive process is able to collect threat data from various sources and to analyze this data to create threat awareness. Publication 5 introduces a layered framework of cyber threat management for cognitive networking. The framework provides functionalities to identify threats, and to run a risk assessment process automatically. Through the previous strengths, the opportunities of the cognitive security management include faster adaptation to a changing environmental and threats, effective resource-usage, enhanced privacy and data confidentiality, higher robustness and resilience, and better situational awareness and overall security management.

5.3 Improving Cyber Security Using Cognitive Process

As it was stated in the previous section, the cognitive network includes many advantages for tactical military communications. The cognitive layer provides several benefits when cyber security architecture for military networking is developed. The following sections present three architectural design cases in which the cognitive behavior potentially improves networking security. In the first case, a self-organizing map is used to build situational awareness in a cognitive network (P4). The second case concerns threat management (P5), and the third one introduces a cognitive service management (P6).

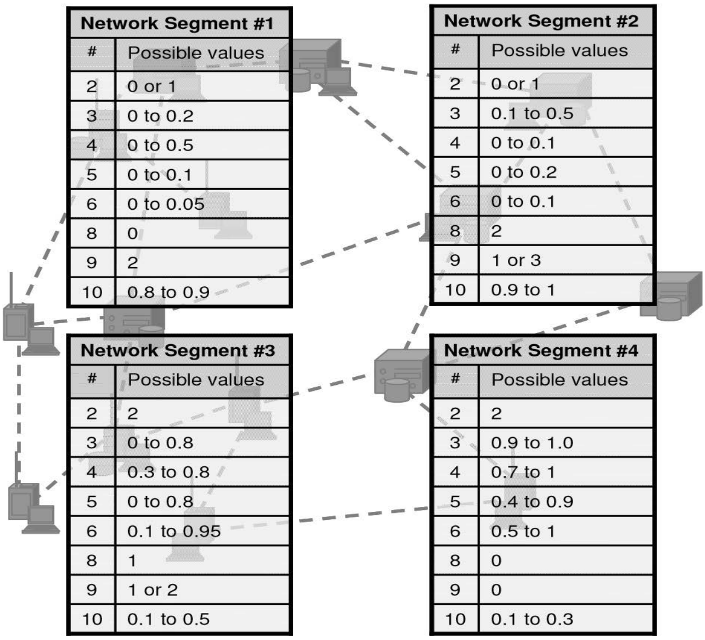
5.3.1 Situational Awareness of Network Security

Situation awareness in a cognitive network- based network is provided through a cognitive process. For making rational decisions, a cognitive system such as a cognitive network must be aware of available resources and capacity, current configuration and previous states of the network. The construction of rational security situational awareness requires an appropriate metric for security that could be measured. The security metric can be defined using a comprehensive approach in which security parameters are considered from all the security perspectives: authentication, authorization, availability, confidentiality, integrity, and non-repudiation [41].

The Self-Organizing Map (SOM) [53] is an efficient tool to analyze and visualize multi-dimensional data. SOM is a type of artificial neural network which is trained by using unsupervised learning to produce a low-dimensional (typically two-dimensional) and discrete representation (called a map) of the input space of the test data samples. In this case, SOM is used to analyze and visualize observed parameter data of network security to create the situational picture of network security. During the training phase, a multidimensional data collection is repeatedly presented to the SOM until a topology preserving mapping from the multi-dimensional measurement space into the two-dimensional output space is finally attained.

The SOM method has been compared to other data mining technologies in many research papers [4, 56, 64]. Performance analyses show that SOM is an efficient method when processing multidimensional data processing. However, the analysis results depend on the features of data sets and preconditions. Other techniques are to be analyzed in further research.

Measurable security metrics are studied in many research papers [38, 82, 88]. Most of them propose qualitative metrics that are not an appropriate approach as the SOM requires quantitative input data. In Publication 4, a rough metric with twelve parameters was defined. The purpose was not to define the best possible metric for security measurements but to build a metric that produces reasonable parameter values to be fed into the self-organizing map. Most of the parameters indicate the percentage level of expected or unexpected protocols and methods of data traffic in each ad hoc network node (see more details in Publication 4).



Network Segment #1

#	Possible values
2	0 or 1
3	0 to 0.2
4	0 to 0.5
5	0 to 0.1
6	0 to 0.05
8	0
9	2
10	0.8 to 0.9

Network Segment #2

#	Possible values
2	0 or 1
3	0.1 to 0.5
4	0 to 0.1
5	0 to 0.2
6	0 to 0.1
8	2
9	1 or 3
10	0.9 to 1

Network Segment #3

#	Possible values
2	2
3	0 to 0.8
4	0.3 to 0.8
5	0 to 0.8
6	0.1 to 0.95
8	1
9	1 or 2
10	0.1 to 0.5

Network Segment #4

#	Possible values
2	2
3	0.9 to 1.0
4	0.7 to 1
5	0.4 to 0.9
6	0.5 to 1
8	0
9	0
10	0.1 to 0.3

Figure 10. The network segmentation and possible parameter values for data generation.

Input data for the SOM was generated by using a segmentation in which the tactical network is divided into four segments with the specific ranges of the network security parameters.

Each segment was able to receive parameter values presented in Figure 10. The range of values of the parameters #1, 7, 11 and 12 are explained in Publication 4. For the demonstration, 2000 samples from each network segment were generated. The parameter values were randomly produced so that they clearly represent the behavior of each network segment. Motivation for using random data was to generate test data for testing the proposed concept. Producing realistic data requires more research.

The values were modified to follow the truncated normal distribution, also known as the Gaussian distribution. The normal distribution is commonly used to avoid the uniform distribution which could cause the SOM feature map to appear flat [53]. The normal distribution is reasonable for analysing overall behaviour of the proposed concept, and thus the use of other distributions was not researched during the study.

Figure 11 presents the U-matrix of a self-organized map. The colors on the map illustrate the distances between the SOM map units. Dark blue colors indicate short distances, and dark red colors long distances between the codebook vectors (map units). Several clusters can be observed from the figure. The clearest three clusters appear on the right side of the map. The map proves that some input samples have common features which form these separated clusters in the output space.

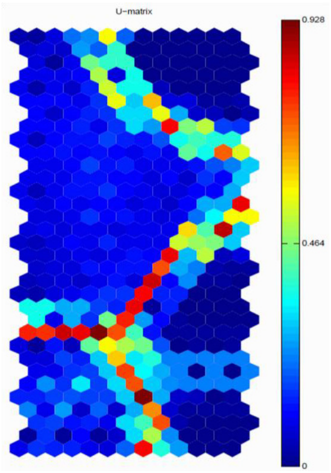


Figure 11. The U-matrix of the data set. Dark colors indicate short distances, and red colors long distances between the map units.

Figure 12 shows the Davies-Bouldin index [48] and a clustered map. The indexes are calculated when the number of the clusters varies between one and ten. The diagram in Figure 12(a) shows that the optimal number of the clusters is four when the maximum number of the clusters is ten. Figure 12(b) presents the optimally clustered map based on the index.

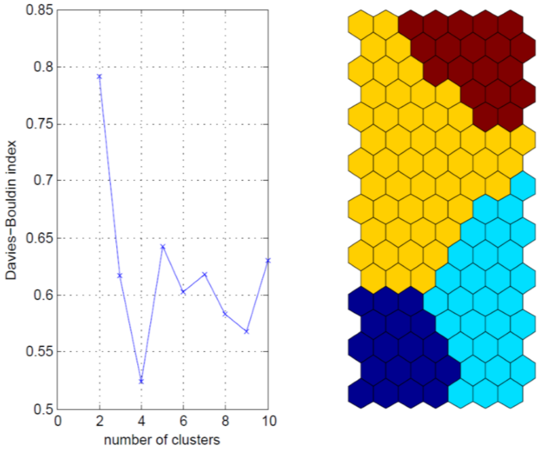


Figure 12. Clustering the SOM with the Davies-Bouldin index. Diagram (a) dictates the values of the index, and Fig. (b) shows the clustered map. The ideal number of the clusters is four according to the index.

The SOM is also a proper tool for monitoring a status of different processes [110]. The observation of the network security status can be figured as a continuous process which generates status information samples in a certain time interval. The current status can be shown on a trained SOM. When the network is operating in desired conditions, the status data sample is located to the map area of normal operations. When an undesired state is obtained, the status data sample is located to the map area of abnormal behaviour.

