National Defence University
Series 1: Research Publications No. 47

Utilizing Trust Management in a High-Security Context

Klaus Zaerens

KLAUS ZAERENS

UTILIZING TRUST MANAGEMENT IN A HIGH-SECURITY CONTEXT

ACADEMIC DISSERTATION

To be presented, with the permission of the Research Council of National Defence University, for public criticism for the degree of Doctor of Military Sciences in auditorium Itälinnake at the National Defence University, Santahamina, Helsinki, on April 1st 2022 at 12 o'clock.

NATIONAL DEFENCE UNIVERSITY
HELSINKI 2022

MAANPUOLUSTUSKORKEAKOULU
JULKAISUSARJA 1: TUTKIMUKSIA NRO 47

NATIONAL DEFENCE UNIVERSITY
SERIES 1: RESEARCH PUBLICATIONS NO. 47

UTILIZING TRUST MANAGEMENT IN A HIGH-SECURITY CONTEXT

KLAUS ZAERENS

NATIONAL DEFENCE UNIVERSITY
HELSINKI 2022

Klaus Zaerens: *Utilizing Trust Management in a High-Security Context*
Maanpuolustuskorkeakoulu
Julkaisusarja 1: Tutkimuksia nro 47
Väitöskirja /
National Defence University
Series 1: Research Publications No. 47
Doctoral dissertation

Author:	M.Sc Klaus Zaerens
Supervising professor:	Professor Jouko Vankka National Defence University, Finland Department of Military Technology
Preliminary examiners:	Adjunct professor, D.Sc. (Tech.) Tuija Kuusisto University of Jyväskylä, Finland
	D.Sc. (Tech.) Sari Uusipaavalniemi Finnish Defence Research Agency
Official opponent:	Professor Sasu Tarkoma University of Helsinki, Finland

Recent publications in PDF format: *http://www.doria.fi/handle/10024/73990*

Cover Design by Veera Anttila. Original artwork by Antonia Tempesta (1611). Plate 1: Roma and Batavia Shaking Hands, from The War of the Romans Against the Batavians (Romanorvm et Batavorvm societas).

ISBN 978-951-25-3270-4 (pbk.)
ISBN 978-951-25-3271-1 (PDF)
ISSN 2342-9992 (print)
ISSN 2343-0001 (online)

Maanpuolustuskorkeakoulu
National Defence University

PunaMusta Oy
Joensuu 2022
Finland

NORDIC SWAN ECOLABEL
Printed matter
4041-0619

To Riitta and Paul

ABSTRACT

Knowledge sharing is a key element of reciprocal collaboration within or between organizations. Time- and context-dependent shared knowledge can enhance situation awareness during operational activities and support decision-making for the parties participating in the knowledge sharing, but the shared knowledge must be trustworthy. Trust management can be used to evaluate the accuracy of shared information or define the trustworthiness of information recipients.

This dissertation discusses the subject of trust management in a high-security environment, where information is sensitive and requirements for data consistency, redundancy, reliability, and timeliness are high. Furthermore, in a high-security environment such as the military, malicious actors attempting to obstruct information transfer, corrupt data, or otherwise interfere for their own purposes is a perpetual threat.

The primary objective of this dissertation is to investigate how trust management can be utilized in information and knowledge sharing for high-security actors. One element of achieving this objective is describing the applicable technological environment, and the selected environment is a cloud computing environment with proposed expansions and additional security requirements. A computational model for defining system resilience was developed to analyze the operative risks of the proposed dynamic environment and identify cybersecurity vulnerabilities. Applying the proposed technological architecture, methods of trust management were explored to create a risk-sensitive knowledge-sharing system in an environment where trustworthiness varies among parties.

The research objectives were met through mathematical and conceptual methods of analysis. Empirical data was used to compare results. The dissertation contributes to several research areas, including cloud computing, cyber security, vulnerability analysis, risk assessment, trust management and blockchain technology. Key research results were:

- a new service model, Knowledge Management as a Service
- a concept for dynamic development of a high-security network
- a computing model for defining vulnerabilities, risks, threats and operational resilience in a cyber operational environment
- algorithms for quantifying changes in knowledge security classifications
- a blockchain-technology-based management system for knowledge sharing.

Keywords: trust management, cloud computing, cyber security, vulnerability analysis, risk management, operational resilience, blockchains, information sharing

TIIVISTELMÄ

Tiedon jakaminen organisaatiossa tai sidosryhmäorganisaatioiden välillä on välttämätöntä pyrittäessä luomaan vuorovaikutukseen perustuvaa yhteistoimintaa. Operatiivisessa toiminnassa käytettävä tieto on sidoksissa aikaan ja kontekstiin täydentäen kunkin osapuolen käsitystä tilannekuvasta. Tällaiseen päätöksenteon tueksi saatavaan tilannetietoon täytyy pystyä luottamaan. Luottamuksen hallinnan avulla voidaan arvioida saadun tiedon oikeellisuutta tai kuvata tiedon vastaanottajan luotettavuutta.

Tässä väitöskirjassa käsitellään luottamuksen hallintaa korkean turvallisuuden ympäristössä, jossa tietosisältö on sensitiivistä, vaatimukset tiedon yhteneväisyydelle, redundanttiudelle, luotettavuudelle ja ajanmukaisuudelle ovat korkeat. Korkean turvallisuuden ympäristössä, kuten esimerkiksi asevoimien ympäristössä on lisäksi jatkuva uhka vihamielisestä toimijasta, joka pyrkii sekaantumaan tiedonvälitykseen keräämällä tietoa omiin tarkoitusperiin, vääristämällä tietoa tai muuten häiritsemällä.

Väitöskirjan keskeisenä tavoitteena oli tutkia korkean turvallisuuden toimijoiden tietojen ja tietämyksen jakamista luottamuksen hallinnan keinoin. Osana tavoitteeseen pyrkimistä oli kuvata soveltuvaa tietoteknistä ympäristöä. Tällaiseksi tietoteknistiseksi ympäristöksi valikoitui pilvilaskentaympäristö ehdotetuin laajennuksin ja turvallisuuteen liittyvin lisävaatimuksin. Ehdotetun dynaamisen ympäristön operatiivisten riskien analysoimiseksi ja haavoittuvuuksien tunnistamiseksi kyberuhkien näkökulmasta laadittiin laskennallinen malli järjestelmän resilienssin määrittämiseksi. Esitettyyn teknologiseen arkkitehtuuriin nojautuen tutkittiin luottamuksen hallinnan menetelmiä riskitietoisen tiedonvälitysjärjestelmän luomiseksi ympäristöön, jonka toimijoiden keskinäinen luottamus vaihtelee.

Tutkimuksen tavoitteeseen päästiin matemaattisten- ja käsitteellisten analyysimenetelmien avulla käyttäen empiiristä aineistoa tulosten vertailussa. Väitöskirja täydentää osaltaan useaa tutkimusaluetta, kuten pilvilaskentaa, kyberturvallisuutta, haavoittuvuusanalyysiä, riskien hallintaa, luottamuksen hallintaa ja lohkoketjuteknologiaa.

Tutkimuksen keskeiset tulokset olivat:

- Uusi palvelumalli Tietämys palveluna (Knowledge Management as a Service)
- Konsepti korotetun turvallisuuden verkon dynaamiseksi muodostamiseksi
- Laskentamalli haavoittuvuuksien, riskien, uhkien sekä liiketoiminnallisen resilienssin määrittämiseksi kybertoimintaympäristössä
- Algoritmit tietoturvatason muutosten kvantifioimiseksi
- Lohkoketjuteknologiaan perustuva tiedon välittämisen hallintajärjestelmä.

Avainsanat: luottamuksen hallinta, pilvilaskenta, kyberturvallisuus, haavoittuvuusanalyysi, riskien hallinta, liiketoiminnallinen resilienssi, lohkoketjut, tiedon jakaminen

AKNOWLEDGEMENTS

This has been a long-term project, to say the least, and a decade inevitably involves any number of developments and changes. I've been afforded a unique opportunity to meet numerous international researchers and to exchange well-argued and fact-based ideas and views with them on topics ranging from music to cooking, from global power politics to nuclear disasters, from the dominance of social media to East Asian privacy protections. I've learned many things about new cultures, international politics, society, security, and IT that few have the privilege to experience. This exposure to different and sometimes opposing viewpoints has ultimately made things less straightforward. To adapt the words of Socrates, I've come to know how little I know.

I'm extremely grateful to the Finnish National Defence University for the opportunity to write this dissertation. In particular I'm grateful for the liberal timetable, which has made it possible for me to work full-time while continuing my research. I'm also deeply appreciative of the academic freedoms granted me during my studies. As a department emphasizing cross-disciplinary applied research, the Department of Military Technology has been a superb home for conducting my work. I'd like to thank Professor Jouko Vankka for the long-term advising during the various stages of research, his cooperation, and the opportunities to bring my expertise to bear in instruction at the National Defence University.

I'm grateful for the comments and feedback from my reviewers, Dr. Tuija Kuusisto and Dr. Sari Uusipaavalniemi. It is thanks to them that I was able to focus and flesh out the objectives and contents of the dissertation in a way that made it possible to present the results in the desired form. My gratitude goes to the Jenny and Antti Wihuri Foundation as well as the Support Foundation for National Defence for supporting the publication of the dissertation articles.

The articles demanded years of work. I'm grateful to Jan Mickos and Jari Mannonen for their sparring and contributions to the contents of my research. Along the way we have envisioned, planned, accumulated experiences, and worked on a variety of projects. Some of the results of our collaboration are found directly in this dissertation, others indirectly. A big thanks to Anu Karjalainen for intermittently wrenching me back to reality and reminding me that there's more to life than work. Thanks to my research colleague Dr. Markus Häyhtiö for the cooperation, encouragement, and support. I'd also like to thank Dr. Lea Kutvonen for her advice on contents and tips concerning the scope of the research as a whole. And thank you, Virpi Tuukkanen, for the valuable support in compiling the Introduction.

I'd especially like to thank Kristian London. His support and assistance in editing and proofing were critical to the completion of this dissertation. I am forever grateful.

I've been fortunate to have a supportive family and many incredible friends and colleagues. Listing them individually would be an impossible task. Each of you has participated in your own way to the creation of this work. If you and I have shared an encounter at some point during our histories, you can be sure that you have contributed in some way to the dissertation you are about to read.

Haluan omistaa tämän työn vanhemmilleni. He ovat vaikuttaneet ylivoimaisesti eniten valmiuksiini, asenteisiini ja arvoihini. Heidän ansiosta tämä tutkimus on edistynyt ja väitöskirja valmistunut.

Non scholae sed vitae discimus.

PUBLICATIONS COMPRISING THE DISSERTATION

This doctoral dissertation by Klaus Zaerens consists of a summary and the following six peer-reviewed publications (papers):

[1] Zaerens, K.: Enabling the Benefits of Cloud Computing in a Military Context.
2011 IEEE Asia-Pacific Services Computing Conference, Jeju Island, 2011, pp. 166-173.

[2] Zaerens, K.: Gaining the Profits of Cloud Computing in a Public Authority Environment.
Int. J. Computational Science and Engineering, special issue on "Advanced Challenges and Research Trends in Cloud and Grid Interoperability," 2012.

[3] Zaerens, K., Mannonen, J.: Concept for the Construction of a High Security Environment in a Public Authority Cloud.
Lecture Notes in Electrical Engineering, Springer-Verlag, September 6, 2012.

[4] Zaerens, K.: Business Resilient Vulnerability Analysis for a Dynamic High Security Environment.
Proceedings of the 2015 18th International Conference on Network-Based Information Systems. September 2015, pp. 242–249.

[5] Häyhtiö, M., & Zaerens, K.: A Comprehensive Assessment Model for Critical Infrastructure Protection.
Management and Production Engineering Review, 8(4), 42-53.

[6] Zaerens, K.: Concept for Controlled Business Critical Information Sharing using Smart Contracts.
2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018, pp. 1-8.

TABLE OF CONTENTS

CONTRIBUTIONS OF THE AUTHOR

The author was the sole author of publications [1], [2], [4] and [6] and the primary author of publication [3]. ICT Technical Architect Jari Mannonen helped to determine the practical requirements for a dynamic high-security cloud environment for publication [3]. Dr. Markus Häyhtiö was the co-author of publication [5]. The author's roles are described in more detail in Table 1.

Table 1. The contributions of the author

Article	**Conceptualization and research design**	**Collecting data / material**	**Interpretation and conclusions**	**Paper writing**	**Overall role**
[1]	X	X	X	X	Sole author
[2]	X	X	X	X	Sole author
[3]	X	X	X	X	Primary author
[4]	X	X	X	X	Sole author
[5]	X	X	X	X	Primary author of chapters 5, 6. Co-author of chapters 2, 4, 7, 8.
[6]	X	X	X	X	Sole author

LIST OF ABBREVIATIONS AND SYMBOLS

CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CNO	Computer Network Operations
CND	Computer Network Defense
CNA / CNE	Computer Network Attack / Computer Network Exploitation
CPS	Cyber-Physical System
CoT	Circle of Trust
DaaS	Data as a Service
DTA	Dynamic Taint Analysis
EW	Electronic Warfare
$f(A_{key})$	encryption of information with key provided by A
$f'(A_{key})$	decryption of information with key provided by A
FDF	Finnish Defence Forces
HaaS	Hardware as a Service
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
ISO	The International Organization for Standardization
IT	Information Technology
KATAKRI	information security audit tool for authorities instated by the National Security Authority (NSA) of Finland
KMaaS	Knowledge Management as a Service
MILDEC	military deception
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OPSEC	operations security
P2P	point-to-point protocol
PaaS	Platform as a Service
PSYOPS	psychological operations
ROI	Return Of Investment
s_{AB}	information sent from information provider A to information recipient B
SaaS	Software as a Service
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
TCO	Total Cost of Ownership
TUVE	national High-Readiness Network (in Finnish: *Turvallisuusverkko*)
VAHTI	Public Sector Digital Security Management Board of Finland
VPN	Virtual Private Network
w_{AB}	trust weight: the amount of trust information sender A has in information recipient B

LIST OF FIGURES

LIST OF TABLES

DEFINITIONS

Key concepts referred to in this dissertation are defined below. Some of these concepts may be defined in different ways in other contexts; the definition provided describes the way the concept is used here. Each definition includes a reference to the original source from which the concept was adopted or adapted or a reference to the dissertation chapter or article in which the concept is discussed in greater detail.

Attack tree methodology is a methodology for observing process execution from a failure perspective. The process being observed must have a starting point and at least one successful endpoint. In the Attack Tree methodology, successful states are all those finite states before the successful endpoint of the initial process (Fung et al., 2005).

Blockchain is a chain of blocks with each block referencing the block that preceded it. The most-difficult-to-recreate chain is the best blockchain (Bitcoin, 2009).

Business is typically viewed as the activity of buying and selling goods and services (Cambridge Dictionary, 2021). In the scope of this dissertation, this definition is extended from a purely commercial context to include the functions of any particular field of endeavor (Merriam-Webster Dictionary, 2021). Despite this expansion, it is important to emphasize that commercial organizations and government organizations are not to be confused, as they serve different purposes (Mintzberg 2017). As this dissertation focuses on fulfilling specific functions as opposed to overall organizational objectives and takes into consideration economic factors in the performance of those functions, the use of the term *business* to refer to the functions of public authorities is justified. Moreover, although governments are not concerned with profitability, public organizations operate under budgetary and monetary constraints.