The monitoring feature is demonstrated in Figure 13. The figure illustrates three pieces of security status data which were generated using unwanted values of the security parameters (no encryption, high service blockage, no authentication applied, etc.). The figure depicts that these samples are located to the map area of the segment 4, which is related to the anomalous operating state. One of the samples clearly belongs to the cluster of the segment 4 inputs, and two of them are located to the boundary area, which can illustrate that the network state is moving towards or away from the undesired state (if time series are examined).

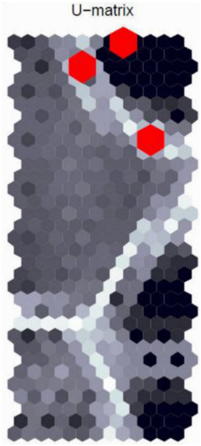


Figure 13. The SOM applied to network state monitoring. Three red polygons illustrate samples of the undesired security state.

5.3.2 Cyber Threat Management in Cognitive Networks

Both rapidly evolving cyber threats and the adaptive and self-acting behaviour of the cognitive military network requires new approaches to build a cyber threat management. Risk management and security mechanisms of the network must adapt to cyber threats and dynamically provide a coordinated response preferably in real-time. Threat management is able to build inside the cognitive process as the framework of Figure 14 illustrates.

The proposed threat management framework consists of three layers which are the network, cluster and node layers. The structure is based on the fact that optimizing of the cognitive network is provided at three levels; a single node, a cluster of nodes, and the entire network.

The framework includes two main functionalities in each network node: the threat management process as a part of the cognitive process and the database element. The threat management process is based on the assessment process introduced by Shore et al [94], and it consists of threat identification, risk assessment and mitigation trade-off sub processes. The threat identification element receives information from security data sources and databases, and then calculates and enumerates the threats and sets out intrusion/attack scenarios, and identifies the relevant vulnerabilities.

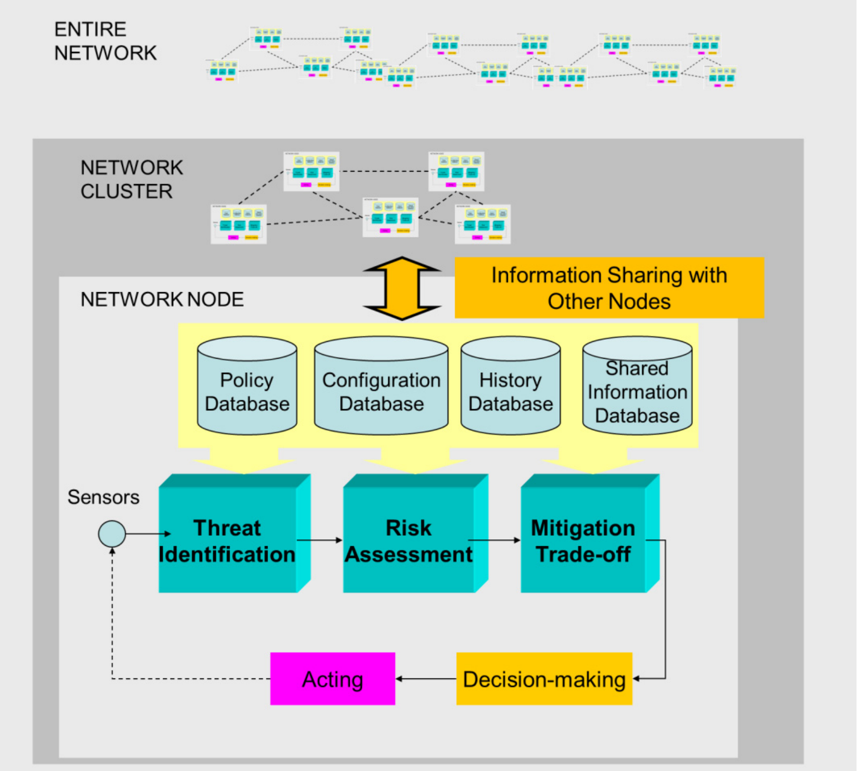


Figure 14. Overview of the framework.

The risk assessment sub process quantifies the risk for each intrusion scenario through the use of event history databases, and policies and mitigation strategies. Quantifying the risk can be done using historical data or statistical sampling. The cyber event or incident may not always result in the same consequences. A number of consequences with differing probabilities (e.g. an attack on a network may result in a temporary outage of one workstation at one extreme, and a complete extended loss of the network at the other) may exist. The expected loss from this event is then the sum of the products of the consequences multiplied by their probabilities. [27]

At the final stage the mitigation trade-off sub process calculates the trade-off cost of mitigation against the risks. The process provides an adaptation map in which different responses to an incident are shown in a sense of costs. The costs of mitigation include such attributes as service availability, connectivity, security levels, etc.

The database element includes four main data storages. The policy database maintains the current security policies that need to be applied at each layer. The configuration database contains all configuration files to keep the network nodes running. Previous data is vital to create cyber threat scenarios during the learning process, and thus it saved in the history database. To keep the database element updated, continuous information sharing between the network nodes is required.

The basis of threat identification is a clear situational awareness of cognitive network's current state. The network should recognize all vulnerabilities in configurations and software. Also, threat libraries must be up-to-date, so that all known attach graphs are recognized. Each network node maintains a detailed list of all relevant threats including each possible intrusion/attack scenario and vulnerability which may be exploited during the current operation.

Several methods exist to calculate the risk level, but the common understanding is that a risk consists of probability of a certain event and consequences caused by the event. Jiaxi [43] presents an integrated risk assessment method that is an integrative method to assess the cyber threat risk of any organization and thus it could be applied to cognitive networks.

The integrated cyber vulnerability assessment can be calculated by applying the following formula:

$$I_{ir} = W_{cai} \times M_s \times LV^T , \qquad (1)$$

where I_{ir} is the vulnerability index, and LV is the security risk vector. M_s is the cyber security risk matrix and $W_{cai} = [w_r \;\; w_a \;\; w_l]$ is a vector, whose value indicates the weight of cyber security risk, damage risk and the damage influence.

According to the method, the level of security risk is divided into five categories, and each category is assigned a value to indicate the relevant risk producing the security risk vector *LV*. The first row of the cyber security risk matrix M_s includes the percentage values of the cyber system risk belonging to each category. The second row consists of the probabilistic factors of incidents introduced by cyber events. The third row contains the influence factors of the incidents in cyberspace. The explanation of the variables and an example of using the formula are presented in Publication 5. It should be noted that the used values are selected arbitrarily for the purpose of testing the proposed method. Real values are subject to further research.

Mitigation of an incident typically causes some trade-off between service availability and the risk level of the network. A network system is a complex combination of hardware and software, and thus it is challenging to build the system without any vulnerability. The mitigation of an incident may need service break-outs or QoS level updates. In some case, a threat is approved to appear if its probability is relatively small and consequences are estimated to be limited.

Policy is a formal statement of operational requirements laid out in a formalized way [94]. In cognitive networking, reliability and survivability requirements create a demand for three security policy domains: the network, the cluster, and the node. The Network policy sets critical network infrastructure obligations which then will drive the policy in the cluster domain. The cluster security policy sets requirements to each node in which the node policy is created.

Information sharing plays an important role for threat management. Data of knowledge bases and threat libraries must be shared in real-time among all the nodes. This requires communication channels are reliable and include capacity enough.

5.3.3 Cognitive Service Configuration

The idea behind cognitive service configuration is to build networks and information services to appear as a moving target for an attacker. In that way, cyber attacks are not defended by placing packet filters or other intrusion prevention systems on the edge of the information system, but the consequences of the attacks are avoided by using a dynamic system configuration that is able to adjust its current configuration by using a cognitive process.

Figure 15 depicts the functional architecture of the cognitive information service configuration that consists of three layers that are the target layer, cognitive layer and reconfiguration layer. The architecture is based on one presented in Figure 9. The target layer is guided by security policies, security situation awareness (vulnerability libraries) and service level agreements. A service level agreement (SLA) [36] defines minimum requirements for information services. SLAs level agreements can contain numerous service performance metrics with corresponding service level objectives.