Business resilience is the ability of an organization to persist in the face of substantial changes in the business (see the definition of *business* as it is used in this dissertation) and operative environment and/or the ability to withstand disruptions and catastrophic events (Acquaah et al., 2011).

Circle of Trust is a consortium established around a specified subject and formed solely of trusted parties (Chapter 2.4.2).

Cloud computing is a model for enabling ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2009).

Common operative picture is a single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness (US JCS, 2020).

Community cloud is a cloud infrastructure provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of these, and it may exist on or off premises (Mell & Grance, 2009).

Cryptography is the science of secret writing used when communicating over any untrusted medium. The five primary functions of cryptography include privacy/confidentiality, authentication, integrity, non-repudiation and key exchange (Kessler, 1998).

Cyber-attack consists of actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain and is considered a form of fires (US JCS, 2018).

Cyber espionage is activity where a state unlawfully acquires classified information from foreign data systems, either by intruding into the systems by technical means or by exerting pressure on an entity within its own jurisdiction that has a technical access to classified information stored in another state (Finnish Security and Intelligence Service, 2019).

Cyber warfare is warfare or war conducted in cyberspace (Chapter 2.1.1).

Cyber weapon is a computer program created and/or used to alter or damage (an ICT component of) a system in order to achieve (military) objectives against adversaries inside and/or outside cyberspace (Maathuis, Pieters & Den Berg, 2016).

Cyber–physical system is a smart system that includes engineered interacting networks of physical and computational components (NIST SPEC PUB 1500-201, 2017).

Cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed or deleted (Andress & Winterfeld, 2011).

Data is information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful (Merriam-Webster Dictionary, 2021). Within the scope of this dissertation, data is transmitted or processed in digital form.

Data as a Service is a service model that enables the user to store and access data regardless of physical implementation while ensuring consistency and redundancy. Typically, Data as a Service is an implementation of a database [1].

Decryption is the process by which ciphertext is transformed back into the original plaintext (Kessler, 1998).

Deception See military deception.

Deployment model is a cloud infrastructure in which service models are implemented and to which consumers are connected [1].

Distributed computing a method of running programs across several computers on a network (Lee et al., 1999).

Distrust is a quantified belief by a trustor that a trustee is incompetent, dishonest, not secure or not dependable within a specified context (Grandison & Sloman, 2002).

Dynamic high-security environment refers, within scope of the dissertation, to a high-security system environment that is not static in terms of application platform or infrastructure. A dynamic approach ensures both sufficient computational capacity and compliance with security requirements in those scenarios where the need for computational activities is high [2].

Ecosystem is, within the scope of this dissertation, a digital business ecosystem that extends the networking paradigm to the knowledge and social layers, to knowledge, processes and economic activities working in cooperation and competition. Digital business ecosystems are designed to evolve under the pressure of economic forces and to adapt to local conditions (Nachira et al., 2007).

Edge computing refers to allowing computation to be performed at the edge of the network, on downstream data on behalf of cloud services and upstream data on behalf of data source services (Shi et al., 2016).

Encryption is the process of transforming unencrypted data, or plaintext, into ciphertext (Kessler, 1998).

Grid computing is a computing paradigm in which numerous computers are interconnected, creating a super computer. It represents a system that coordinates resources that are not subject to centralized control, using standard, open, general-purpose protocols and interfaces to deliver nontrivial qualities of service (Foster, 2002).

Hacktivism is computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism (Merriam-Webster Dictionary, 2021).

Hardware as a Service is a lower-level service model than Infrastructure as a Service. It enables the user to precisely specify the type of service resources needed. For example, a service can include a server or a firewall [1].

High-security environment /-system is such an environment or system where any breach towards information or information system integrity, confidentiality or availability could have severe and hazardous impact to operations, assets or individuals (Chapter 1).

Hybrid cloud is a cloud infrastructure that is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) (Mell & Grance, 2009).

Information is the communication or reception of knowledge or intelligence (Merriam-Webster Dictionary, 2021).

An **information system** is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information resources include information and related resources, such as personnel, equipment, funds, and information technology (NIST FIPS PUB 200, 2006).

Infrastructure as a Service is the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources and allows the consumer to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications and possibly limited control of select networking components (Mell & Grance, 2009).

Knowledge is defined as awareness, understanding, or information that has been obtained by experience or study, and that exists either in an individual's mind or is possessed by people generally (Cambridge Dictionary, 2021). Within the scope of this dissertation, the focus can be narrowed from people to organizations or professions, which makes it more usable for certain technical systems.

Knowledge management is the process of creating, sharing, using and managing the knowledge and information of an organization (Girard, J.P. & Girard, J.L., 2015).

Knowledge Management as a Service is a service model in which the user is able to access knowledge in a more pervasive way [1].

Military context is, within the scope of this dissertation, viewed as an ecosystem of systems, environments, and stakeholders where the main actor is a legitimized and sovereign state-controlled armed forces and all operations, functions, and actions thereof.

Military deception (MILDEC) is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JP 3-13.4., 2012).

North Atlantic Treaty Organization, or North Atlantic Alliance, is an intergovernmental military alliance between thirty North American and European countries (NATO).

Pervasive computing is the awareness of web capabilities: mobile and web applications adapt performance according to infrastructure features (Mei, Chan & Tse, 2008; Saha & Mukherjee, 2003).

Platform as a Service is a capability provided to the consumer to deploy into the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment (Mell & Grance, 2009).

Point-to-point protocol is data transfer (transportation of packages) protocol between two peers (RFC 1661, 1994).

Private cloud is a cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed and operated by the organization, a third party or some combination of these and it may exist on or off premises (Mell & Grance, 2009).

Public cloud is a cloud infrastructure provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization, or some combination of these. It exists on the premises of the cloud provider (Mell & Grance, 2009).

Reputation is a community-based feature of entity to assist evaluating the trustworthiness and predicting the future behavior without prior experience (Xiong & Liu, 2003).

Risk is effect of uncertainty on objectives (ISO 31000:2018, 2018).

Risk management is a process that uses vulnerability assessment results to answer the following additional questions: (1) Based on the vulnerabilities identified, what is the likelihood that the system will fail? (2) What are the consequences of such failure? (3) Are these consequences acceptable? (Baker, 2005).

Role is a set of connected behaviors, rights, obligations, beliefs, and norms as conceptualized by actors in an organization or in a social situation (Chapter 2.4.1).

Security level is a characterization of a system's relative information security value where at the lowest (i.e., value zero) no security controls are implemented and at the highest (i.e., value one) theoretically all vulnerabilities, known and unknown threats are identified and mitigated, information is secured from any impact towards confidentiality, integrity, or availability, and business resilience is ensured in all situations. In practice, having a fully secured system is neither viable nor appropriate. A system's security level is always bound to environment and context and as a value is not, therefore, comparable to any security level value from any other system [4, 5].

Service level agreement is a contract between a service provider and its customers that document what services the provider will furnish and defines the service standards the provider is obligated to meet (TechTarget, 2020).

Service model is the model that defines the level and contents of cloud capabilities offered to consumer [1].

Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and a projection of their status in the near future (Endsley, 1988).

Service oriented architecture is a style of software design where services are provided to components by other application components via a communication protocol over a network. Its principles are independent of vendors and other technologies (Medium, 2019).

Smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties (Buterin, 2020).

Software as a Service is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings (Mell & Grance, 2009).

Survivability is provided by a system class that is able to execute a task in reasonable time, even if significant parts of the system are paralyzed due to an attack or damage (Barbacci, 1996).

Threat is the potential cause of an incident that may result in a breach of information security or compromise business operations (ISO/IEC 27001:2013, 2013).

Trust is a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context (Grandison & Sloman, 2002).

Trust management is limited to computative trust management for the purposes of this dissertation. Widely accepted features of computative trust management include subjectivity, expected probability and relevance (Abdul-Rahman & Hailes, 1998; Zhou, Xu & Wang, 2011).

Trust transitivity is a concept in which it is assumed that if agent A trusts agent B, and that agent B trusts agent C, then by transitivity, agent A trusts agent C (Jøsang & Pope, 2005).

Trustworthiness is deserving of trust or confidence (Dictionary.com, 2020). It expresses dependability and reliability.

Ubiquitous computing. See pervasive computing.

Utility computing is a computing paradigm in which consumer pays as one uses the resources and service provider provisions the services to consumers as per request (Yeo & Buyya, 2006).

Virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure sensitive data is safely transmitted (CISCO, 2020).

Virtualization uses software to create an abstraction layer over computer hardware that allows the hardware elements of a single computer—processors, memory, storage and more—to be divided into multiple virtual computers, commonly called virtual machines. Each virtual machine runs its own operating system and behaves like an independent computer, even though it is running on just a portion of the actual underlying computer hardware (IBM, 2019).

Vulnerability is a weakness of an asset or group of assets that can be exploited by one or more threats. An asset is as anything that has value to an organization, its business operations and their continuity, including information resources that support the organization's mission (ISO/IEC 27005:2018, 2018).

Vulnerability analysis/assessment is the process of identifying, quantifying and prioritizing (or ranking) the vulnerabilities in a system (Chapter 2.3).

1

INTRODUCTION

The importance of trust management is increasing as the Internet continues to open up, various collaborative environments grow more common, and social networking affects decision making. Despite this gradual increase in the significance of trust management, its multilateral nature, the need to ensure the trustworthiness of parties, and large information sets with high response-time requirements have largely kept commercial providers and applications from introducing it in public authority environments.

Public authorities in the security field have sought and developed numerous means to improve cooperation through information and communications technology (ICT). Various collaboration tools and environments have been deployed, and integration of processing and data storage systems has improved. Concepts like semantic knowledge processing, connectivity, and social networking enable improved cooperation between authorities. However, these concepts create new challenges. Coupled with requirements for data accuracy, consistency, and redundancy, the amount of information demands excessive computational and data storage capabilities. Furthermore, openness can be hard to manage in an environment where sensitive information is handled or the technical availability and the fault tolerance of the system must be ensured at all times. Finally, the processing and sharing of critical operative information can increase hostile interest in a system environment.

All of these challenges appear in high-security environments or systems. The definition of a high-security environment can be derived from the National Institute of Standards and Technology (NIST) approach of categorizing information system criticality based on three security objectives for information and information systems and analyzing the impact at the event of comptonization. These security objectives are confidentiality, integrity, and availability (NIST FIPS PUB 199, 2004). Confidentiality is compromised if information is disclosed without authorization. Integrity is compromised if information is modified or destroyed without authorization. Availability is compromised if information or the information system cannot be accessed. In a high-security environment or system, the impact of comptonization is high if any failure in reaching security objectives could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals (NIST FIPS PUB 199, 2004).

This dissertation examines information sharing in high-security environments by applying observations from public authority systems more broadly to military systems in which the need for computational capacity is high and the reliability of information is always critical. Others sectors, such as healthcare and finance, share many of the characteristics, security objectives, and challenges of this military high-security environment. As in terms of technology architecture, the information or data content is not relevant to the logical solution, solutions developed for military or public authority systems can be applied to other contexts where security demands careful consideration and the trustworthiness of information system needs to be ensured.

The business world has long been interested in improving the cost-effectiveness of information technology infrastructure and computing, and the maturity of old technologies has enabled their combining into the paradigm now known as cloud computing. Corporations are desperately hunting for clients, application environments and applications to make good on this paradigm's claims: cost-effectiveness, scalability, and fault tolerance. This dissertation explores the cloud computing paradigm in terms of its capacity to meet computational needs for ensuring identification and guaranteeing information reliability.

As a natural consequence of technology and market development, several projects related to the use of cloud computing technology have been launched over the years in high-security systems. Public authorities and armed forces have traditionally required isolated computing environments for mission-critical data, which has prevented wide experiments within operational systems. However, the benefits of cloud computing that can be achieved in these kinds of systems are the same as those that can be achieved in any organization: cost-effective computing and a decrease in the total costs of ownership.

When adapting common commercial solutions such as cloud computing to high-security contexts, there is a need to understand the level of security they provide and the organization's requirements for guaranteeing a secure service ecosystem. Ensuring the security of a technological platform containing solutions for infrastructure, hardware, and operative software allows the construction of a collaborative environment and points the way to an effective approach for achieving a trust-based scheme for information sharing.

1.1. Research purpose and objectives

The purpose of the research is to present novel collaborative information technology solutions for high-security environments by tapping increased computational capabilities and large amounts of available information.

The aim is to enable a survivable system providing reliable information and a trustworthy, secure information-sharing platform to improve situation awareness and to facilitate operative decision-making. Achieving this aim requires examination of both technological system management and information management.

For this dissertation, cloud computing was initially selected as the approach to the technological platform because it was an emerging paradigm. Later, the justifications for this selection also came to include the maturity of centralized computing technology and the theoretical promises of infinite computational capabilities.

But before adapting any new technology in high-security environments, system prerequisites need to be examined. Since high-security systems contain sensitive information, system security and potential vulnerabilities are critical considerations. In addition, extreme environments require robustness, system survivability, and overall reliability. Finally, the complexity of the technological system needs assessing, as do the multiple stakeholders and actors involved in utilizing features that enable the harnessing of the advantages of cloud computing. Taken as a whole, these dimensions make up the service ecosystem (Ng & Maull et al., 2009; Grönroos, 2011) and, in this instance, increase the number of potential threat vectors to which a system is exposed.

When prioritizing the risks to be mitigated, the impact a specific threat poses to the system needs to be assessed (Lewis, 2014). Such mitigative actions should be analyzed in terms of cost and profit. In a dynamic environment, this quantified assessment must be designed to recognize that any change in system setup always changes the overall security level of the system and must take place before the introduction of any new technologies into the environment. Understanding the consequences of any risks entailed in any decision made regarding the environment is critical.

After a careful assessment of risks, security level, and platform vulnerabilities have been performed, services can be developed. As noted before, information quality, correctness, and reliability need to be ensured in situation-awareness systems. In high-security environments, information can be of system, sensor, or human origin, which means threats can be realized in any variety of ways. Technical components may behave deficiently, especially under extreme conditions. Humans can make errors or deliberately emphasize a specific message. Or a malicious actor may exist inside the system, sabotaging the data flow with inaccurate information. All such misleading elements should be recognized and eliminated from the decision-making process.

The scope of this dissertation is limited to the trustworthiness of information regardless of data source: whether a failure occurs because a component fails to send correct information or because a malicious actor forces a component to send incorrect information is immaterial. In this instance, the approach to the trustworthiness and reliability of information is based on a specific case involving information sharing between collaborating parties. Within such a collaborative ecosystem, information needs to be shared even if the stakeholders do not fully trust each other; in other words, at some point a decision must be made as to whether the benefits of the information sharing outweigh the benefits of remaining outside of the ecosystem. This applies especially in cases of situation-awareness systems, in which comprehensive situation awareness requires information from partner and stakeholder organizations.

In summarizing the research objectives, this dissertation attempts to answer the following three questions:

What are the security and other key related implications of adopting a cloud computing paradigm in an environment containing sensitive information, and what new functions are needed to ensure the confidentiality of operations and information?
What are the measures for quantifying business resilience?

How could the concept of trust management be implemented in a collaborative information-sharing ecosystem where the stakeholders do not fully trust each other in such way that the confidentiality of the information provider is ensured, sharing is controlled, and the information quality meets the criteria for the collaboration?