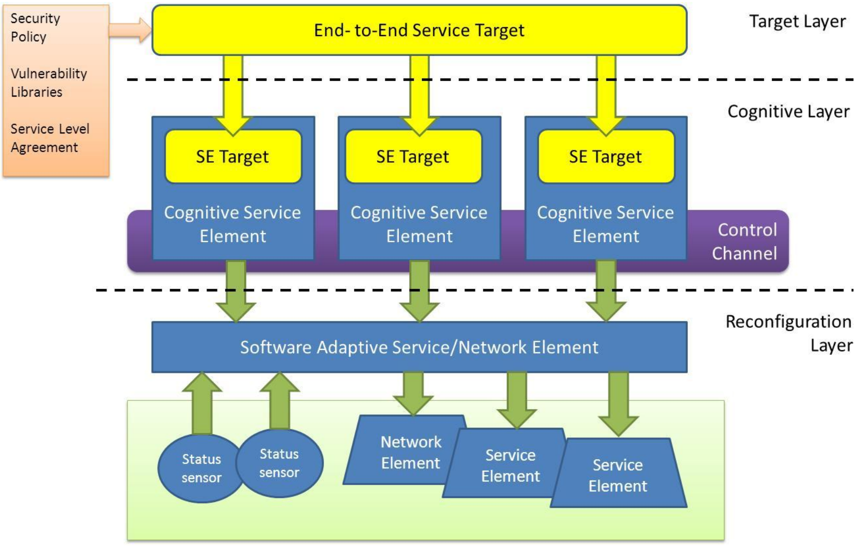


Figure 15. The overview of the cognitive information service structure.

The purpose of the target layer is to define an end-to-end service target for each information service. A service goal can be, for example, an availability level or sub services available for dedicated users. The goal is fed to the cognitive layer as a set of individual goals (service element targets) for each cognitive service elements. The main task of the cognitive service element is to decide how network and server parameters are reconfigured in network and service elements at the reconfiguration layer.

Each cognitive service element uses the previously defined cognitive process to make a decision for adaptation. The optimization of decisions is processed at several levels depending on the service structure. The optimization may occur at the service element level, server level or entire service system level.

The software adaptive service and network element is required for adjusting service configuration and networking parameters. The cognitive behavior needs software-adaptable hardware and devices. The element transforms the higher level decisions to actual configuration orders at the configuration level. A configuration order may include e.g. new IP addresses, or a change of transport protocol. Table 4 lists some reconfigurable protocols or attributes.

The status sensors monitor current situation. Sensor information is used for decision-making, and the sensor information may launch a new adaptation phase. The adaptation phase is also initialized when the end-to-end target is changed according to vulnerabilities, policies or service level modifications.

Table 4. Reconfigurable protocols or attributes by the cognitive process.

Protocol/attribute	Alternatives/options
Application protocol	HTTP, HTTPS, FTP,
Transport protocol	TCP, UDP, others
IP address	Changing IP addresses
Port number	Changing standard ports, changing port numbers randomly
Encryption key	Key lengths
Encryption algorithm	AES, DES, Blowfish
Firewall filters	Blocking certain sources and destinations, dropping desired protocols

Publication 6 presents an example which demonstrates how cognitive service reconfiguring protects against distributed denial-of-service (DDoS) attacks. In the DDoS attack, an attacker controls a few handler computers that use a large number of agents to generate flooding traffic to the target system. During the attack, the target server reconfigures system parameters so that the DDoS attack has no effect. The cognitive process tunes system parameters and adjusts filter settings so that the incoming packets from illegitimate origins are blocked out.

5.4 Cyber Security Architecture Based on Cognitive Networking

The previously presented conceptual applications utilize the cognitive features to solve a sub problem of network cyber security. To fully support the cognitive capabilities of the coherent phase, a holistic architectural approach is required. This section presents a cognitive network-based network cyber security architecture for tactical military communications (P7).

Existing cyber security or enterprise architectures do not include or take into account the cognitive features when addressing security controls design in a communications network [96]. Thus, the proposed security architecture that is presented in the following paragraphs, is not based on any existing security architecture frameworks, but it rather complies with the layer structure of the ITU-T X.805 recommendation [90].

5.4.1 Overview of the Proposed Cyber Security Architecture

The overview of the cognitive network-based cyber security architecture for the military networks is presented in Figure 16. The architectural design is based on a block diagram that describes functional element at five functional layers. The functional layers of the architecture are the Security Policy and Management Layer, Cognitive Layer, Application Security Layer, Service Security Layer, and Infrastructure Security Layer.

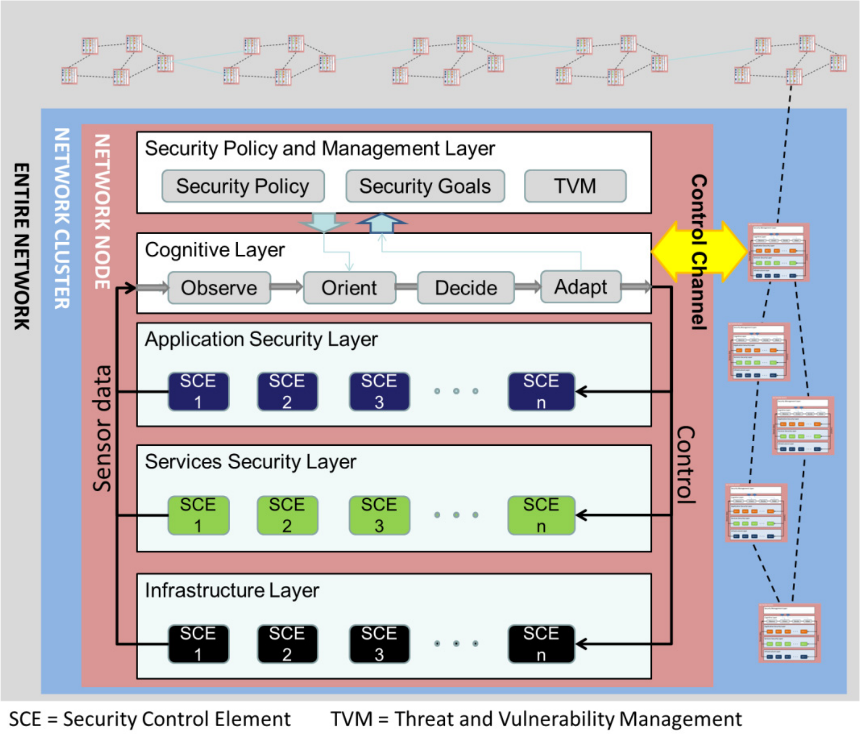


Figure 16. Overview of the cyber security architecture.

The layers appear in each network node throughout the entire network. At the top, cyber security policy and end-to-end goals are set and executed by the Security Policy and Management Layer that controls the Cognitive Layer. The top layer also includes the Threat and Vulnerability Management (TVM) element that provides threat and vulnerability information for the Cognitive Layer.

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 is based on the previously introduced OODA loop presented in Figure 8. The layer is connected to the Application Security Layer, Service Security Layer, and Infrastructure Security Layer by two manners. 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 are designed at three separated layers in accordance with the ITU-T X.805 recommendation [90]. The Infrastructure Security Layer includes the security controls of network transmission facilities, and individual networking elements. The infrastructure layer represents the most critical part when building blocks of networks, services and applications [90]. The Services Security Layer concerns security of services a network provides to the end-users. The 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.). The Applications Security Layer focuses on security of the network-based applications accessed by end-users. The applications are supported by network services and infrastructure. In the military networking context, the applications include basic Command and Control (C2) applications, file transport/storage applications, voice messaging and email, video collaboration, etc.

5.4.2 Infrastructure Security Layer

The Infrastructure Security Layer architecture describes the security controls to protect data transition, communication links, and their supporting control capabilities such as routing, and network access. Network elements at the layer include individual routers, switches, servers, and the communication links, wireless or fixed, between them.

In a context of tactical networking, the Infrastructure Security Layer consists of deployable network nodes that provide both networking and information service capabilities to war fighters. The layer protects user data packets while transported through the network nodes, as well as, being transported across wireless and fixed communication links. Securing the infrastructure layer also includes the protection of the control information (e.g. routing information) when it is processed or shared.