As described earlier, in order to understand the applicability of any new technology in a high-security context, the impact on the system's security level must be evaluated. Therefore, the results from exploration of the second research question provide tools for evaluating the applicability of results from investigating research questions 1 and 3.

Figure 1 presents the various disciplines and domains of scientific research involved in this dissertation and the research question that addresses each domain. Theoretical domains and their classifications are adopted from IEEE Taxonomy (2021).

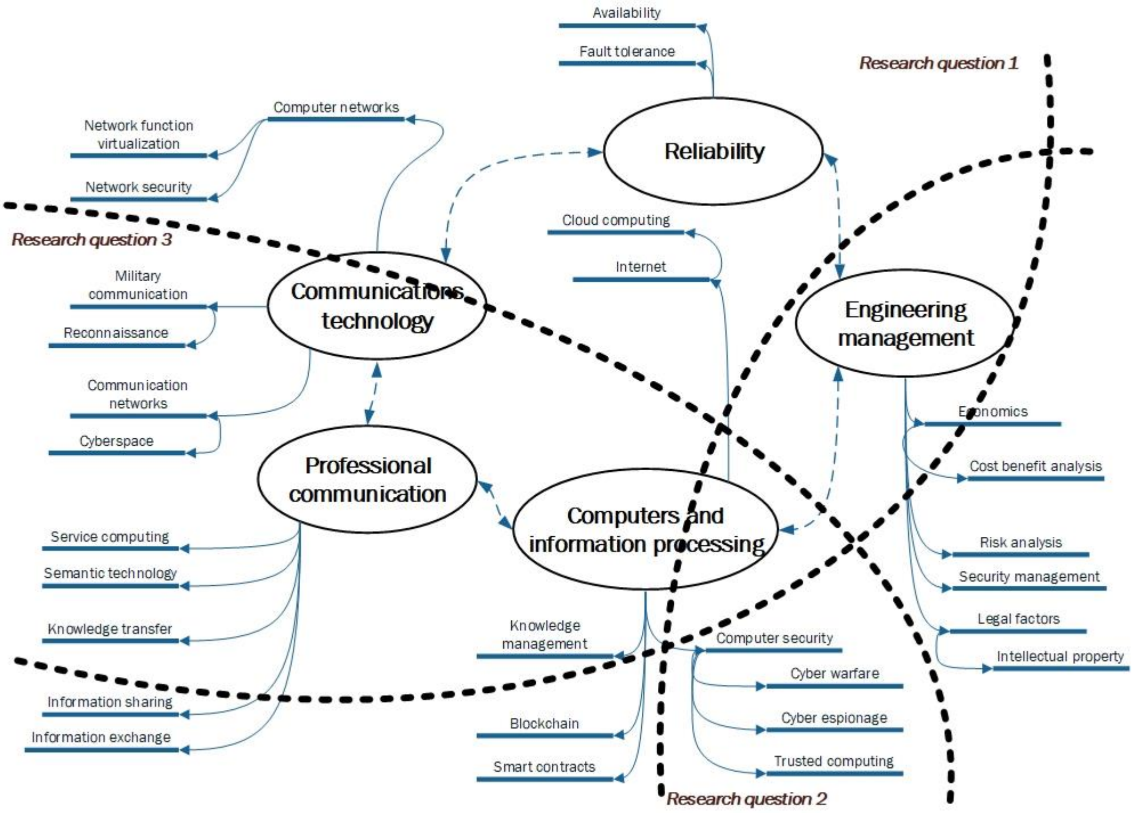


Figure 1. Theoretical domains of the dissertation and research questions.

Figure 1 illustrates how the research objectives are derived from the questions and theoretical foundations. Research question 1 addresses the infrastructure that enables the computational capabilities for any advanced, sophisticated ICT system. The infrastructure level provides most services for managing data. Research question 3 addresses an application-level innovation that utilizes the technologies and services provided by the technological infrastructure. The application level provides most services for managing information and knowledge. Research question 2 addresses maintaining the security level of the novel system, exposing risks to it, and the economic justification for investing in such a system.

1.2. Dissertation design

At a high level, the research process applied in this dissertation follows the information systems research framework presented by Hevner et al. (2004). As illustrated in **Figure 2**, this dissertation consists of three overarching themes. The relationship between the research questions and the six publications comprising the dissertation is presented in Table 2.

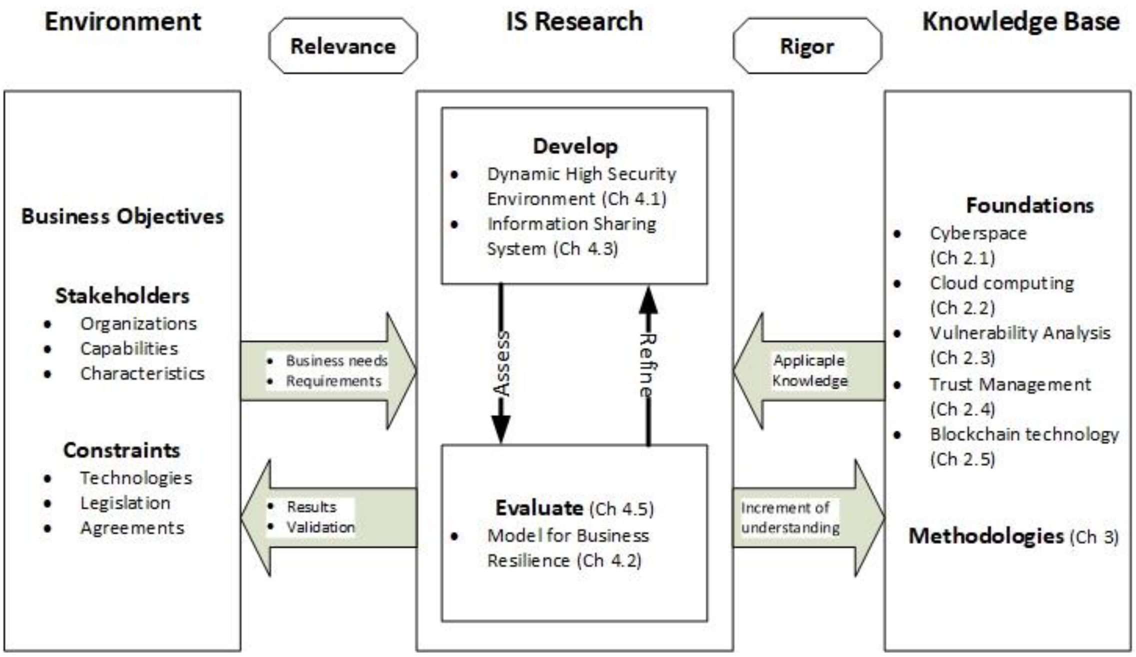


Figure 2. Research process

Table 2. The relationship between research questions and publications

Article	Research question 1	Research question 2	Research question 3
[1]	X		
[2]	X		
[3]	X		
[4]		X	
[5]		X	
[6]			X

The first section of this dissertation addresses infrastructure and the identification of applicable cloud computing environments with an eye to the special characteristics and requirements of high-security systems containing confidential information. This section is divided into three articles: the first focuses on the military context in particular, the second extends the examination to public authority systems in general, and the third presents a specific proposal regarding the requirements for a dynamic high-security environment.

The second section describes a quantitative model that provides a tool for evaluating information-security levels and addresses the cost-benefit ratios of improved security. This section consists of two articles. The first presents a quantitative model for assessing known threats and vulnerabilities, and the second extends the model to unknown threats, supply chains, and multiparty business ecosystems.

The third and the final section consists of one article, which describes a proposed system for an information-sharing platform that utilizes modern technologies in the environments described in and enabled by the proposals made in the first two sections. The structure of the dissertation is summarized in **Table 3**.

Table 3. Structure of the dissertation

<table>
<tr><td colspan="6">CH 1. Introduction</td></tr>
<tr><td colspan="6">CH 2. Theoretical foundations</td></tr>
<tr><td>CH 2.1 Cyberspace</td><td>CH 2.2 Cloud computing</td><td>CH 2.3 Vulnerability Analysis</td><td>CH 2.4 Trust management</td><td colspan="2">CH 2.5 Blockchain technology</td></tr>
<tr><td colspan="6">CH 7. Methodology</td></tr>
<tr><td colspan="6">CH 8. Results and discussion</td></tr>
<tr><td colspan="6">CH 9. Conclusions</td></tr>
<tr><td colspan="6">CH 10 Future research</td></tr>
<tr><td colspan="6">Appendix: Original publications</td></tr>
<tr><td>Article [1]</td><td>Article [2]</td><td>Article [3]</td><td>Article [4]</td><td>Article [5]</td><td>Article [6]</td></tr>
</table>

1.3. Limitations and assumptions

While more detailed descriptions of technical implementations offer a fruitful avenue for research, they are excluded from the scope of this dissertation. This dissertation is limited to the presentation of system logics and the theoretical analysis of their vulnerabilities.

Also excluded are service design and development, as well as a more detailed and comprehensive examination of requirement management in public–private partnerships. This dissertation focuses on the characteristics of unknown threats in an ecosystem with several stakeholders, and a public–private partnership network within a military context merely serves as an example of such an ecosystem. Nonetheless, the problem setting presented can be adapted to any private-sector environment with subcontracting parties.

Other topics excluded from the dissertation scope include further investigation of situation awareness, the establishment and maintaining of a common operative picture, and the detailed exploration of any other system that utilizes shared information for decision making. The articles and theoretical discussion are limited to the trustworthiness of information or knowledge, and do not address dimensions of utilization or application or the system impacts of information inaccuracy.

The dissertation does not address operation capability in any given environment where information is shared; it focuses on monitoring the information managed within said environment.

The military and public authorities are challenging environments for academic research, as public access to a wide range of practical information is restricted. Incidents in the cyber environment, capabilities, technical architectures, and physical equipment are generally classified as confidential or secret. This dissertation only contains information and data classified as public. Although a limitation in many ways, it nevertheless allows public presentation and discussion of the conclusions. Even so, as the material is a limited representation of the entirety, the implications and observations presented in the dissertation are limited to this subset.

2

THEORETICAL FOUNDATIONS

This chapter describes previous related work in this field of research, including definitions of central concepts. As the dissertation addresses multiple approaches to trust management and the factors that enable it, the theoretical foundations have been divided into subchapters, each focusing on different theoretical dimension.

The chapter is organized as follows. First, the high-security context is examined from the perspective of cyberspace, followed by a brief description of the foundations of cloud computing. The discussion continues with a focus on vulnerability assessment, technical-system survivability, information security, and data sensitivity in a high-security context. Finally, the chapter concludes with relevant investigations into the fields of trust management and blockchain technology.

2.1. Theory: Cyberspace

There are multiple definitions for cyberspace, each designed to serve the purpose of the organization publishing the definition. For example, the International Organization for Standardization (ISO) defines cyberspace as a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (ISO/IEC 27032:2012, 2012). This definition addresses the term broadly, emphasizing the stakeholder's connection to technology and leaving open the possibility for process standardization. Another, more technology-oriented definition of cyberspace, this time from the Government of the United Kingdom, is "the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept" (UK Cabinet Office, 2017). This definition focuses on cyberspace as consisting of separate technological systems connected to each other and containing all private and public systems connected with a common infrastructure. The Finnish Defence Forces (FDF) consider cyberspace as an operational environment that consists of digitalized information systems and in which all physical structures, actors and stakeholders are included (Laari et al., 2019).

For the purposes of this dissertation, the definition of cyberspace is relatively narrow: an electronic medium through which information is created, transmitted, received, stored, processed or deleted (Andress & Winterfeld, 2011). This definition is more information oriented and does not address the actual intentions, objectives, or preferences of actors or representations in the physical environment. Adopting this definition makes it easier to focus on the system environment from the perspective of data, information, and knowledge. It should be noted that the narrowness of the definition does not distort the results presented here, since the physical elements, infrastructure, and stakeholders impact the information itself, not the results.

Limiting observations to a high-security context allows for a sharper focus on the operative environment of cyberspace. Today's business-critical computational systems handle operational data, commands, and directives. Systems are also used for communication and collaboration between organizations. Computational systems containing sensitive and/or business-critical information make attractive targets for hostile actors or tempting challenges for individual hackers. The more important a system is in terms of operations or the more sensitive the data it contains, the more interesting it is as a target for adversarial actions.

2.1.1. Cyber warfare

Cyber warfare and cyber espionage cannot be disregarded in any current discussions of high-security contexts (Libicki, 2017). The involvement of state actors in operations impacting the private and public sectors has become commonplace. Certain governments resort to industrial espionage to boost their domestic economy and steal intellectual property from foreign companies (Libicki, 2017). State actors have the resources and the motivation to sharpen their cyber warfare and espionage skills during peacetime. In addition, the cyber space is safe environment to operate in, as risks of detection are limited due to extremely difficult attribution (Morgan, 2021). This chapter briefly outlines the characteristics of cyber warfare to the extent necessary to describe the environment and actors involved in high-security environments.

According to international legislation, warfare or war in general requires that the participants be organized groups or nations with political goals (Lewis, 2011). However, according to Andress and Winterfeld (2011), terrorist groups and individual hackers can also be seen as engaging in cyber warfare. This dissertation adopts the latter point of view, as the focus is on observing system performance after an attack; the original actor and/or the means they employ are not of interest.

The modern battlefield combines a traditional battlefield environment with cyberspace. There has been discussion as to whether cyberspace is a distinct domain of warfare, or whether it ought to be included the traditional domain (Welch, 2011).

The FDF states that cyberspace is embedded in all four recognized domains of warfare: land, sea, air, and space (Laari et al. 2019). However, some doctrines and some armed forces consider cyberspace a separate domain of warfare, if one dependent on the others (US JCS, 2018). For example, NATO officially proclaimed cyberspace as an operational domain at its 2016 summit in Warsaw (NATO, 2017).

Although this dissertation does not delve into a deeper discussion of the definition of warfare or debate the justifications for cyber-attacks or the nature of criminality, the complexity of the field needs to be understood, including its implications for and vulnerabilities in terms of legislation. National governments have nearly reached a global consensus that international law applies to cyberspace; however, there are still on-going discussions as to how international law ought to be applied in this context (CCDCOE, 2019). A taxonomy of cyber-related concepts is presented in **Figure 3** (Klimburg & Tiirmaa-Klaar, 2011). If we consider cyberpower as illustrated there, it is easy to find examples of events or phenomena in what we cannot unambiguously define as hostile interventions against national sovereignty, political hacktivism, criminal activity, industrial espionage (performed by enterprises), system malfunction, or simply a bored teen (Straub & Traylor, 2018). Moreover, information warfare operations conducted by governmental organizations can be modified to appear as any of those mentioned above (Sevis & Seker, 2016).

Bilateral US–Russian terminology defines a cyber-attack as the offensive use of a cyber weapon intended to harm a designated target. In this model, a cyber-attack is defined by weapon type, not the nature of the target. A cyber-attack can, thus, consist of a cyber weapon wielded against either a non-cyber asset or a cyber asset, but a non-cyber weapon used against a cyber asset would not be considered a cyber-attack (Rauscher & Yaschenko, 2011). Maathuis, Pieters and Den Berg (2016) propose a more specific definition for a cyber weapon. They define a cyber weapon as "a computer program created and/or used to alter or damage (an ICT component of) a system in order to achieve (military) objectives against adversaries inside and/or outside cyberspace." They go on to present the characteristics of advanced cyber weapon: target-specific, intangible (i.e., nonkinetic), less expensive, potentially configurable, non-reusable unless no countermeasures are taken, and violent to the extent of the objective. Furthermore, the creator of this weapon has a diversity of knowledge about the target and its objectives.

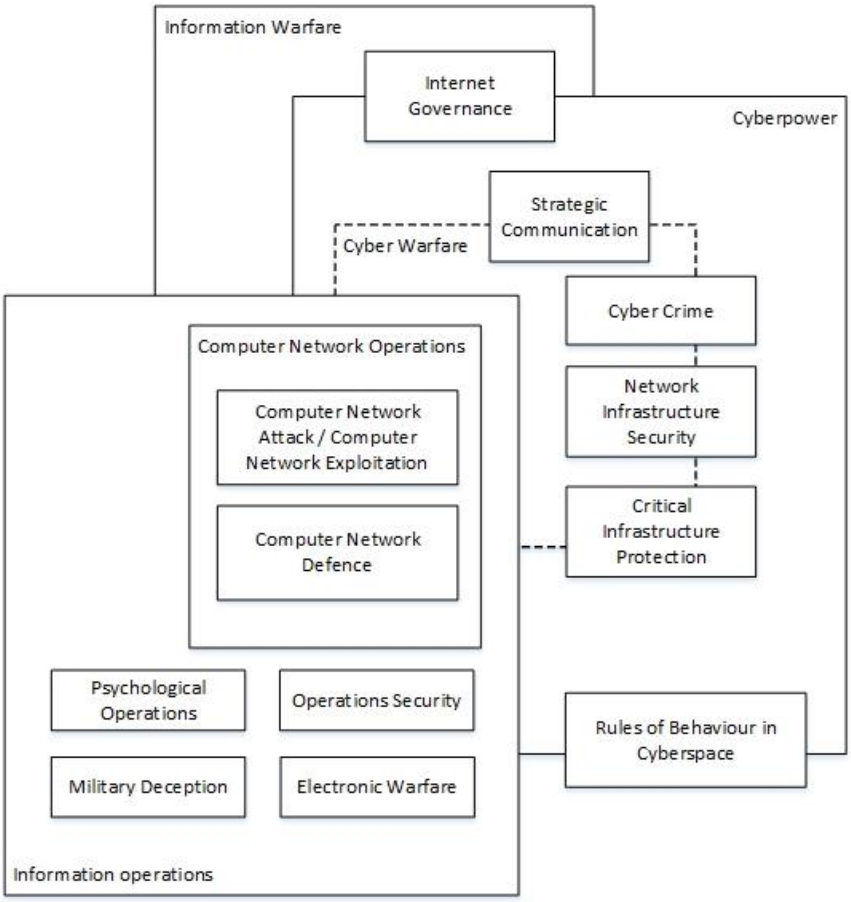


Figure 3. Taxonomy of cyber-related concepts

Cyber warfare includes tactical areas such as psychological weapons, physical weapons, computer network attacks, computer network defense, computer network exploitation, and logical weapons. Logical weapons are tools that can be used in cyber warfare, or to adopt a more detailed definition, a set of tools that might be used to conduct Computer Network Operations (CNO). These logical weapons can be divided into groups by phase of cyber-attack. The phases of attack and their respective tools are reconnaissance tools, scanning tools, access and escalation tools, exfiltration tools, sustainment tools, assault tools, and obfuscation tools. Many of these types of tools are free or have free versions accessible to the public via the Internet (Andress & Winterfeld, 2011).

Traditionally there has been little overlap between the concepts of information warfare and cyber warfare. Modern approaches to hybrid warfare rely on cyber warfare to increase the impact of information warfare measures (Loui & Hope, 2017). Loui and Hope (2017) describe the latest approaches to cyber-attacks as attacks on knowledge infrastructure. For example, instead of hacking a cyber–physical target, such as an energy grid or transportation system, disruptive operations can be designed to hack a knowledge infrastructure by causing a logistics problem or spreading fake news on election day (Loui & Hope, 2017).

2.2. Theory: Cloud computing

The purpose of cloud computing is to enable the use of ICT infrastructure more cost effectively and offer greater pervasiveness (Kumar et al., 2021). Cloud computing has derived characteristics from a variety of technologies, paradigms, and architectures, such as distributed computing, grid computing, pervasive computing, service-oriented architecture, utility computing, Internet computing and global computing. Because of this, it was initially unclear that cloud computing presented an entirely new paradigm. In particular, paradigm comparisons were made between cloud computing and grid computing, utility computing, and pervasive computing (Vaquero et al., 2009; Wand et al., 2008; Mei et al., 2008). This dissertation accepts the views presented by Wang and von Laszewski that cloud computing is a paradigm distinct from the others mentioned above.

There has been much discussion surrounding an accurate definition of cloud computing. The definitions presented vary more or less according to organizational, business, or operational environment or interests (Vaquero et al., 2009; Wand et al., 2008; Mei et al., 2008).

This dissertation relies on an extended version of the initial definition of the cloud presented by the NIST (Mell & Grance, 2009), which is: “a cloud is an enormous, scalable system that is always available, so customers can use its resources on an on-demand basis. It is location independent and accessible through the network. A cloud should also be easy to use, with the complexity of the underlying technology hidden from the end-user”.

2.2.1. Cloud computing characteristics and benefits in public authority environments

Due to information sensitivity, utilization of cloud computing in public authority or military environments is not a straightforward solution. The primary characteristics of cloud computing in public authority environments in general and military environments specifically are listed in Table 4.

In the systems of public authorities or government agencies, the usage of clouds is more restricted than in many other instances. When confidential content is involved, a scenario in which the consumer does not have any control over the location where the data is processed is unacceptable. Despite virtualization, data is always processed on some physical server subject to the laws of the country in which it is located. Especially in military systems, it is crucial to know at a minimum where the data is processed and what organizations and administrative authorities have access to the data.

Table 4. Cloud Computing Characteristics in a Public Authority Environment [1]

Characteristic	**Description**
Data processing	Unlimited computational capabilities and storage of the cloud enable processing of greater amounts of data.
On-demand self-service	Consumers connect to the cloud and request resources from the cloud as needed. The cloud infrastructure and services comply with consumer demands.
Security	Consumers' access to resources and data is strictly controlled, monitored and limited by access rights.
Broad network access	The cloud can be accessed over the network by standard mechanisms from any location with any kind of device.
Excessive knowledgebase	All relevant information from various sources is available to consumers at all times.
Resource pooling	The computing resources support multi-tenancy. Physical and virtual resources are dynamically assigned and reassigned according to consumers' demands. A given arbitrary consumer does not necessarily have any control over or knowledge of the exact locations of resources.
Rapid elasticity	Cloud capabilities can quickly scale in and scale out. To consumers, capabilities appear to be unlimited.
Traceability	Every action by a consumer or in a service in the cloud must be traceable.
Survivability	The cloud system must be fault tolerant. It should automatically recover to an operational state from different disaster scenarios.
Measured service	Cloud systems automatically control and optimize resources. Resource usage can be monitored, controlled and reported.

Cloud computing is claimed to be cheaper than having an on-site network system. This argument is based on the fact that an organization does not have to buy servers of its own; it simply pays for the use of resources that exist in the cloud (Kraska et al., 2009). If the organization builds its own computational infrastructure, the system must be scaled so that relatively infrequent peak loads can be processed (Armbrust et al. 2009). If an organization chooses not to underprovision their system, their hardware layer will be excessively capable. The result is that the system is expensive and will be idle most of the time. In the cloud paradigm, an organization uses the resources on an on-demand basis and can expect to always have sufficient resources. At times of peak load, the system resources in use scale up, and once the peak is over, the resources in use scale down. Scaling up does not necessarily cost any more than basic use. In the cloud, there are no costs of ownership. This is why outsourcing infrastructure to the cloud tends to be very tempting to many corporations. From the cloud resources' vendor's point of view, such scaling maximizes utilization of the physical hardware when the cloud is large and serves numerous customers. In addition, the larger the cloud, the smaller the hardware acquisition costs, and with technological homogeneity in operations, the total costs per operation are smaller than if the organization owned its own on-site hardware. This leads to cheaper vendor prices for customers.

Outlining the characteristics of cloud computing in private clouds can be accomplished by examining the overall benefits of cloud computing in private clouds. Private clouds roughly resemble private networks, with the system scaling within the system hardware. That hardware can be leased instead of owned, but multi-tenancy at the service, data, or application level is usually limited. Any savings from the decrease in total costs of ownership are indirect and enabled by better utilization of existing hardware.

The main benefits for the military lie in the usage of service-oriented architecture (SOA)-based applications on a virtualized platform, which better leverages the utilization of existing hardware. Furthermore, in private clouds, the technical homogeneity of the system improves manageability and operating costs. With standardized and consistent platforms, it is possible to develop automated maintenance routines that deliver savings over the long run.

At first glance, it seems the benefits of pay-per-use do not apply in a cloud bounded by organizational limits. However, monitored and measured resources and usage control mechanisms enable optimization of resources within an organization and guarantee service levels for individual departments or divisions.

The other benefits of cloud computing are related to the underlying technology. Homogeneity within the service layer facilitates better manageability. Service orientation and decoupling are essential features for geographic distribution of systems and resilient computing (Kim 2009).

Virtualization, distribution, and scalability improve the reliability of cloud systems and offer better fault tolerance and a solid platform for advanced disaster-recovery techniques (Brewer, 2000). Unlike on-site systems or traditional server architecture, data in the cloud is not stored on one server alone; it is distributed to multiple servers and accessed via different virtualization schemes (Kossmann et al., 2010). Fault tolerance protocols ensure that if one of the data locations is not available, the system automatically recovers from this situation. Failures are not exposed to users, who experience enhanced availability and fault tolerance (Brewer, 2000).

2.2.2. Research gap in cloud computing

The previous subchapter addressed the characteristics of cloud computing in a public-authority context. Numerous articles and blog posts have been published on technical problems and other obstacles that must be taken into consideration when adapting cloud computing to this context, and analysis of the characteristics of the context leads to the identification of certain critical limitations (Kumar, Dubey & Pandey, 2021; Linthicum 2017). These limitations are listed in **Table 5**, along with examples of corresponding measurable parameters. The limitations are grouped under the five most critical problems that must be resolved before the benefits of the paradigm can be fully exploited in operational and tactical high-security systems. **Table 5** presents the relationship between each limitation and these problems, which form a gap in the existing research.

Table 5. Characterization of limitations in a high-security environment

Limitation	Example of parameters	Research gap to be addressed
Knowledge timeliness	• Age of information • Toleration limits for age of information	Knowledge management
Knowledge correctness	• Error margin of information	
Knowledge reliability	• Probability of incorrect information	
Latency for computation	• Bandwidth • Data size • Amount of computing nodes • Service propagation • Computational variables (MIPS, processors) • Utilization of services	Capability limitations in private clouds
Latency for service	• Availability of services • Idle time of services • Service propagation	
Fault tolerance	• Usability • Recovery time • Downtime / month	Fault tolerance and disaster recovery
Complexity of the cloud	• Number of layers • Number of vendors • Number of interfaces in architectural topology	Complexity of virtualization

Authorization	• Number of logical interfaces • Number of users • Number of user roles • Number of different device types • Number of computing nodes, networks, vendors	Security issues

2.3. Theory: Vulnerability analysis

This dissertation relies on vulnerability analysis to determine the security level of a proposed solution. Vulnerability analysis or vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Modeling the critical infrastructure and identifying the most severe vulnerabilities are key tasks for the authorities responsible for national security. One motivation behind vulnerability analysis is to have a measurable approach to policy-making. It answers the question of which components should be made more resilient to attacks and determines the probability of a successful attack on a component. The combination of component vulnerabilities and attack probability makes it possible to quantitatively evaluate the vulnerability of a sector. And yet the analysis is only as comprehensive as the model.

Much research has been conducted on attack, vulnerability, and computer security risk analysis. Some studies are based on network specifications (Hariri et al. 2003; Jajodia, Noel & O'Berry, 2005; Li, Yang & Xie, 2015; Zeng & Xiao, 2015), some rely on graph representations (Hariri et al., 2003; Jenelius & Mattsson, 2015; Lv et al., 2013) and perhaps the most popular approach is utilizing tree constructions, like attack trees or fault trees (Hariri et al., 2003; Fung et al., 2005; Fung & Hung, 2005; Kumar & Singh, 2015; Bozdag et al., 2015; Straub & Traylor, 2018). Vulnerability analysis is closely related to survivability analysis and research (Mead et al., 2000; Moore, Ellison & Linger, 2001; Cardoso et al., 2001). There are also more comprehensive approaches that combine several methodologies, like model-based vulnerability and a risk analysis method for critical societal infrastructure, like the approach presented by Lewis (2006). It makes use of network modeling as well as fault tree analysis. Instead of analyzing the system environment of the components, data contents can be approached via dynamic taint analysis (DTA) (Newsome & Song, 2005; Kand et al., 2011; Adrian & Cheney, 2015). This is an extremely powerful method for detecting vulnerabilities in applications, like the one Herrera presented for Java malware (Adrian & Cheney, 2015).

Critical infrastructure has a long history of vulnerability assessment and risk management methodologies, as described in the following examples. Ferreira (2019) presents a model that considers risk assessment from the perspectives of assets, threats, and vulnerabilities. The model focuses on the kinetic impact of an attack, and the value of a target is evaluated both from the aggressor's and the user's points of view. Using Ferreira's model for ICT system assessment would be difficult, since the actual structure of the system is not considered, only the system as a whole. In addition, the information loss from the system would not be considered in Ferreira's model.

In his model for critical infrastructure sites, Baker (2005) proposed using a threat–system matrix to prioritize and rank system vulnerabilities. The matrix presents the impact a certain threat poses on specific component in an accessible manner. However, the model does not consider dependencies between threats or system components. This discrete approach to the elements considered in the model means mitigating complex failures or advanced attacks would require additional measures. In a subsequent study, Onwubiko C. and Onwubiko A. (2019) propose modelling of cyber security return of investment (ROI). The study introduces key perform indicators that could be used to calculate the cost of the investment. The KPIs address enhancements at both the individual and system levels as well at the government and community levels. The model does not account for the value of the actual system to be protected, which should be a starting point in all investment decisions.

In this dissertation, the approach presented by Lewis (2006) is adopted as a starting point for vulnerability assessment and business resilience determination, due to its scalability from critical network infrastructure to an individual system component. Its simplicity and practicality allow for additional methodologies and tools to enhance the generated risk-assurance level.

The main steps of model-based vulnerability analysis and risk analysis are (Lewis, 2006):

1. Listing of assets. Identifying all the components of the system.
2. Network analysis. Categorizing and analyzing relationships between the components. Identifying the most critical component.
3. Fault tree analysis. Building a tree representation of the vulnerabilities to create a fault or failure in a component. With vulnerability probabilities, the likelihood of failure occurring in a component can be estimated.
4. Event tree analysis. The outputs of the previous step are input into an event tree. The event tree contains all possible events obtained by single and multiple combinations of faults. With this step, assurance of all relevant vulnerabilities is enhanced.
5. Event matrix analysis. The number of processed events can be reduced using an event matrix, by enumerating the single and double faults in the event tree.
6. Risk assessment and resource allocation. Determining optimal allocation for funding to improve component resistance to vulnerabilities.