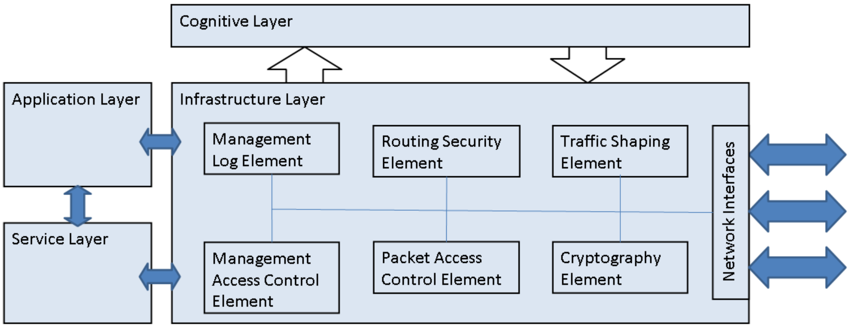


Figure 17. Infrastructure Security Layer.

Figure 17 presents the architecture of the Infrastructure Security Layer consisting of six separated security elements. The infrastructure layer is connected to the other layers as depicted in the overall architecture (see Figure 16). The features of each element are described in more detail in Publication 7.

5.4.3 Services Security Layer

Network services are often built-upon one and another causing a challenge when implementing security controls at the Service Security Layer. For example, in order to provide a secure email service, the network has to provide a simple IP service that relies on enabling services such as DHCP, DNS, and authentication [90]. Also, cryptography and QoS services must be provided to meet end-user's quality and security requirements for the service.

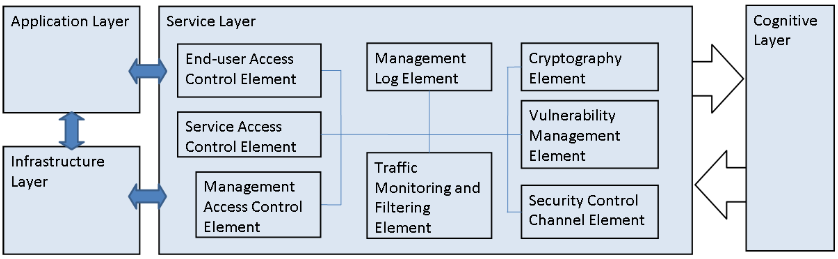

Application Layer
Infrastructure Layer
Service Layer
End-user Access Control Element
Service Access Control Element
Management Access Control Element
Management Log Element
Traffic Monitoring and Filtering Element
Cryptography Element
Vulnerability Management Element
Security Control Channel Element
Cognitive Layer

Figure 18. Services Security Layer.

The Services Security Layer includes the security controls that protect data used and processed by network services. Figure 18 presents the architecture of the Service Security Layer with six security elements. The layer has input and output connections to the cognitive layer so that the layer is able to control the security elements, and to collect status data. The features of the security elements are described in more detail in Publication 7.

5.4.4 Application Security Layer

Protection at the applications layer focuses on securing data generated by end-user applications that are locally installed or network-based (server-client solutions). In the military networking environment, the applications have high requirements for processing, sharing and storing classified information to ensure operational security. Securing the applications layer also includes the protection of the control or signaling information used by the network-based applications.

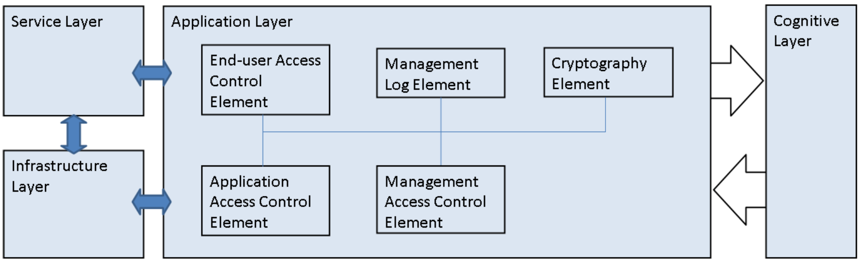


Figure 19. Application Security Layer.

Figure 19 presents the architecture of the Service Security Layer. The Cryptography Element, Management Log Element and Management Access Control Element provide the same functionalities as those at the infrastructure layer (see Figure 16). The properties of the security elements are described in more detail in Publication 7.

5.4.5 Other Layers

The cognitive layer implements the cognitive process. The layer receives status information from all the security elements in the system. Simultaneously, the cognitive layer controls the security elements according to the decisions made during the cognitive process. The cognitive layer obtains the end-to-end security goals from the Security Policy and Management Layer.

The cognitive layer is distributed over the entire network through a control channel. Reliable information sharing is critical when parameters are optimized over the network. For optimizing and decision-making, several algorithms have been developed [60]. In a sense of parameter optimizing, the network is divided into three zones. The first zone includes a single node, and it requires no control channel as the optimization is completed locally. The second optimizing zone consists of several nodes that form a sub network with specific end-to-end goals. The third optimizing area includes all the nodes, and optimizing is performed within the entire network.

The Security Policy and Management Layer enforces the security policy through an automated process without any manual enforcement creating fewer possibilities that the policy is not followed. Typically, the security policy includes access control, configuration rules and processing of classified information. The main task of the security goal management is to define the end-to-end security goals for the network performance. The security goals include for example approved encryption algorithms, key lengths, access protocols and controls, overall security controls in each node, etc. The Threat and Vulnerability Management (TVM) element maintains a threat assessment, and through the layer the network is able to adjust its parameters to defend against current threats. The element also provides threat and vulnerability information for the risk assessment implemented at the cognitive layer.

5.4.6 Architecture Evaluation

An assumption is that designing a network architecture with security functions will produce more secure architectural design and eventually more secure networks. However, it is still imprecise how to seamlessly evaluate a security architecture. 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) [86]. Evaluation of architectures is important, and in the case of cyber security it is even critical. In the next sections, we discuss evaluation methods and provide an evaluation of the proposed architecture.

Evaluating Security Architectures

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, every security assessment has to face this challenge. A chance remains that a network system includes a vulnerability although all components have been checked. Thus, it is difficult to develop a security evaluation method that provides reliable and exact feedback about the network system [70].

Many methods for evaluating and assigning assurance levels to information and communications systems have been developed. The well-known security evaluation criteria such as TCSEC [107], ITSEC [40] and Common Criteria (CC) [15] were developed to evaluate computer security within products and systems, and to provide an international standard for computer security certification. The purpose of the evaluation criteria is to establish a trust between the customer and the product vendor [70]. Some criticisms against these evaluation criteria have shown up [47]. 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 certificate 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.

In addition to the evaluation criteria, several network security evaluation methods are presented [1, 62, 69, 75]. However, these models concentrate on a specific sub functions without evaluating overarching security architecture. The models include the performance evaluation of security architecture for wireless local area networks [75], and the evaluation of a Massively Parallel Architecture [62] for network security applications such as malware detection, security breaches, and covert channels. The existing network security evaluation methods also include the model-based security evaluation of in-vehicle network architectures [69] and the novel quantitative approach for measuring network security [1] that presents a model to calculate the risk level of a network system by using vulnerability history data.

Although, network security architecture evaluation lacks of appropriate evaluation methods, software architecture assessment models may be applied to the network development. J. Bosch introduces four types of software architectural assessment; mathematical modelling, simulation-based, scenario-based and experience-based assessment [5]. From these, mathematical modelling and simulation-based method are challenging as they require exact performance parameters that do not exist before code is written. The experience-based assessment is more subjective than the others. From these assessment methods, the scenario-based evaluation seems to be the most promising, and it was used for the evaluation of the proposed cyber security architecture.

Evaluation of the proposed security architecture

Although the scenario-based evaluation framework is not originally developed for network security architecture, it is a promising approach to evaluate a high-level network security architecture [3]. The evaluation process includes a scenario-based architecture review. Using scenarios is maturing process and has proven to be a successful practice [14]. The framework includes six phases that are presented in more detail in Publication 7.

An important phase of the process is to create security scenarios. A coherent and logical security scenario is a key for the relevant evaluation results. To generate a reasonable scenario, threat modelling and security requirements must be considered closely. Threats can be well defined and classified using several threat models [98]. In the evaluation phase, the selected security profile is analyzed using a risk-based approach. The process of associating risk values with each scenario in the profile is described using the standard risk model [78]. The risk R_i of each scenario i is calculated by:

$$R_i = L_i * I_i \,, \qquad (2)$$

where L_i is the likelihood and I_i is the impact of the scenario i. The OWASP Risk Rating Methodology [78] uses the simple numerical values (0 - 9) for likelihood and impact to simplify the analysis process. The overall risk severity level is achieved as a combination of the levels of impact and likelihood (see Publication 7). 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 using the severity levels in the scenario-based evaluation [50]. The likelihood of the scenario i is calculated by:

$$L_i = VF_i * LR_i \,, \qquad (3)$$

where VF_i is the average of the vulnerability factors for each scenario. LR_i is the lack of security element resistance that is achieved by:

$$LR_i = 1 - Min(\alpha_j) \,. \qquad (4)$$

Each security element has the improvement effect α_j (from 0 to 1) that increases security resistance. If multiple elements are applied to a single scenario, the smallest improvement effect α_j is chosen. The overall impact I_i is achieved as the average of the impacts I on corresponding security objectives for each threat scenario. For evaluating the proposed architecture, four most-likely threat scenarios for tactical military networking were described, and the vulnerability and impact factors based on the OWASP Risk Rating Methodology [78] were defined (see Publication 7).

The evaluation results are presented in Table 5. The security controls applied to each scenario are chosen from the presented architecture layers (see Fig. 17 - 19). The improvement effect α_j is estimated for each security element. For the first threat scenario, the mitigating security elements are the Node Access Control Element (NACE), Application Access Control Element (AACE) and Service Access Control Element (SACE) that has the improvement value of 0.75 as they partly protect against unauthorized access.

Table 5. Evaluation results.

#	Threat Scenario	Security Element (*α*)	Impact Factors				Vulnerab. Factors				Risk Level
			LC	LI	LA	LAC	ED	EE	AW	ID	
1	Unauthorized access by node capture	NACE (0.75), AACE (0.75), SACE (0.75)	9	1	1	9	3	3	9	1	**Low** *I*=5, *V*=1
2	Eavesdropping of wireless links	CE(1.0), TSE (1.0)	9	1	1	9	3	9	9	9	**Low** *I*=5, *V*=0
3	Denial-of-Service	RSE (0.75), PACE (0.5), TMFE (1.0), VME (0.5)	2	1	9	7	3	3	6	1	**Low** *I*=4.75, *V*=1,6
4	Violation of network operations	RSE (0.25), MACE (0.75)	2	7	7	7	3	1	1	1	**Low** *I*=5.75, *V*=1,1

As the attacker has the physical access, software-based access controls do not prevent from entering to a hard disk or other databases. The Loss of Confidentiality (LC) and Loss of Accountability (LAC) are high (9) in a node capture, while the Loss of Integrity (LI) and Loss of Availability (LA) are low (1) as services are distributed and the captured node automatically released from the networking system. Ease of discovery (ED) and Ease of exploit (EE) are difficult (3) but still possible as the attacker is well aware of capturing opportunities (Awareness, AW=9). In the cognitive system, an indication of capture is provided actively (Intrusion detection, ID=1).

In Scenario 2, the protecting elements are Cryptography Element (CE) and Traffic Shaping Element (TSE). If the encryption algorithms used in communications are strong enough as expected, the improvement effect is 1.0. Similarly, it is expected that TSE provides 100% traffic flow confidentiality. The impact factors are equal to Scenario 1 as critical data is lost by eavesdropping. ED is difficult (3) but once a link is discovered recording traffic is quite trivial (EE=9). Eavesdropping is well known (AW=9) and it is almost impossible to detect (ID=9).

The security elements concerning Scenario 3 are Routing Security Element (RSE), Packet Access Control Element (PACE), Traffic Monitoring and Filtering Element (TMFE) and Vulnerability Management Element (VME). The improvement effect of RSE is estimated to 0.75 as routing management may prevent lots of DoS attacks. PACE may drop lots of DoS packets but when the attacker hides DoS commands in a payload, PACE is unable to discover it. In theory, TMFE should detect all DoS attempts (α=1.0) as it is able to form complete situational awareness. VME shares information about potential DoS attack vectors which helps protecting against DoS attacks (α=0.5). The impact factors LC and LI are low while LA is very high (LA=9). Tracing the attacker is challenging but possible (LAC=7). ED and EE are difficult (3) as the mission critical network is hard to access and includes specific protocols. Vulnerabilities for DoS attacks are obviously known (AW=6), but not public in mission critical communications systems.

In Scenario 4, threat protection is achieved by RSE and Management Access Control Element (MACE). RSE concerns routing violations, but most of the violation is conducted at the cognitive layer (α=0.25). MACE prevents most of the hostile accesses to the network management including the cognitive process (α=0.75). The impact factor LC is low (2) as data theft is not a goal. On the other hand, LI, LA and LAC are quite high (7) due to the effects on networking capabilities and trust. The vulnerability is difficult to find (ED=3). The other factors EE, AW and ID are very low (1) as the vulnerabilities at the cognitive and management layers are unknown, and the attacks are detected actively due to complete situational awareness.

The numerical values of the likelihood and impact factors are calculated using Equations 1 - 3, and finally converted to the likelihood and impact levels (low 0 ≤ 3, medium 3 ≤ 6 and high 6 – 9), and the final risk value is obtained by using the risk severity levels (see Publication 7). The results show that the security elements of the architecture decreased the risk level to low in all the scenarios. The result indicates that improvements are still to be designed to achieve the lowest risk level for each scenario.

5.5 Summary

As the NEC roadmap states, the networking in the coherent phase is based on CN. The cognitive approach and behavior could be used to improve cyber security from many perspectives as the proposed approaches for SA, dynamic configuration and threat management demonstrate. However, the greatest benefit is obtained when the whole cyber security architecture is designed above a cognitive layer.

The cognitive-network based architecture provides many advantages such as auto-configuration, network parameter optimization and adaptation. The cognitive layer controls all networking layers by collecting status data, and providing control data to the security control elements. The cognitive-network based system adapts to new cyber threats rapidly and automatically without manual configuration.

However, implementing the architecture is challenging and requires more research. The modern information systems and networks are layered and contain a lot of software. The cognitive layer increases this complexity which inevitably opens new attack surfaces. Cognitive processing may not sense all the errors of the decision-making chain.

Evaluating the architecture is important, but difficult. Unless the architecture functions are not implemented or simulated, it is very challenging to verify how cyber security requirements are fulfilled. The scenario based method used in this thesis gives only rough estimation, and lots of future work must be conducted to achieve precise results.

6. Discussion and Conclusions

The main objective of this thesis was to develop cyber security architectures for future military networks. Instead of developing and presenting a single novel architecture, the thesis focuses on the challenge how the cyber security architecture for tactical military networking must be developed during the network evolution. The thesis presents a several architectural models that could be used in different phases of the NEC roadmap. In this chapter, we discuss on the relevance of developing military cyber security architecture and the challenges of implementing the presented architectures.

6.1 Relevance of Developing Cyber Security Architectures

Developing military capabilities is a long, demanding process. It requires a long term planning and procurement. Military technologies have a long life cycles as the budgets are not enough to replace all systems and technologies in a short period. Thus, the current military capability is a mixture of old and modern systems. To overcome these challenges e.g. European Union recommends several solutions. These includes a reduction of redundant and obsolete capabilities, favouring optimization, promoting innovations and integration [65].

An architecture framework is an efficient tool to enable the management of the nation's investments in technologies, programs, and product support necessary to achieve the national strategy and support employment and maintenance of the armed forces [100]. An architecture is a basis for the development of integrated plans or roadmaps that are used to conduct capability assessments, guide systems development, and define the associated investment plans as the basis for aligning resources and as an input to the defence planning [100].

A security architecture plays an important role as it concentrates on how to secure information sharing and processing in a network infrastructure. The security architecture must be developed in line with the overall enterprise or CIS architecture to fit security controls and capabilities to current and future ICT technologies used in military communications systems. The objective of a network security architecture is to reduce network complexity, minimize the network attack surface and standardize network security. By reducing and centralizing the number of security stacks, the architecture improves network performance and creates efficiencies. [108]

The NNEC and FMN development roadmaps also set requirements for security. The security architecture development have to follow the overall roadmap to provide efficient, cost-effective and viable security controls, protocols and processes for future networking. In the short and mid-term development, security enhancements include interoperability and common solution issues while the long term development requires totally new approaches such as cognitive-based security architectures.

In developing the security architecture, it is essential to determine what problems an organization is trying to solve. Some common areas addressed by the security architecture include resources (to be protected), threats, the likelihood of each problem (threat), and architecture review and updating [46]. A challenge is to maintain the architecture updated reflecting the current state of security threats to the network. The high-level network cyber security architecture should be designed to support the evolution of threat environment and future technologies, and the development of the operational requirements for a mission.