In Lewis' approach, each system component is identified, along with any possible faults and threats to that component. A component is listed if the possibility of threat to that component multiplies during a single attack. This possible multiplication of threats is processed using event matrix analysis, which treats all threats as equal: they are distinguished by the probability of occurrence, not the severity of possible damage (Lewis, 2006). Lewis (2006) presents a method for determining the costs of improving security with a relative percentage per single threat, but it considers reduction in attack probability for only one component at time.

When extrapolating these models from a traditional critical infrastructure environment to network-based high-security ICT systems, the sensitivity of the information and knowledge stored in the system must be considered. As the Finnish Security and Intelligence Service states in its 2019 national security review, cyber espionage is active and emerging (Finnish Security and Intelligence Service, 2019). The targets of cyber espionage vary from public administration information to businesses' key R&D information and individuals' confidential communications (Finnish Security and Intelligence Service, 2019; Stubbs, Menn & Bing, 2019). Sometimes cyber espionage is difficult to distinguish from cybercrime, hacktivism, or military activities, since all aggressors use similar attack vectors (Klimburg, 2012). However, from the business resilience perspective, cyber espionage has a potentially huge impact in the form of losses based on immaterial properties, business advantage, and/or any sensitive business-critical information.

As stated before, vulnerability analysis has been widely used in military contexts to identify vulnerable targets and the preventive action that can be taken against threats (FDF, 2021). Process management already exists for it, as does the system software to support it. In dynamic, high-security environments, it is a tool to improve awareness of security levels.

2.3.1. Research gap in vulnerability analysis

Past vulnerability assessment or risk management methodologies have generally been created for a specific purpose or domain, which results in a narrow perspective. Those models that assess and quantify cyberspace-related threats, vulnerabilities, and risks do not consider business resilience, the gain-loss calculation of enhancements, or the costs to survivable operations (Giannopoulos, Filippini & Schimmer, 2012). A similarly narrow approach characterizes the business resilience models presented in literature from the business domain. Discussions of business resilience tend to be limited to economic or management features of business continuity (see, e.g., Vargas, & González, 2016; Morisse & Prigge, 2017). There is no extensive consideration of threats, immaterial losses, or cyberspace-related vulnerabilities (Onwubiko C. and Onwubiko A., 2019).

Table 6 presents the limitations of existing models in assessing vulnerability, risk, and business resilience and lists the corresponding research gap that needs to be addressed.

Table 6. Limitations of existing vulnerability, risk, and business-resilience assessment models

Limitations / deficiencies of current models	**Research gap to be addressed**
Models limited to a certain purpose, domain, or function and/or partial assessment	A comprehensive model that contains the following assessments: • Threats • Vulnerabilities • Risks • Business resilience
Business resilience has a cyber–physical nature	Lacks in resilience improvements: • the operative continuum • the business continuum in the short and long terms • reputation
Industrial espionage has increased significantly and should be taken into consideration in models	Protection of immaterial assets and determining cost-benefit ratio.
In theory, malicious actors have unlimited resources	The protective mechanisms against persistent advanced threats.
The result of the model becomes obsolete immediately after model execution	Security-level changes needs to be analyzed in real time

2.4. Theory: Trust management

This chapter presents a brief overview of concepts and technologies key to the field of trust management.

The definition of trust presented by Grandison and Sloman (2002) is used in this dissertation because it is both simple and sufficiently comprehensive: according to them, trust is a quantified belief by a trustor with respect to the competence, honesty, security, and dependability of a trustee within a specified context (Grandison & Sloman, 2002). And as the key focus of the dissertation is computative trust management, a characterization of this concept is also in order: widely accepted features of computative trust management include subjectivity, expected probability, and relevance (Abdul-Rahman & Hailes, 1997; Zhou et al., 2011).

In a high-security environment, trustworthiness between stakeholders is generally recognized, due to mutual respect for the other's profession and officiality in general. Within this context of collaboration and cooperation, the participating authorities compose a virtual community made up solely of trusted parties (Grandison & Sloman, 2002). This sort of consortium can be called a Circle of Trust, and within that Circle, each participant shares information in a way that helps other participants improve operational success. This theoretically enhances the overall performance of the virtual community to the benefit of all participants.

A Circle of Trust can be considered a virtual community. In this sense, it resembles the knots investigated by Gal-Oz et al. (Gal-Oz, Gudes & Hendler 2008). A knot is defined as a subset of community members identified as having relations of strong mutual trust, either directly due to a trust model or indirectly via transitive trust. As a result, the members of a knot can rely on each other's recommendations even if they do not rely on the same experts. The Gal-Oz knot model emphasizes symmetry of trust and lacks a mechanism for weighted trust relations, which is a way of quantifying distrust within a Circle of Trust. Trust may vary based on whether an actor is the recipient or sender of information or other factors, and as a result, trust between actors is not necessarily symmetrical. The reality is one actor may have to rely on information supplied by another actor even if they suspect the information is not of high quality and may or may not be the best that can be provided by the provider. Asymmetric situations of this nature occur when the trading actors have divergent capabilities in terms of providing and testing the reliability of the transmitted data. Technically stronger and more capable actors with more resources can use deception in information sharing and still demand full accuracy and information of the highest quality in return (JP 3-13.4., 2012). In short, trust varies between actors within the context of a Circle of Trust.

Jøsang and Pope (2005) have published several papers in which they discuss the features and possibilities of trust transitivity. Their research offers a potential platform for enhancements to a Circle of Trust, suggesting transitivity be limited by a threshold achieved through the chaining of weighted arcs. This does not negate the fact that the first recipient owns the received data after interpretation. And as the trust transitivity method needs an external broker to control the threshold of the chained arcs, it is potentially vulnerable to data exposure.

Chen et al. (2008) have published a methodology in which the attributes of trust are delegated to subjective trust evaluation. This approach considers aspects of distrust and includes a mechanism for avoiding data exposure independent of trust values. Delegation of attributes and building a global trust map can quantify the accumulation problem and, at minimum, increase knowledge of leaked and possibly accumulated information. It also solves the problem of collateral damage resulting from deception, because the trust values can prevent an actor from sending distrusted information via trusted arcs. The collateral damage of deception is described in more detail in chapter 2.4.3.

To ensure persistent operations, it is essential that the maintenance of a subjective trust map or similar registry of trust relations be continuous. This can be computationally challenging. Xia et al. (2011) have worked on a subjective trust model based on fuzzy logic algorithms that helps determine which subjective information is relevant to each node.

Trust is by definition subjective. Gal-Oz et al. present the idea of subjectivity as a consideration in defining the relationship of the parties involved in information transfer (Gal-Oz, Yahalom & Gudes, 2011). In other words, the recipient of the information acknowledges the relationship of sender to recipient, and this relationship is limited to their roles in a specific context, which enables judging of the trust metrics of the other nodes according to expertise or some other aspect. The basic principle is that a change in role or other aspect might impact a change in subjectivity and preferences as well as the ability to evaluate trust in the other nodes.

2.4.1. Trust management in a public authority environment

While concepts like semantic knowledge processing, connectivity, and social networking enable improved cooperation between government authorities, they also present new challenges. Openness can be hard to manage in a highly secure environment. As mentioned before, the processing and sharing of critical operative information increases hostile interest in a system environment.

One special case of information sharing is the delegation of operative situational data to improve situation awareness within the Circle of Trust. Such collaboration improves the accuracy of each actor's individual awareness and enhances the awareness of all actors involved in the operation (Courtney, 2017; NCSC-FI, 2021; Tolga, 2019; US White House, 2017). This cooperation enables better communications, safer procedures, and more effective actions in operations for all of the authority organizations participating in the Circle of Trust.

The potential and possible utilizations of situation awareness have increased alongside technical evolution. Sensors and mobile devices increase the effectiveness of data collection from locations that traditionally have been difficult to access. More data can be collected and stored than previously, facilitating the creation of a view of a situation that is more truthful, accurate, and comprehensive.

Most of the acute challenges in improving situation awareness are related to the refinement of significant information from within huge amounts of data, unstable data transfer connections, and especially in field operations, limited data capacities. And as mentioned before, data correctness, reliability, redundancy, and timeliness have also been discussed in several publications. Less consideration has been given to evaluation of the trustworthiness of data sources or the security issues involved in delegating situational data to recipients of varying trust levels. This aspect is relevant in high-security environments, where there is always the possibility of a malicious actor receiving confidential information or sending unreliable data to influence a decision-making process (Rohith & Batth, 2019; Tolga 2019).

In high-security contexts, the participants in the trust relationship are bound to a role. A participant represents some actor or unit within an organization, and the unit has a task, a goal, and special expertise specified by the organization. In this environment, two interacting actors from different units trust each other's represented role, not necessarily the other actor itself. Yet the trustworthiness between two roles can be fixed at the process level, and the individual actor might have specific preferences, interests, or experience that affect quantitative trust. Similarly, data providers such as sensors can be modeled as actors within a trust relationship and represented by the ownership of an organizational unit.

2.4.2. Circle of Trust benefits in high-security environments

In the scope of this research, a Circle of Trust is defined as a consortium focused on a specific subject and solely made up of trusted parties. This means each participant has a sufficient amount of trust in the other participants in relation to the subject. In this context, "sufficient trust" can be characterized as a readiness to deliver and receive knowledge unconditionally without risking the participant's own operative ability. The motivation for creating the consortium is to construct a united force to gain improved capability in operations aimed at a unified goal (Hulme, 2017). To achieve this, it is essential to have an open, transparent exchange of information between participants, and in order for the circle to be sustained, all participants should benefit directly or indirectly from collaboration and mutual cooperation. The participants rely on being able to gain operative advantages from participation in the Circle. Such advantages could include, for instance, improved efficiency in operative actions or overall reduction of operative costs. In practice, this interaction could take the form of sharing situational information among participants. Moreover, it has been argued that a Circle of Trust formed by bringing together the public authorities from different countries offers the only real possibility for improving situation awareness in order to operate successfully in cyber warfare or similar hostile events. Large malicious actions undertaken as cyber-attacks are always conducted at the international level, and routing often conceals the origins of the actor (Morgan, 2021). Determining the actor requires international collaboration based on openness of information, and defending against malicious actions at the national level can be only reactive in nature, which is why countermeasures are only effective when conducted at the international level (Hulme, 2017). The information collected by an international consortium can help identify the existence of malicious actors and detect false information in the attacked systems.

An example of a Circle of Trust is illustrated in **Figure 4**. In the figure, *A* represents a situational information provider, while *B* and *C* are recipients of the information. The arrows represent the direction of information flow. Because theoretically information trading should take place in both directions, arrows are also drawn from recipient to provider. Each arrow contains two parameters: *s* for the situational information and *w* for the weighted trust between the information provider and recipient. Note that if, for example, $w_{ake} \neq w_{AB}$ then $s_{AC} \neq s_{AB}$. In practice this means that the situational information provided by the provider to each recipient is not the same unless the trust relationship between the provider and each recipient is exactly the same. Also note that the trustworthiness of the recipient is in direct relation to the correctness and completeness of the situational information provided by the information provider.

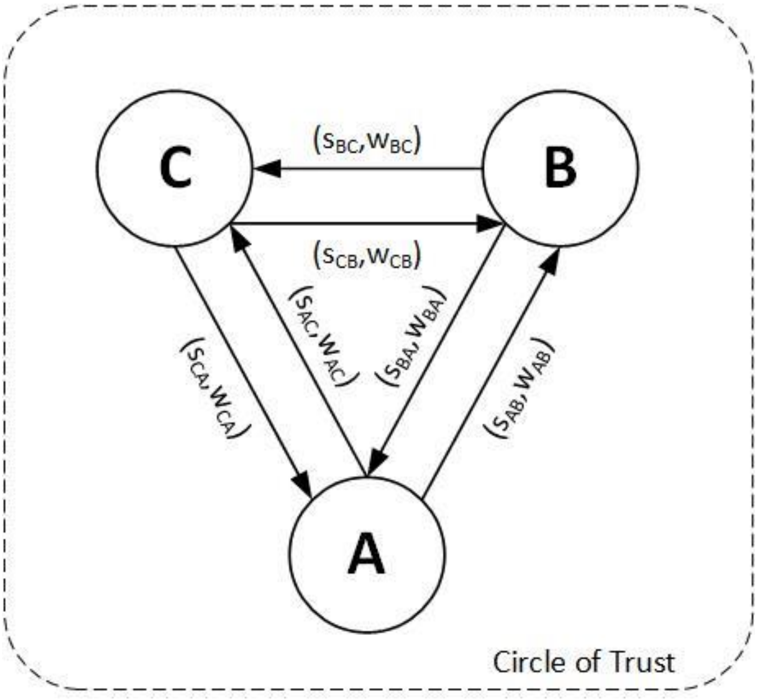


Figure 4. Circle of Trust

As stated before, a Circle of Trust allows the improving of situation awareness through the trade of intelligence and reconnaissance information among Circle participants. This trade generally takes the form of mutual sharing in which the quality and amount of traded information are in equilibrium among participants (Prunckun, 2019).

Trading can also be used to identify possible leakages (Prunckun, 2019). If a member of the Circle is suspected of being a malicious actor, labeling or watermarking information makes it possible to trace the flow of information and, thus, to detect and identify the source of the leakage. If there is certainty regarding an intrusion into system, a Circle of Trust makes it possible to feed deceptive information to the malicious actor without breaking routines or disconnecting the actor from the grid too soon (Jaafar & al. 2020; JP 3-13.4., 2012). Moreover, the capabilities of the hostile actor can be monitored and evaluated by observing the actions they perform within the controlled environment (Handel, 1982; FDF, 2021).

A Circle of Trust is a generic, scalable concept. On an international scale, we can consider military alliances such as NATO as an example of a Circle of Trust (Bajerová, 2017). On a national scale, examples can be found in the collaboration between public authorities, such as between the police force and aid and rescue services. At an organizational level, a ministry such as the Ministry of the Interior and the agencies it supervises can form a Circle, as can the supply chain of a financial ecosystem. At the technological level, all nodes in a high-security network form a definite Circle of Trust.

2.4.3. Challenges in information sharing

The Circle of Trust concept has its challenges. The Circle should enable openness of information exchange, but this openness also increases the risk of revealing too much sensitive information to the public.

Situational data inherently contains some information about the collector or origins of the data. This information can relate to location information, resources, or capability (FSB, 2020; Klimburg, 2012). It can also be used against the originator. Revealing information is always a risk, and information delivery should be controlled in some manner so that information, knowledge, or capabilities are not leaked to hostile or untrusted recipients (Prunckun, 2019; FDF, 2021).

Absolute trust does not exist in reality

Within a closed Circle of Trust, some parties are always more trustworthy than others. For example, in a military alliance, some nations cooperate more deeply than others and some nations may have doubts about others due to historical factors. In other words, the existence of sufficient trust can vary significantly among actors, with the consequence that the participants in the Circle of Trust do not exhibit equal levels of trust in all other participants. In public authorities, trust within one's own organization is usually unreserved. This trust is based on shared experience, common procedures, and a sense of professional community. It is much more difficult to trust another authority or a different organization. We can find this element of distrust at each level of the Circle of Trust concept. The main concern is the leakage of sensitive information, as illustrated in **Figure 5** (Prunckun, 2019). After revealing information to recipient *C*, the supplier *A* is no longer able to manage the revealed information. If *C* has a connection to party *D*, *C* may provide information to *D,* even though it does not belong to the Circle of Trust. Assuming that *A* is the only information source, *D* will receive information $s_{CD} \subseteq s_{AC}$.