The security architectures are useful only if they could be implemented into actual operational networks to provide better protection against emerging cyber threats. However, there may appear many perceived architectural conflicts between security and other architectural goals. These other architectural goals must be separated into those that are complementary to the needs of secure design, and to those that are independent of secure design; and those that are at times at odds with the goals of secure architecture design. [85]

Building and implementing security in networking systems is a demanding work. A dilemma is that the more we add new security features into the system the more complex the networking systems become. And the management of vulnerabilities becomes more challenging requiring increasing amount of resources to collect, and analyze vulnerability information. Therefore, rigorous network cyber security changes to risk management as complete information of system state is impossible to collect in real-time.

6.2 Implementation of Network Cyber Security Architectures

The components, protocols and functions described in the security architectures must be feasible to implement. Feasibility means cost-effectiveness, technological maturity, complexity management, and options to integrate new features into the legacy systems. In the following, the feasibility of the architectures is considered from technology maturity and complexity point of view.

Implementing the multilevel security framework requires more research. However, the functionality of CBIS and PCN has already been demonstrated, but complete implementations are still far ahead. Some products to support the traditional approach to MLS are available [81]. A challenge with CBIS is to build lightweight key management for tactical use.

Delay-tolerant networking requires dynamic trust management as network connectivity is unstable, but implementations providing these functionality are not produced yet. Also, dynamic key management system is required. Some key management prototypes are already developed and tested [112] to support low-bandwidth, high-latency networks. Capabilities include, e.g. no handshakes prior to communication, both unicast and multicast security, join and leave features, and over-the-air rekeying. For overall privacy protection and delay-tolerant capabilities, cooperation between system layers is required [109]. A challenge is to build this cross-layer functionality.

Implementation of threat management features requires automated threat identification that is a challenging process. The system should have a clear list of all threat types and possible vulnerabilities. At the same time, attackers are looking for new attack scenarios and graphs. It is challenging to implement cognitive threat management features that automatically recognize new threat types and vulnerabilities.

To keep services available for legitimate users, a control channel is required in the cognitive service production. The control channel provides a new attack surface for an attacker. Control channel attacks may paralyze the entire information system leaving the user without any service. The control channel adds traffic between the client and the server, and it requires high- level security protocols that also consume the limited bandwidth of the tactical networks. A challenge is also how end-to-end targets are formulated so that lower level elements are able to make the most optimal decisions. It could be difficult to formalize vulnerability information into an understandable format. This could be provided by using standardized format although a risk is that some information is lost.

One of the major challenges with cognitive networking is decision-making process and learning functionality. It is possible to teach computers to act in a certain way in a limited scenario, but the problem is how the system learns in the situation where no data in prior exists. The complexity of a large cognitive system increases enormously. Every single security element is software-controlled which causes a lot of new software code to be run. Managing software defined security elements requires another software-based management layer at each network node. A complex, software defined system requires a lot of computational capacity. That consumes electric power and requires powerful microprocessors. The nodes are connected to each other through links that include separated control channels to build a solid, network-scale management plane. Even though the CN provides automated and dynamic management for network operators, and thus simplifies an operator's configuration environment; the practical implementation may appear complex and unreliable.

Ensuring security of information sharing between cognitive nodes is vital for network optimization. For optimal functioning the nodes of cognitive network must exchange a huge amount of control information. The corruption of 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, cognitive networking no more exists.

The new architectural design with a cognitive process and software controlled security controls may create emerging and unknown cybersecurity threats. Security challenges of the cognitive process are researched and discussed in several sources [7, 11, 13]. Cognitive networks face some unique security threats not appearing in conventional wireless or wired networks. The cognitive process itself may appear vulnerable. For instance, incomplete situation awareness or a disturbed decision-making process may lead to the decision not to use any security controls. An attacker is able to change the information environment by violating sensor data, information sharing and history data (databases). 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. In addition to the above-mentioned threats, some unknown threats will always exist, and thus it is important to research vulnerabilities of cognitive systems all the time.

6.3 Conclusions

The main message of this research is to describe how cyber security architectures for tactical military networking should be designed in line with the general development of military networking capabilities and architectures. The main purpose was to develop cyber security architectures for the phases of the network enabled capability roadmap. The development of the network enabled capabilities for networking and information infrastructure also requires that the security architecture is designed to meet the security goals of each phase.

Cyberspace, cyber warfare and cyber threats 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.

As concluded in Chapter 3, the tactical networking environment is difficult for networking. The networks should be mobile, reliable and secure at the same time. Network Centric Warfare (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.

Developing cyber security capabilities is part of the NEC development. The security architectures must align with the phases of the NEC and FMN roadmaps that set the technological and functional architectures for military networking and information services. The cyber security architectures support the requirements described for the secure networking and information infrastructure. The short and mid-term development aims to coordination and collaboration. The security architectures provide common security solutions and multilevel security capabilities. The long term development requires totally new approaches as the networking infrastructure will be based on new paradigms such as cognitive networking.

Cognitive networks is a promising approach to improve capabilities in military tactical networks. In theory, the cognitive networks bring many advantages that enhance network performance and especially cyber security in the battlefield conditions. The cognitive network is based on a cognitive process that has the ability to observe, orient, decide and execute these decisions within the network parameters. Cognitive networking will provide smart functionality for future communication networks. Automated cognitive processes ensure better capacity allocation, less human configuring and management and more security features. But while the human control over the networks decreases, cyber threats are going to even more complicated.

The cognitive network-based cyber security architecture provides a new architectural design as it uses the cognitive process to manage network security. All the functions are controlled by the cognitive layer according to collected information from internal and external sources. The cognitive behaviour enables enhanced threat management and automated, dynamic maintenance of security. The main challenges of implementation are increased complexity and decision making process to provide the most optimal decision in the complex networking environment. New processes such as cognitive decision-making and information sharing make software and hardware more sophisticated. Extra communication channels and data processes set up new vulnerability points. An attacker may use these channels and processes to disturb and prevent normal processing.

The main results of this thesis can be summarized as follows:

- Cyber security must be considered in a long term military capability development to ensure cost-effectiveness, overall security of networking and interoperability with legacy solutions.
- The phases of the NEC development require different types of architectural approaches for cyber security. In the long term, the coherent phase requires a novel approach as networking will be based on the cognitive networks.
- In the short and mid-term development, the architecture for privacy protection, delay-tolerant networking, and multilevel security provide part of the solution for developing cyber security. However, the implementation of the architectures requires more research and development.
- In the long term capability development, emerging cyber threats and future networking technologies require novel approaches to build secure military networking systems. Cognitive networking requires cognitive security management and control.
- The thesis presents the novel cognitive network-based cyber security architecture that provides an overall security architecture to build automated, self-configurable security management and control for future tactical military communications.

- The capabilities of the cognitive network-based cyber security architecture ensure improved cyber threat management, and situational awareness. Cognitive behavior enables dynamic service configuration to protect services against cyber attacks.
- The implementation of the presented architecture requires more research to development protocols, cross-layer functions and management features. The evaluation of a security architecture is a challenging task, and it requires simulations and practical implementations to measure the features designed in the architecture. The evaluation results are only indicative.

There are several areas that could be researched further. These include the protocols of security controls and management, the performance of the cognitive layer, and the evaluation of the architectures.

The security protocols should be light-weight and support distributed architecture. Resources in the tactical environment are limited which means that the protocols must provide minimum overhead to communication links. The protocols themselves should be secure and reliable.

The cognitive layer and the algorithms for decision-making and parameter optimizing need to be researched. Again, the solutions must be suitable for tactical communications in which networking and computational resources are scarce, and all the security functions must be implemented without a single point of failure.

An important field of the future research concerns architecture evaluation. Through evaluation an architectural designer is able to find weaknesses in the security design. However, the current evaluation methods and criteria are not designed for the architecture level evaluation, and they typically require a real product for evaluation. Thus, developing new evaluation methods is beneficial.

References

[1] Ahmed M. S., Al-Shaer E. and Khan L., A novel quantitative approach for measuring network security, In Proceedings of *the 27th IEEE Conference on Computer Communications (INFOCOM)*, IEEE, 2008.

[2] 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.

[3] Alkussayer A. and Allen W. H., A scenario-based framework for the security evaluation of software architecture, In Proceedings of *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT),* IEEE, 2010, pp. 687 - 695.

[4] Bacao F., Lobo V. and Painho M., Clustering census data: comparing the performance of self-organising maps and k-means algorithms, In Proceedings of *KDNet Symposium on Knowledge-Based Services for the Public Sector*, Bonn, Germany, 2004.

[5] Bosch J., *Design and Use of Software Architectures: Adopting and Evolving a Product-line Approach*, Addison-Wesley, 2000.

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

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

[8] Candolin C. and Kiviharju M., A roadmap towards content based information security, *The 6th European Conference on Information Warfare (ECIW)*, ACPI, 2007.

[9] Candolin C., *Securing military decision making in a network-centric environment*, Doctoral Dissertation, Helsinki University of Technology, 2005.

[10] Cerf V. et al., *RFC 4838: Delay-Tolerant Networking Architecture*, Network Working Group, Internet Research Task Force, 2007.

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

[12] Ciampa M., *Security+ Guide to Network Security Fundamentals*, Cengage Learning, 2011.

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

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

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

[16] Crawley E., de Weck O., Eppinger S., Magee C., Moses J., Seering W.,Schindall J., Wallace D. and Whitney D., The Influence of Architecture in Engineering Sys-

tems, *Engineering Systems Monograph*, The ESD Architecture, Massachusetts Institute of Technology, 2004.

[17] *Defense Management: DOD Needs Better Information and Guidance to More Effectively Manage and Reduce Operating and Support Costs of Major Weapon Systems*, Report to Congressional Committee, United States Government Accountability Office, July 2010.

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

[19] *Deployed Tactical Network Guidance: Appendix D to Guidance for 'End State' Army Enterprise Network Architecture*, Chief Information Office (CIO), United States Army, Version 1.0, May 2012.

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

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

[22] Dwork C., Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener (editors) *Automata, Languages and Programming*, volume 4052 of Lecture Notes in Computer Science, Springer Berlin/Heidelberg, 2006, pp. 1–12.

[23] Fall K., A Delay-Tolerant Network Architecture for Challenged Internets, In Proceedings of *the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03)*, ACM, 2003, pp. 27-34.

[24] Fasbender A., Kesdogan D. and Kubitz O., Analysis of Security and Privacy in Mobile IP, In Proceedings of *the 4th International Conference on Telecommunication Systems, Modeling, and Analysis*, CFP, 1996.

[25] Fette B. A., *Cognitive Radio Technology*, Academic Press, 2009.

[26] *Finland's Cyber security Strategy*, Government Resolution, Secretariat of the Security Committee, 24.1.2013. ISBN: 978-951-25-2438-9.

[27] Frank M. V., *Choosing Safety: A Guide to Using Probabilistic Risk Assessment and Decision Analysis in Complex*, *High-Consequence Systems*, Routledge, 2010.

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

[29] Garnier J., Bischoff L., André M., Lavit B., Peyrichon M., Blanquart J. and Scuto N., Architecture Frameworks– A standard to Unify Terms, Concepts, Life-Cycles and Principles. In Proceedings of *NATO STO-MP-IST-115*, May 2013, pp.1–20.

[30] Glowacka J. and Amanowicz M., Application of Dezert-Smarandache theory for tactical MANET security enhancement, In Proceedings of *Communications and Information Systems Conference (MCC)*, 2012 , pp. 1 – 6.

[31] Glowacka J., Parobczak K. and Amanowicz M., On mechanism supporting situational awareness of a tactical ad-hoc network node, In Proceedings of *Military Communications and Information Systems Conference (MCC)*, 2013, pp. 1 – 8.

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

[33] Hallingstad G. and Dandurand L., *CIS Security (Including Cyber Defense) Capability Breakdown*, NATO Consultation, Command and Control Agency Reference Document RD-3060, The Hague, Netherlands, November 2011 (NATO Unclassified).

[34] Hallingstad G. and Oudkerk S., Protected Core Networking: An Architectural Approach to Secure and Flexible Communications, *IEEE Communications Magazine*, Vol. 46, Issue 11, November 2008, pp. 35 – 41.

[35] Harnack J., Life cycle planning from product development to long term sustainment. In Proceedings of *IEEE AUTOTESTCON*, 2012 (pp. 29-33).

[36] Hiles, A.*, The Complete Guide to I.T. Service Level Agreements: Aligning It Services to Business Needs*, Rothstein Associates Inc, 2002.

[37] Hong W., Shaoqian L., Xiping Z., and Liang Z., A framework of the PHY-layer approach to defense against security threats in cognitive radio networks, *IEEE Network*, 2013, Vol 27, Issue 3., pp. 34 – 39.

[38] Huang R., Yan D. and Fangchun Y., Research of security metric architecture for Next Generation Network, In Proceedings of *IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC)*, IEEE, 2009,pp. 207 – 212.

[39] *Improving Web Application Security: Threats and Countermeasures*, Microsoft Corporation, Microsoft Press, 2011.

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

[41] Jacobs S., *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance*, IEEE Press Series on Information and Communication Networks Security, John Wiley & Sons, 2011.

[42] Jamshidi M., *Systems of Systems Engineering: Principles and Applications*, CRC Press, 2008.

[43] Jiaxi Y., Anjia M. and Zhizhong G., Vulnerability Assessment of Cyber Security in Power Industry, In Proceedings of *IEEE PES Power Systems Conference and Exposition (PSCE)*, IEEE, 2006, pp. 2200 - 2205.

[44] Jimenez-Molina A. and In-Young Ko, Cognitive Resource Aware Service Provisioning, In Proceedings of *the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2011, pp. 438 – 444.

[45] Johnson N., Duric Z. and Jajodia S., *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*, Springer Science & Business Media, 2012.

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

[47] 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.

[48] Keller J., Krisnapuram R. and Pal N. R., *Fuzzy Models and Algorithms for Pattern Recognition and Image Processing*, Springer Science & Business Media, 2005.

[49] Kiviharju M., *Cryptographic Key Management Architectures for Environments with Independent Subdomains*. Licentiate's thesis, Helsinki University of Technology, Finland, 2009.

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

[51] Kliazovich, D. et al, Cognitive Information Service: Basic Principles and Implementation of a Cognitive Inter-Node Protocol Optimization Scheme, In Proceedings of *the IEEE Global Telecommunications Conference*, 2009, pp. 1 - 6.

[52] Koch, R. and Rodosek G. D., The role of COTS products for high security systems, In Proceedings of *the 4th International Conference on Cyber Conflict (CYCON),* IEEE, 2012.

[53] Kohonen T*., The Self-Organizing Maps*, Springer-Verlag, 3rd Edition, Heidelberg, Berlin, 2001.

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

[55] Krafzig D., Banke K. and Slama D., *Enterprise SOA: Service-oriented Architecture Best Practices*, Prentice Hall Professional, 2005.

[56] Kumar D., Rai C.S. and Kumar S., An Experimental Comparison of Unsupervised Learning Techniques for Face Recognition, *International Journal of Computer, Control, Quantum and Information Engineering*, Vol 1, No 4, 2007.

[57] *LandWarNet 2020 and Beyond Enterprise Architecture*, CIO/G-6, United States Army, Version 1.0, 7 August 2013.

[58] Layton T. P., *Information Security: Design, Implementation, Measurement, and Compliance*, CRC Press, 2006.

[59] Li Zhu and Huaqing M., Unified Layered Security Architecture for Cognitive Radio Networks, In Proceedings of *Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, 2011, pp. 1 – 4.

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

[61] Marques H., Ribeiro J., Marques P., Zuquete A. and Rodriguez J., A security framework for cognitive radio IP based cooperative protocols, In Proceedings of *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2009, pp. 2838 – 2842.

[62] Mason B. C., Ghosal D. and Corbett C., Evaluation of a Massively Parallel Architecture for Network Security Applications, In Proceedings of *18th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, IEEE, 2010, pp. 85 - 91.

[63] McCabe J. D., *Network Analysis, Architecture, and Design*, The Morgan Kaufmann Series in Networking, Morgan Kaufmann, 2010.

[64] Mingoti S. A. and Lima J. O., Comparing SOM neural network with Fuzzy c-means, K-means and traditional hierarchical clustering algorithms, *European Journal of Operational Research*, 2006, 174.3, pp. 1742–1759.