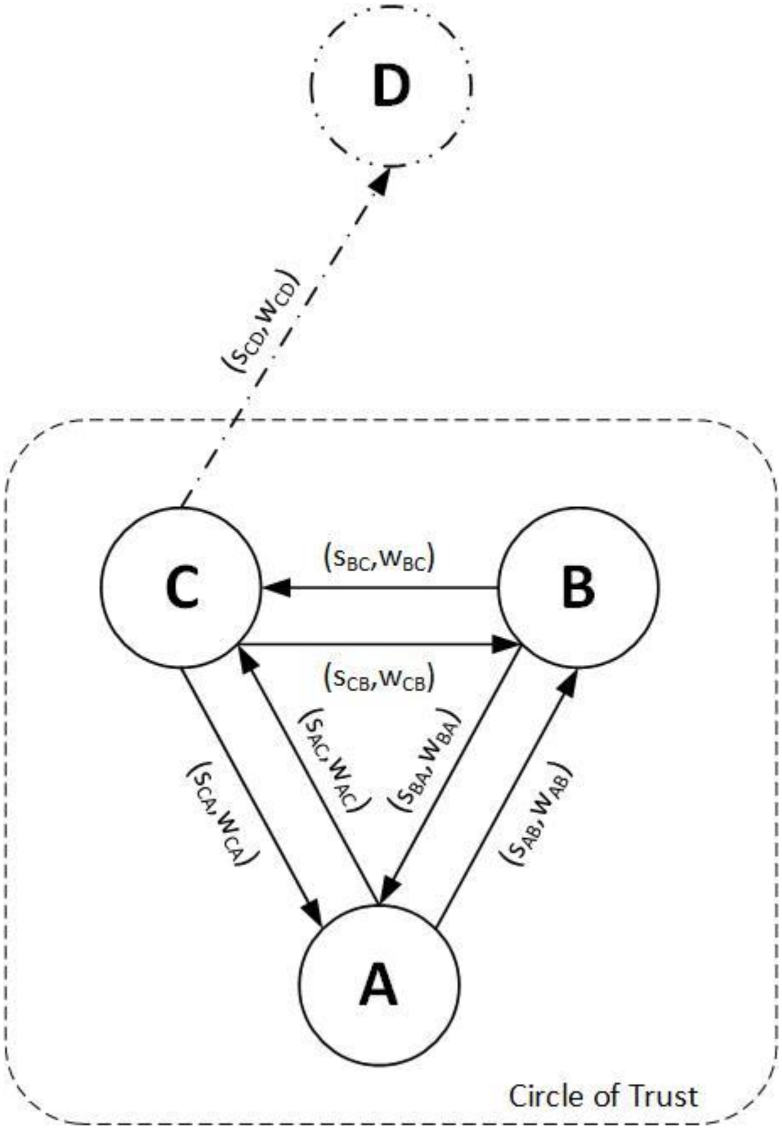


Figure 5. Leakage of information

Another dimension of this challenge is the publicness of distrust: in other words, if one actor is not ready to release all information unconditionally to all other actors even though it is bound to the principle of openness within the Circle, how publicly can these limitations on the information released be introduced and maintained.

Managing information sharing in an open network

Leakage of information was raised in the previous section. Regardless of how much or how little a party trusts its allies, the information they provide may be necessary. The usual convention is that, in order to receive information from other parties, one must give or send information one has collected. This actually forms a trading system in which tradable information is defined by its usefulness, timeliness, trustworthiness, accuracy, and comprehension. As previously noted, absolute trust does not exist in reality. A Circle of Trust or any alliance is an attempt to form a framework in which the agreed level of information quality is established in writing and the parties can at least rely on the exchange of information taking place. In the role of information provider, the parties try to minimize the amount of information sent while hoping to receive the maximum amount of information in return. The recipients' primary goal is to have a sufficient amount of information to form situation awareness with regard to a specific set of circumstances. The question is: what amount of information provision is sufficient to achieve that goal?

Another issue arises when information is sent to the recipient. After transmitting information, the provider loses all control over that information. Conversely, when the receiver has interpreted the received information, they immediately own the information and can use it for any purpose they deem necessary, including sending the information to parties not trusted by or simply not intended by the original source. Having a secured connection does not resolve this issue, as the received information is presented in a decrypted form.

Accumulation of information can also be a problem, as illustrated in
Figure 6. If A sends information fragment s_{AB} to recipient B and information fragment s_{AC} to recipient C, it is possible that both recipients B and C send on these information fragments on the less-trustworthy party D. D may then combine information fragments $s_{AB} \cup s_{AC}$ and create a more comprehensive situation awareness that indirectly poses an increased risk for the originator A.

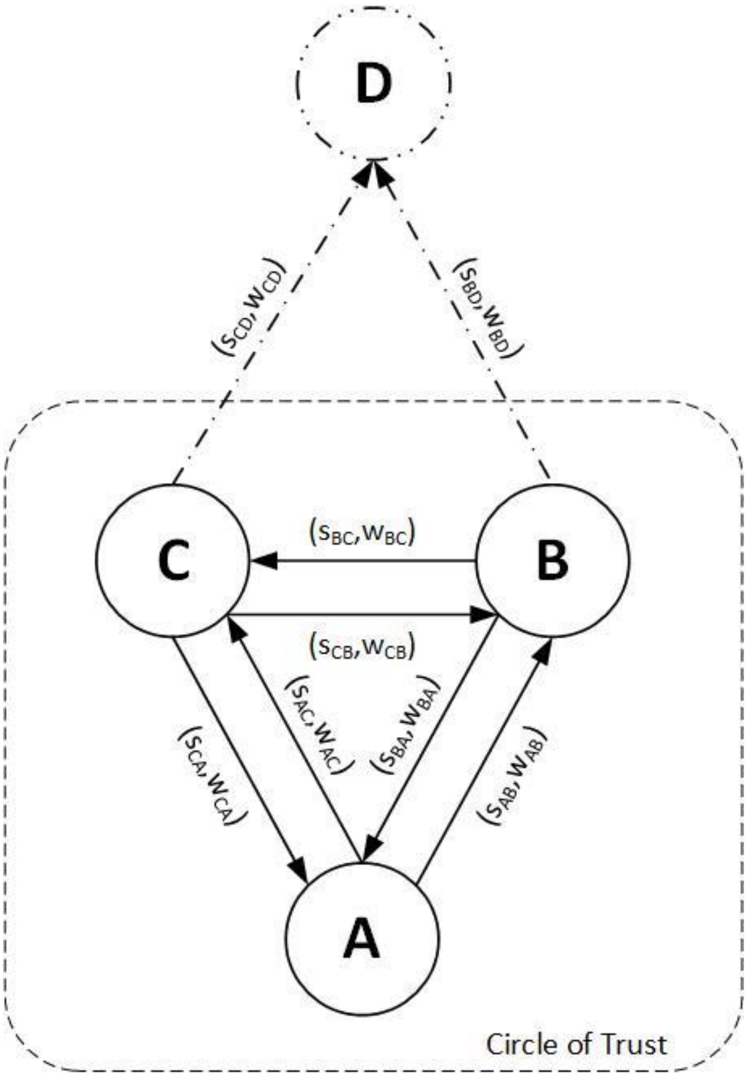


Figure 6. Accumulation of information

Collateral damage of deception

Previously we described the possibility of deception using the example of an identified intrusion into a secure environment (JP 3-13.4., 2012). The challenge is how to notify the other participants in the Circle of the intrusion without risking that this information reaches the intruder. This problem setting is formalized in **Figure 7**, in which A has some distrust in C (i.e. w_{AC} is small) and decides to send them false information s_{AC}. At the same time, C and B have a strong trust relationship (i.e. w_{BC} and w_{CB} are large) and A and B also trust each other. If C transmits the information s_{AC} as s_{CB}, B receives false information, which might be very harmful not only for B but for A as well. After exposure of the deception, the trust weight w_{BA} is likely to decline, which can influence the future exchange of information and equilibrium of that trading relationship.

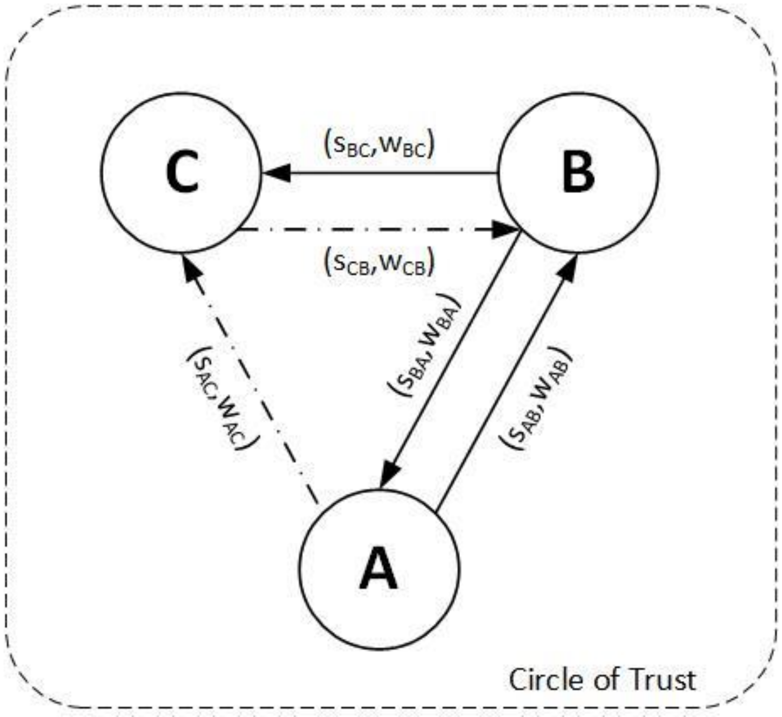


Figure 7. Collateral damage of deception

A special case occurs when one participant in the Circle of Trust identifies an intruder within the Circle. If the other participants are not trustworthy enough to be informed about the intruder and deceptive data is fed to the intruder, how can the other participants be notified not to trust information they receive from the intruder?

This special case in ensuring correctness becomes more important when considering a threat where some malicious actor inserts false information into an operative decision-making process. In this instance, the aim of the perpetrator is to have influence on the decision itself and the environment around it. The impact on various sources of information will affect the corresponding decision-making processes. When a single sensor is being disruptive, the data receiver can easily detect failure in the data feed. Detection is much more difficult if the sensor starts infrequently sending abnormal values, metrics or information. Yet it is even more challenging to detect data that is almost correct when similar results are provided by a large number of sensors. A situation like this can occur if several sensors are occupied by a hostile actor, as in the Sybil attack presented by Douceur (2002). Such scenarios can have impacts of enormous significance. For example, the modification of temperature values from a region can have an impact on the decision to limit the use of some technical equipment. In military operations, this can give a significant advantage to the opponent (Prunckun, 2019). Similarly, most technical equipment is vulnerable in extreme weather conditions.

2.4.4. Research gap in trust management

The problems addressed in the previous subchapters are summarized in **Table 7** along with the corresponding research gap to be addressed. The purpose is to outline trust management research in terms of overcoming the obstacles presented in **Table 7**. The research gaps are limited to a Circle of Trust representing a high-security public authority context. One distinctive feature of such a Circle of Trust is the paradoxical nature of the parties' willingness to share information: when it comes to knowledge that creates simultaneous situation awareness, all participants within the Circle

- are keen to receive information from each other despite some inaccuracies
- are forced to share information in order to ensure future information in return from others
- do not want to share overly detailed information or expose their own capabilities
- trust some participants more than others
- are afraid that some malicious actor will receive sensitive information.

Table 7. Information-sharing limitations in the existing research

Limitations / deficiencies of current models	**Research gap to be addressed**
Absolute trust does not exist in reality	Theory for controlling leakage of information
Managing information sharing in an open network	Theory for preventing accumulation of information
Preventing collateral damage of deception	Management scheme for shared misinformation

2.5. Theory: Blockchain technology

The aim of this dissertation is to create a trustworthy system for information sharing in high-security environments. The previous chapter introduced the theory of trust management and addressed challenges in information sharing. With regard to actual sharing platforms, new technologies have emerged that utilize cryptography and promise to maintain absolute integrity and consistency. One prominent technology, blockchain utilizes the decentralized management of assets and ensures the consistency of information by encrypting transactions with previous states of information. Information management and consistency are solved by miners, who verify the correctness of the system and the final states of the information and receive a small fee for their efforts (Nakamoto, 2008; Bitcoin, 2009).

The most famous implementation of blockchain technology is the Bitcoin system. Bitcoin is a cryptocurrency without any centralized management or issuer, such as a bank (Nakamoto, 2008). All participating nodes in the Bitcoin system have information on all accounts in the system and are responsible for ensuring the correctness of account balances. Accounts are anonymized, but the contents and the transactions are public. If some amount of the Bitcoin currency is to be transferred to another account, a transaction entry is created including the previous addresses of the currency, the amount of currency and the recipient address. This entry is encrypted and delegated to the system nodes to be verified, validated, and committed. System nodes that commit the transactions are called miners and receive Bitcoin currency as a reward (Nakamoto, 2008). This work increases the amount of currency in the Bitcoin financial system, ensuring its growth.

The Bitcoin success story has inspired several other areas of application that could harness a similar technology. Bitcoin implementation has some limitations, such as scripting and a lack of meta-protocols (Buterin, 2020). There is also a need for transferring agreements between stakeholders in a more comprehensive manner. Ethereum is one project that addresses these limitations by introducing an abstraction layer on top of the basic blockchain platform (Buterin, 2020). The layer contains a built-in Turing-complete programming language that ensures more complex systems can be implemented. In Ethereum, contracts can have data, conditions, and operations and, like functions, can return a value. Another interesting feature is that a contract itself can create another contract, and the role of this created contract within the system can differ from the originating contract. This allows the implementation of more sophisticated systems, such as escrow management, reputation management, identity management, or gambling applications in which a third party is needed to guarantee the agreement between the contracting parties (Buterin, 2020; Stajano & Clayton, 2011).

Within the scope of this dissertation, blockchain technology is used as an enabler. With its programmable smart contracts, the Ethereum platform provides a comprehensive platform that ensures the deniability of transactions, traceability, reliability and a trustworthy system. Relying on techniques similar to those used in escrow and gambling applications, the anonymity of the information source can be maintained while sustaining trust in the overall system.

3

METHODOLOGY

Achieving the ultimate aims of this dissertation as described in Research purpose (Chapter 1.1), requires the examination of a range of areas and concepts. Multidisciplinary research of this nature demands a methodology that will support its complexity. It is essential that, despite varying approaches to research objectives, each research phase be coherent and constructive and support the progression of results. For these reasons, a hermeneutical approach was selected as the primary research methodology for this dissertation, supplemented by qualitative research (Niiniluoto 1980).

In a hermeneutical approach, understanding of the subject of research increases as the research progresses. The approach can be described as a spiral, in which individual results support each other and build comprehension incrementally (Siljander 1988).

One feature of a hermeneutical methodology is that interpretations and concepts remain in flux; the study can be modified and improved as it progresses. This is a very useful approach in military contexts, where limitations exist in the executing of real-life experiments and the validating of research results (Lappalainen, Jormakka 2004). It also enables the possibility of proceeding on to another research objective even when results are not comprehensive, because future research can lead to the validation, completion, or discarding of previous results.

Consequently, a variety of methods were applied to explore the various dimensions of the dissertation research. A summary of these methods is provided in Table 8. The results from the completion of each partial problem provided the basis for the subsequent studies in an iterative manner, and deductive reasoning was used to transfer each problem definition to the subsequent studies. This approach enhanced and validated the research as a whole as it progressed from one phase to the next.

The investigation of each partial problem began with a literature review that created a theoretical foundation for the resulting findings. These theoretical foundations were initially developed for non-military or non-high-security contexts, which is why a gap analysis of applicability was required for Articles [1], [2], [3], and [6]. As this dissertation involves numerous scientific domains and aims at multi-disciplinary solutions, the literature review presented at the beginning of each article was relatively extensive. In addition to introducing concepts and establishing the theoretical background, the literature review sought theoretical links between domains. This approach helped pinpoint the relevant aspects of various theoretical approaches, exposing research gaps and creating continuity and coherence within the research.

As mentioned above, in terms of conceptual review, the method of analysis applied in all articles was primarily qualitative. In Articles [1], [2], and [3], quantitative data was extracted from existing commercial computing systems and complemented with requirements outlined in the common high-security guidelines established by the Finnish government in VAHTI 2016, KATAKRI 2011, and the High-Readiness Network (VAHTI, 2016; KATAKRI, 2011; TUVE). Access to the material used in Article [3] was limited due to its classification as restricted by both commerce and government. In Articles [4] and [5], mathematical analyses were conducted to improve the proposed models based on empirical observations of the phenomena being studied. The base models were initially approximations for solving the problem presented or adapted from a different domain and finalized based on observations from ICT production systems [5], [6] or on the feedback received from stakeholder systems (e.g. insurance companies in [4]). In Article [4], the dimensions of topical threats were summarized in the results of a cyber-security survey conducted by the Finnish Transport and Communications Agency (Finnish Cyber Security Center 2014). In order to apply a business-resilience model that had already been developed, an algorithm for real-time security-level monitoring was also produced for Article [4]. The primary function of the algorithm was to examine whether real-time monitoring of security levels is feasible based on a mathematical model. In this instance, a persuasive methodology based on practical arguments supported by analysis, evaluation, and experience was used to determine feasibility (Kelly, 1980; Shaw, 2003).

Table 8. Summary of research methods by article

Research Method	**Article [1]**	**Article [2]**	**Article [3]**	**Article [4]**	**Article [5]**	**Article [6]**
Conceptual analysis	x	x	x	x	x	x
Interview					x	
Document analysis	x	x	x	x	x	x
Mathematical analysis				x	x	x
Case studies			x		x	x
Simulation						x

In Article [5], an interview was used as a supplementary data source to complement the public information available on two case studies. This approach was a necessity, because the information discussed was highly classified from the perspectives of business secrecy and/or national security. The interviewee was selected based on expertise in the subject matter, knowledge of the cases discussed, and the interviewee's role as an authorized spokesperson for the organization. Applying the observations gleaned from these case studies, the model created for Article [4] was then expanded into the enhanced threat assessment model presented in Article [5]. Although the classified status of the cases and the restrictions this imposed on discussion were limitations, the results were too important to be bypassed. Furthermore, it was clear from the start that the validity and the reliability of the results would be revealed to the public at a later time.

In Article [6], a conceptual analysis of information sharing was conducted for a logical architecture that utilized blockchain technology and smart contracts. The evaluation compared this solution to more traditional, virtual private network (VPN)-based point-to-point (P2P) information transfer. Part of the logical system architecture, the information-sharing monitoring service, was presented. Algorithms for maintaining trust and monitoring the balance of information-sharing among stakeholders were implemented and then simulated using artificially constructed test data that mimicked various scenarios. More details from the implementation and test scenarios are described in the following subchapter. A multi-strategy approach was adopted in conducting the research for Article [6]. Qualitative dimensions, such as the objectives of maintaining trustworthiness, were combined with quantitative dimensions, such as the algorithm monitoring the balance of information shared among stakeholders (Bryman, 2006). This approach ensured a functional solution from both the user perspective and the computational perspective.

Due to the high security requirements and low number of actual implementations, it proved difficult to obtain sufficient objective data across the studies. In order to overcome this hurdle, a gap analysis utilizing data from large-scale commercial environments was conducted, and results were cross-checked with the results of the corresponding research.

3.1. Simulation for Determining Trade Balance of Shared Information

As noted in the previous chapter, trade balance monitoring algorithms were defined and implemented. The algorithms themselves are described in greater detail in 4.3. This chapter focuses on the simulation and evaluation of the developed algorithm. Restricted access to the Python source codes and test data is available at BitBucket (Zaerens 2021).

The trade-balance monitoring algorithms are based on the number of sent and received messages from each system counterpart and the trust value of those counterparts from a system perspective. Moreover, the algorithm takes into consideration whether a stakeholder prefers to limit the delivery or the details of the information within the system. For those messages that a counterpart receives from the system, a feedback value is returned to the system, indicating the relevance, accuracy, and quality of the information received.

This trade-balance monitoring algorithm was tested through simulation to observe what happens when the number of messages increases. Table 9 presents various basic simulation scenarios, quantities of messages, and quantities of stakeholders. A test set generator tool was developed to create the scenarios. The test set was generated using a Round Robin algorithm in which all stakeholders share same number of messages via the system unless otherwise specified by the scenario.

Table 9. Simulation scenarios for trade-balance algorithms

Scenario ID	**Number of stakeholders**	**Number of simulated messages**	**Description of simulation scenario**
1	4	1,000	Fully random test set.
2	4	1,000	Statistically directed test set with accuracy mode set to 85 %.
3	4	1,000	Basic "happy case" scenario (i.e., the stakeholders trust each other).
4	4	10,000	Scenario where recipients give negative feedback on received messages.
5	4	10,000	Scenario where senders deliberately limit the details of information sent.
6	4	10,000	Random large set.
7	4	10,000	Scenario for testing information leakage. One recipient deliberately receives less detailed information.
8	4	10,000	Scenario for testing accumulation of information.

For each scenario at least four test sets were created in order to observe repetitiveness and to eliminate flaws in the test material or the algorithms.

4

PRIMARY RESULTS AND DISCUSSION

The key research results are covered in this chapter. Presented by research objective, they are discussed in terms of significance with regard to the objective in question. The discussion includes an evaluation of the validity and reliability of the research approach and results.

4.1. Utilizing cloud computing in a high-security environment

Research question 1, "What are the security and other key related implications of adopting a cloud computing paradigm in an environment containing sensitive information, and what new functions are needed to ensure the confidentiality of operations and information?" was addressed in the first three articles. The first two articles examined the benefits of cloud computing in high-security environments containing sensitive information, with the first Article [1] concentrating on military contexts specifically and the second expanding the examination to public-authority environments in general. In the latter, the environment was extended to include multiple stakeholder organizations, which brought increased complexity to the overall technological architecture. Extending the examination to a broader context increased the applicability of results in high-security environments in general.

Based on the key characteristics of cloud computing, five main obstacles to utilizing the technology in high-security systems were identified: support for knowledge management, limitations on computational capability, complexity of virtualization, fault tolerance, and security.

As a solution to these challenges, a new service model called Knowledge Management as a Service (KmaaS) was proposed (see Figure 8). The benefits of this model include prioritized data, improved fault tolerance, improved management for virtualization, and more advanced security measures. The second Article [2] extended and deepened the description of the technical architecture of a fault-tolerant cloud computing environment and then presented the logical approach to dynamic security-environment management. This work continued in the third Article [3], which described the fundamentals of dynamically incremental security zones and listed the most essential features to be considered in implementation.

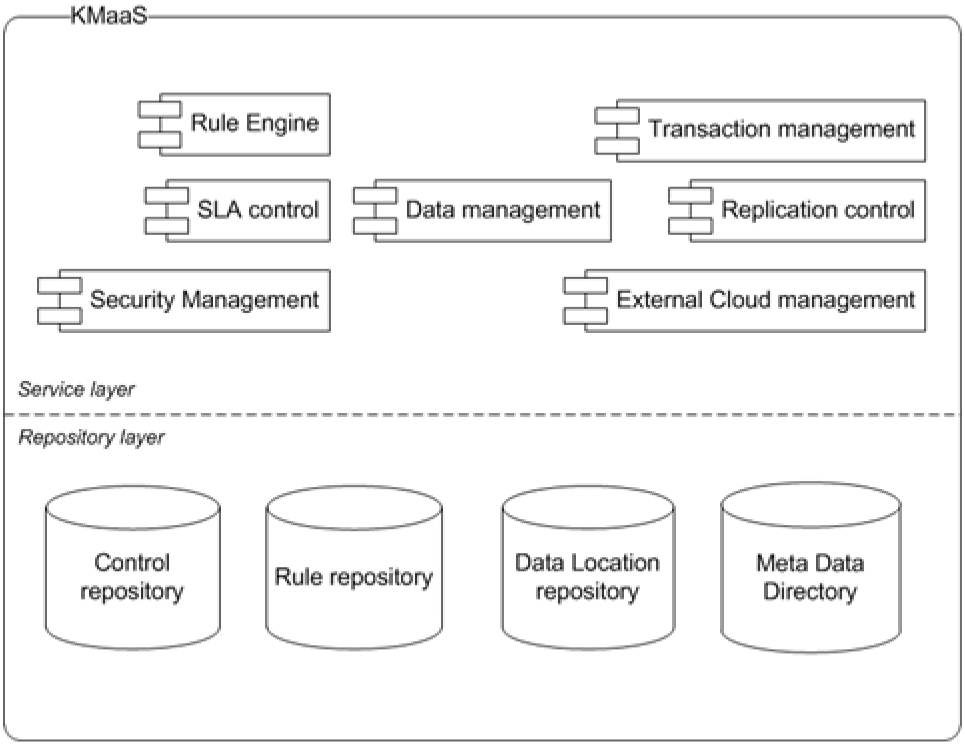


Figure 8. Logical architecture of Knowledge Management as a Service

The most essential finding from the early phase of the research was the description of a secure environment that ensures computational capability for authorities for as low a cost as possible. Furthermore, this environment would be adaptable to various other environments and contexts. Services that add value for users but were impossible to implement in the past due to technical limitations offer tremendous possibilities for future research. Furthermore, the security dimensions of such systems need more observation and research.

As a result, the research on the application of the concept of cloud computing in a military context indicated that security-related factors prevent the applicability of public cloud computing environments in these high-security contexts, and the proper computing environment would not differ much from a private network as security requirements increased. As a consequence, the research shifted to investigate how requirements for cost effectiveness of this environment could be improved through increasing the rate of system utilization, as well as exploring the technical solutions needed to enable this increase.

One conclusion in this specific military context was that the best solution for utilization at the national level is a shared public authority system accessible to different organizations through the application of dynamic security zones. The Finnish Defence Forces can be used as an example of an organization whose need for computational capacity is relatively low during peacetime and vast during a crisis. Correspondingly, another authority might use more capacity during peacetime; if a crisis of national proportions occurs, said capacity could be limited. However, defining procedures around the dynamic availability of computational capabilities is a political question, not a technical one, which is why the establishment of information or computational priorities are excluded from this dissertation.

Both a process and a structure for the dynamic construction of a high-security network were presented, along with the recommendation to standardize requirements, the contractual approach, and network administration. This proposal enables the deployment of hybrid clouds in high-security environments. Furthermore, the findings can be adapted to other systems where information of varying security levels needs to processed in the most cost-effective way, one example being a high-security system that utilizes the edge computing paradigm as an additional computing resource. In edge computing, data is computed near its origins, "at the edge of network" (Shi & al., 2016). In such systems, different security levels may be defined for the edges and the core system. For instance, different security requirements may be defined for mobile devices than for the centralized core system.

As noted before, the concept of KmaaS was also presented as a part of this research. Instead of concentrating data fragments, KmaaS emphasizes the meta level and semantics of information. A semantic approach focuses on the knowledge extracted from data rather than on the data itself. This approach can be seen as an enabler for future research into artificial intelligence, where systems are developed to consider connections through meta-level phenomena.

KmaaS is a particularly important concept in rapidly changing environments involving vast amounts of data. If decision-making based on data is required, the most essential information should be extracted and phenomena described instead of a single data element being presented to the observer.

KmaaS can be applied to evaluating the quality of information when sharing it within a contract-based ecosystem. As accuracy of information can be hard to determine, KmaaS can assist in interpreting phenomena and evaluating its usefulness. The lower the level of information detail, the greater the significance of accuracy and the protocols ensuring it. However, when it comes to sharing situation-awareness data with other stakeholders, the more useful semantics can become in decision-making.

Adopting knowledge levels will also enhance user understanding of transferred information if a single data source malfunctions, is hosted by a malicious actor, does not provide any information, or lacks a manual component.

4.2. Enhancing business resilience

The second research question, "What are the measures for quantifying business resilience?" was addressed in the fourth and the fifth articles. The goal of the fourth Article [4] was to create a mathematical model that can be used to evaluate changes in security level in a dynamic environment. Before such a change can be measured, a numeric model for establishing a baseline is needed. The proposed model defines key components and a process for identifying them when determining security level. It also offers a mechanism for evaluating the cost of changes in security level. This proposed approach used the value of information to be secured, as opposed to the value of investments, as the basis for establishing costs. This approach liberates the analysis from observations regarding a system's sophisticated technical capabilities. Instead, the value of information in terms of business continuity is evaluated from the perspectives of risk and threat, and an assessment regarding the adequacy of security measures is performed. Figure 9 presents the relationship between business resilience, components, and threats.

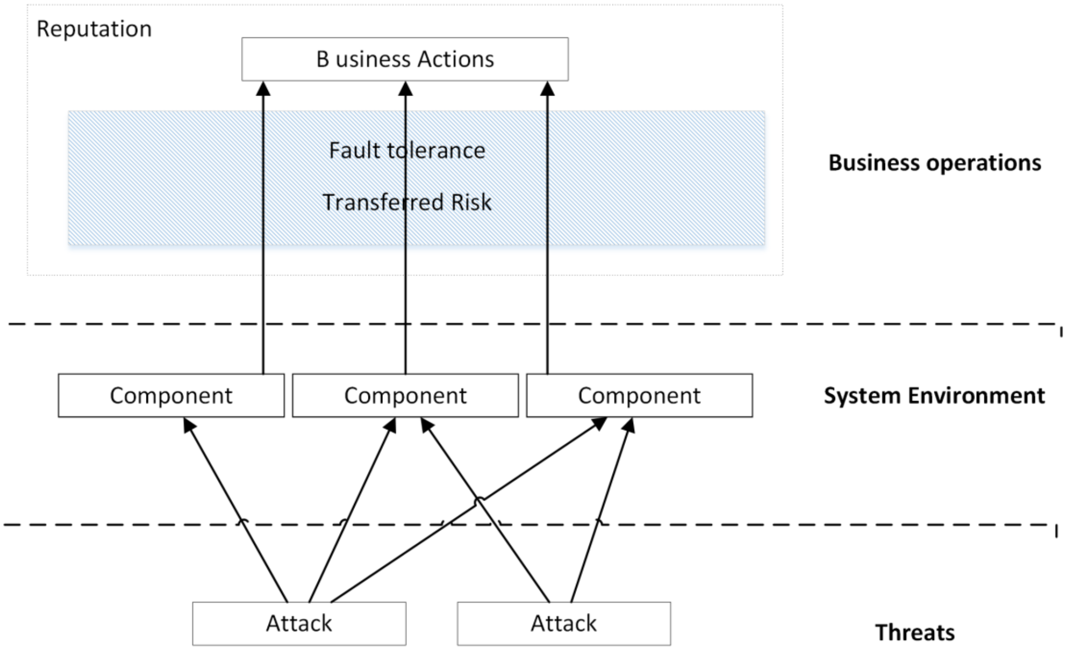


Figure 9. Illustration of the relationships between business resilience, components, and threats

As the model developed is generic and not created for any specific context, field, or domain, it allows the use of the most applicable risk-assessment frameworks for a specific system or environment. Such frameworks include, for example, the ISO's ISO 27005 (ISO/IEC 27005:2018, 2018), the Cloud Security Alliance's Cloud Controls Matrix (CCM Ver4, 2021), and the SANS Institute's Vulnerability Assessment (SANS Institute, 2021).