[65] Missiroli A. (ed.), *Enabling the future European military capabilities 2013-2025: challenges and avenues*, Report n:o 16, , EU Institute for Security Studies, May 2013.

[66] *MOD Architecture Framework*, https://www.gov.uk/mod-architecture-framework. [cited 26.5.2015]

[67] Moffat J., and Alberts D. S., *Maturity Levels for NATO NEC Command*, TR21958 v 2.0, Defence Science & Technology Laboratory UK, Dec 2006.

[68] Molsa J., Karsikas J., Karkkainen A., Kettunen R. and Huttunen P., Field test results and use scenarios for a WiMAX based Finnish broadband tactical backbone network, *Military Communications Conference (MILCOM)*, IEEE, 2010, pp. 2014 - 2019.

[69] Muter M. and Freiling F. C., Model-Based Security Evaluation of Vehicular Networking Architectures, In Proceedings of *Ninth International Conference on Networks (ICN),* IEEE, 2010, pp. 185 - 193.

[70] Müter M., Model-Based Security Evaluation of Vehicular Networking Architectures, In Proceedings of *IEEE Ninth International Conference on Networks (ICN),* IEEE, 2010, pp. 185 - 193.

[71] *National Information Assurance (IA) Glossary*, Committee on National Security Systems (CNSS) Instructions No. 4009, 26 April 2010.

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

[73] *NATO Future Mission Network (FMN) Concept*, Version 2.0, 2012 (NATO Unclassified).

[74] *NATO Network Enabled Capability Feasibility Study: Executive Summary*, Version 2.0, Report, NATO Consultation, Command and Control Agency, October 2005 (NATO Unclassified). *[Online]: http://dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf*, Accessed 15.1.2015.

[75] Nayak D., Phatak D. B. and Gulati V. P., Performance evaluation of security architecture for wireless local area networks by indexed based policy method, In Proceedings of *IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication*, IEEE, 2005, pp. 37 - 40.

[76] Nikander P., Ylitalo J. and Wall J., Integrating Security, Mobility, and Multihoming in a HIP way, In Proceedings of *Network and Distributed Systems Security Symposium (NDSS'03)*, Internet Society, 2003, pp 87 - 99.

[77] *Open Security Architecture. [Online]: www.opensecurityarchitecture.org*, Accessed 20.8.2014].

[78] *OWASP Testing Guide*, The Open Web Application Security Project (OWASP) Foundation, Version 3.0, 2008.

[79] Palaganas R. F., Implementing NATO Network Enabled Capability: Implications for NATO Response Force's Envisioned Roles, *Information as Powers*, Volume 1, U.S. Army War College, January 2007.

[80] Paquet C., *Implementing Cisco IOS Network Security (IINS): Foundation Learning Guide*, 2nd Edition, Cisco Press 2012.

[81] Pfleeger C.P. and Pfleeger S.L., *Security in Computing*, Prentice Hall Professional, 2003.

[82] Premaratne U., Samarabandu J., Sidhu T. and Beresh B. and Tan J.-C., Application of Security Metrics in Auditing Computer Network Security, A Case Study, In Proceedings of *the 4th International Conference on Information and Automation for Sustainability (ICIAFS)*, IEEE, 2008, pp. 200- 205.

[83] *Programme of Prime Minister Alexander Stubb's Government*, Finnish Government, June 2014.

[84] Qiu R. C., Hu Z., Li H., Michael and Wicks M. C., *Cognitive Radio Communication and Networking: Principles and Practice*, John Wiley & Sons, 2012.

[85] Ramachandran J., *Designing Security Architecture Solutions*, John Wiley & Sons, 2002.

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

[87] Ruiz J., Arjona M., Maña A., Rudolph C. and Paatero J., An Engineering Process and Modelling Framework for development of Secure Systems, In Proceedings of *NATO STO-MP-IST-115*, May 2013, pp. 1-10.

[88] Savola R. M. and Abie H., Development of security metrics for a distributed messaging system, In Proceedings of *International Conference on Application of Information and Communication Technologies (AICT)*, IEEE, 2009, pp. 1 - 6.

[89] Schiller J., *Cyber Attacks & Protection*, CreateSpace, Paramount, CA, 2010.

[90] *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.

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

[92] Sherwood N. A., *Enterprise Security Architecture: A Business-Driven Approach*, CRC Press, 2005.

[93] Shi-Chang L. et al., Research on MANET Security Architecture Design, In Proceedings of *International Conference on Signal Acquisition and Processing (ICSAP'10)*, IEEE, 2010, pp 90 - 93.

[94] Shore, M. and Deng, X., Architecting Survivable Networks using SABSA, In Proceedings of *6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, IEEE , 2010, pp. 1 - 7.

[95] Suri N., Benincasa G., Tortonesi M., Stefanelli C., Kovach J., Winkler R. and Watson S., Peer-to-peer communications for tactical environments: Observations, requirements, and experiences. *Communications Magazine*, IEEE, 48(10), pp. 60-69, 2010.

[96] *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].

[97] Sweeney L., k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05), 2002, pp. 557-570.

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

[99] Symington S., Farrell S. Weiss H. and Lovell P., *Bundle Security Protocol Specification*, Internet-Draft, IETF DTN Research Group, November 2010.

[100] *The DoD Architecture Framework*, Version 2.2, US DoD, August 2010.

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

[102] Thomas R. W., *Cognitive Networks*, Doctoral Dissertation, Virginia Polytechnic Institute and State University, June 15, 2007.

[103] Thomas R. W., DaSilva L. A. and MacKenzie A. B., Cognitive Networks, In Proceedings of *the International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, IEEE, 2005, pp. 352 - 360.

[104] Thomas R. W., DaSilva L. A., Marathe M. V. and Wood K. N., Critical Design Decisions for Cognitive Networks, In Proceedings of *IEEE International Conference on Communications, (ICC),* IEEE, 2007, pp. 3993 - 3998.

[105] 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 Communications Magazine*, Vol. 44, Issue 12, 2006, pp. 51 - 57.

[106] TOGAF, Open Group, http://www.opengroup.org/architecture/togaf [cited 26.5.2015].

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

[108] *US Army Network Security Reference Architecture*, Version 1.0, CIO/G-6 Reference Architecture Series, 1 August 2013.

[109] Vasilakos A. V. and Spyropoulos T., *Delay Tolerant Networks: Protocols and Applications Wireless Networks and Mobile Communications*, CRC Press, 2012.

[110] Vermasvuori M., Enden P., Haavisto S. and Jamsa-Jounela S.-L., The use of Kohonen self-organizing maps in process monitoring, In Proceedings of *the First International IEEE Symposium Intelligent Systems*, Vol. 3, IEEE, 2002, pp. 2 - 7.

[111] Wang H., Wang Y. and Han J., A Security Architecture for Tactical Mobile Ad hoc Networks, In Proceedings of *The IEEE Second International Workshop on Knowledge Discovery and Data Mining (WKDD)*, IEEE, 2009, pp. 312-315.28

[112] Weidinger M. and Hansen J. D., Security Solution for Network-Enabled Capability, In Proceedings of *NATO RTO PCN Workshop*, Istanbul, Turkey, January 2009.

[113] Westin A. F., *Privacy and Freedom*, Atheneum, New York, 1967.

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

[115] Zheng Y., Lu H. and Sun Y., An Intelligent and Cognitive Service Delivery Platform Model, In Proceedings of *the IEEE Second International Symposium on Intelligent Information Technology Application*, Shanghai, 2008, pp. 137 – 140.

Errata

Publication 1

No erratas

Publication 2

No erratas

Publication 3

No erratas

Publication 4

No erratas

Publication 5

In the introduction paragraph, the statement "traditional human based network management" is imprecise and interpretable. In this context, "traditional human based" means manually provided configuration management. A network operator adjusts network parameters manually without automated processes. Next generation network management will include automated, and even self-learning network management but in some sense human control may appear to ensure automated system provides reasonable results.

In Section 4.2, the expected damage from an event or incident is defined as the sum of the probabilities of each possible consequence. The correct definition is the sum of the products of the consequences multiplied by their probabilities.

Publication 6

No erratas

Publication 7

No erratas

Aalto-DD 170/2015

9 789526 064550

ISBN 978-952-60-6455-0 (printed)
ISBN 978-952-60-6454-3 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

Aalto University
School of Electrical Engineering
Department of Communications and Networking
www.aalto.fi