The model presented in the fourth Article [4] considers known threats to the system and evaluates risks to a business. Empirical observation and two classified case studies made it plain that the model is not sufficient for modern cyber-security environments in which hostile parties have sophisticated methods, enormous resources, and ample time at their disposal. Even so, the fifth Article [5] extended this approach to considering previously unknown threats and outlined potential defensive actions to securing a system from such attacks.

In addition to addressing research question 2, a new quantitative model for security management was presented in Article [4]. As stated above, the model considers known and unknown threats to the system. As the model can determine changes in security level, it can be utilized to evaluate the overall security of a dynamic high-security cloud environment. Furthermore, it was determined that improvements to information security in high-security systems must be considered in terms of various aspects of business resilience in order to allocate resources efficiently.

As a result, an algorithm for real-time monitoring of security level was proposed. The algorithm was designed to calculate the impact of a change in the environment or a system component on the security level of the system as a whole. The novelty of the findings lay in modeling the impact of a change in system configuration on system security level. Observations from two test cases later indicated that the level of monitoring should be considered carefully, since the update procedures are relatively slow when computing at a sufficient level of detail. The higher the accuracy, the greater the increase in the latency of update operations. As a result, a scheme whereby the model is utilized for approximation and the level of system detail is monitored was proposed as maximizing confidence in the system's overall security level.

No comparable model that considers the system's actual business value and uses that as a limit for security measures has been described in the literature in the field or in other sources. A similar attempt was initiated by Onwubiko C. and Onwubiko A. (2019), but their contribution was limited to identifying metrics or key performance indicators (KPI) that can be used to assess the cost-benefit ratios of cyber security investments.

Furthermore, the model proposed in Article [4] considers immaterial elements of the business, the organization's public reputation and trustworthiness after an attack, and various risk-mitigation activities. One observation was that not all useful mitigative actions are technical: collaboration, processes, insurance, and awareness of residual risk are also useful.

The European Commission General Data Protection Regulation (European Commission, 2018) came into force in EU countries during the spring of 2018. The proposed resilience-based model can evaluate the risk level of an organization in relation to the standards outlined in the regulation. The proposed fine to be levied on an organization after a data breach is determined by the business value and magnitude of the breach. Based on this model, an organization can minimize the data compromised during various kinds of attacks. In addition, the loss value can be also determined in relation to security measures.

4.3. Circle of Trust

The third research question "How could the concept of trust management be implemented in a collaborative information-sharing ecosystem where the stakeholders do not fully trust each other in such way that the confidentiality of the information provider is ensured, sharing is controlled, and the information quality meets the criteria for the collaboration?" was answered in the sixth Article [6].

Organizations that operate in a high-security environment need to collaborate with other organizations in order to share information, create more comprehensive situation awareness, and/or prepare for events that other organizations have already dealt with. Sharing and receiving information can be critical to the success of addressing large-scale crises and events. However, how much information is shared and at what level of detail is determined by the trust the supplying organization has in the recipient. This is why, when evaluating systems used to assist in decision making, it is essential to discuss trust in the system and the reliability of information it contains.

The goal of the sixth Article [6] was to present an implementable solution for information sharing in an operative environment. A conceptual environment was defined and the concept of Circle of Trust presented. The logical architecture of an enhanced information-sharing management system is illustrated in

Figure 10. The Circle of Trust represents an ecosystem in which the participants theoretically have sufficient trust in each other to share the sensitive information in their possession. In this model, participants also expect to receive information that improves operative success and would otherwise be too costly to get. However, as trust is neither fixed nor absolute, the system implementation must address the dynamic nature of trust, possible malicious actors within the system, and anonymity of information origin. Information can be seen as a currency to be traded, which is why a contract-based rule engine is proposed to prevent stakeholders from freeriding in the system.

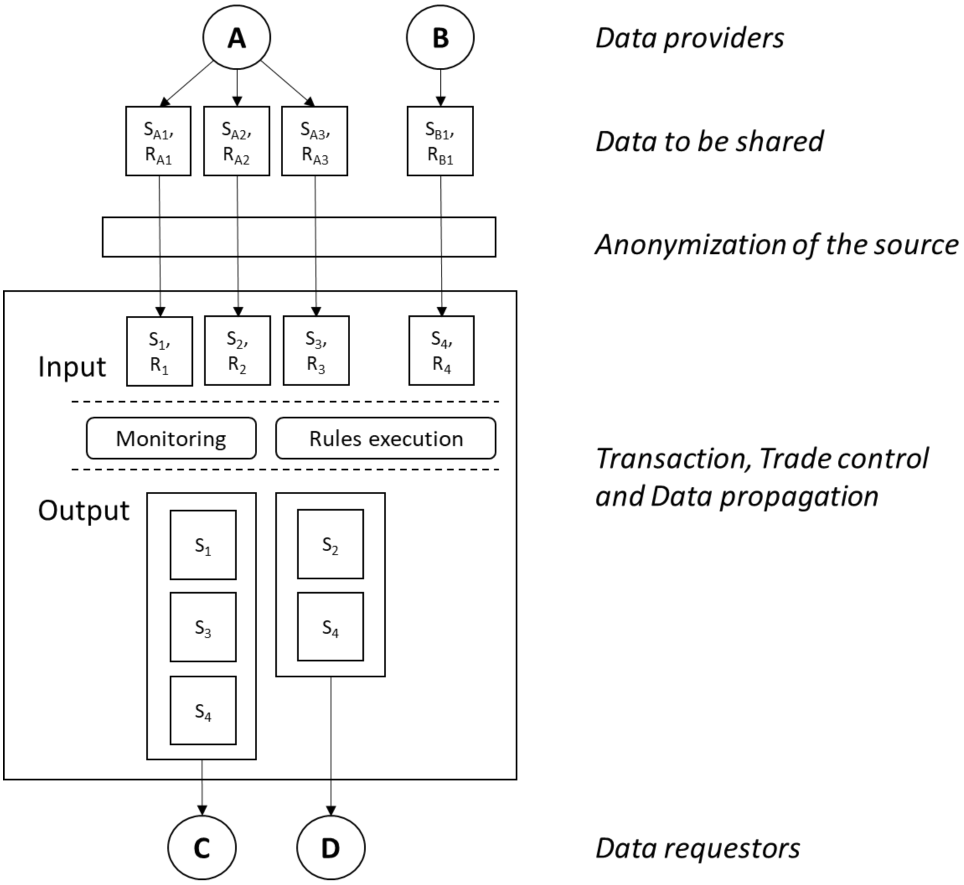


Figure 10. Enhanced Information Sharing Management

In modern cyber-security scenarios, the impact of a malicious actor needs to be carefully examined. It is highly probable that any system being studied has already been compromised. In the proposed system, information delivery to recipients can be controlled based on the preferences of the information supplier. In addition, the information supplier can change the delivery rules after publishing the information within the centralized system. These rules are then applied before any recipients fetch the information from the system. This mechanism allows the mitigation of three risks involving known malicious actors within the system: leaking sensitive information to the malicious actor, the accumulation of information within any stakeholder's hands, and/or collateral damage resulting from deception.

In most if not nearly all trust management systems presented in related research, information sharing is viewed from a positive perspective: information is shared if there is enough trust between counterparts. The model presented in this dissertation also views distrust as a tool in information sharing. Distrust in the recipient does not necessarily mean that information ought to be held back. Especially in military contexts, it might be useful to send false information if the information supplier has recognized that the recipient is not trustworthy (JP 3-13.4., 2012). But if false information is supplied to the system, all trustworthy recipients should be prevented from receiving it, in order to maintain the reputation of the supplier as trustworthy.

A model and algorithms for trade control (See

Figure 10) were developed and implemented (Zaerens, 2021). As the trade control component monitors and controls system trustworthiness, it is a key enabler of the overall system. The component also governs obligations and rights between participating parties and manages their trading balance and trust value from a system perspective. This is achieved by managing information as a currency. Assigning information a value allows measurement of agreement-based obligations regarding information sharing for each counterpart. The model considers trust values between stakeholders, varying technical capabilities among information providers in creating the information to be shared, and determining a value for information based on the information's relevance for its recipient.

Key properties of the trade control component:

- general properties for each counterpart
    - trading balance
    - trust value within the system
- counterpart as an information provider
    - from whom is certain information restricted
    - what is the level of detail of information shared with each recipient
- counterpart as an information recipient
    - feedback on relevance or accuracy of information received

The model encourages the sharing of all information and rewards information accuracy and relevance. Encouragement and rewards are based on the idea that the trading balance for a counterpart increases in relation the amount of shared information that is relevant and accurate. Information relevance is assessed by information recipients through a feedback process. The model punishes spamming and neglecting obligations. Some simulation results from the scenarios mentioned earlier are illustrated in Figures 11-15. Not all values are included in the chart; it is rather a snapshot after a certain amount (X-axis) of information is sent in a.

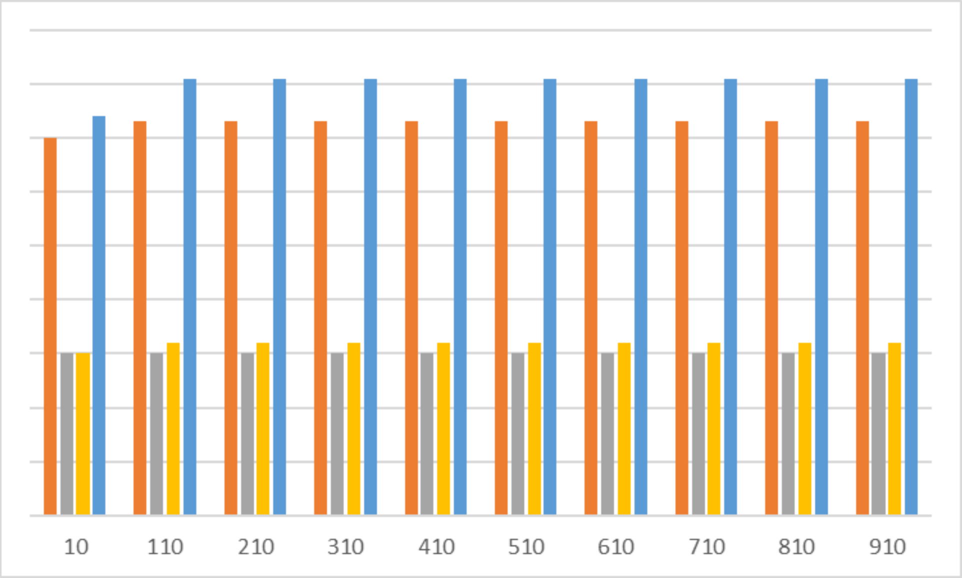


Figure 11. Trade balances in simulation scenario 3

In scenario 3, all stakeholders are trustworthy. The trust value is constant. If information is shared and received evenly, the trading balance is quite constant too.

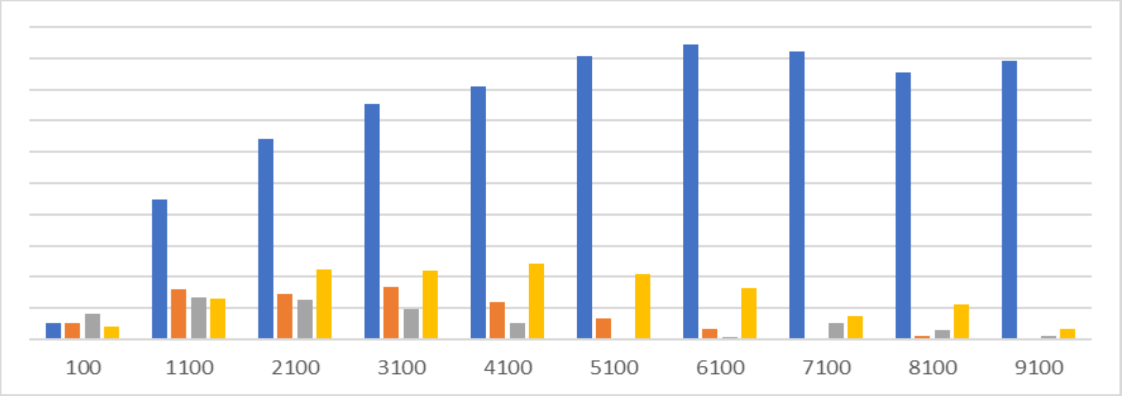


Figure 12. Trade balances in simulation scenario 4

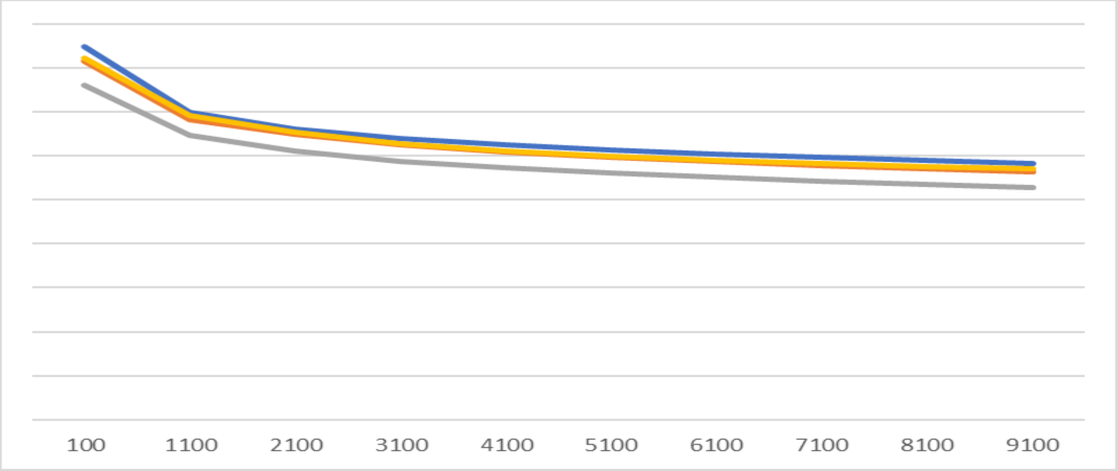


Figure 13. Stakeholder trust in simulation scenario 4

Scenario 4 presents a case in which one party provides more information than the others and the relevance of all shared information could be better. As a result, the party's trust values decrease over time, and the same pattern can be observed in the trading balances.

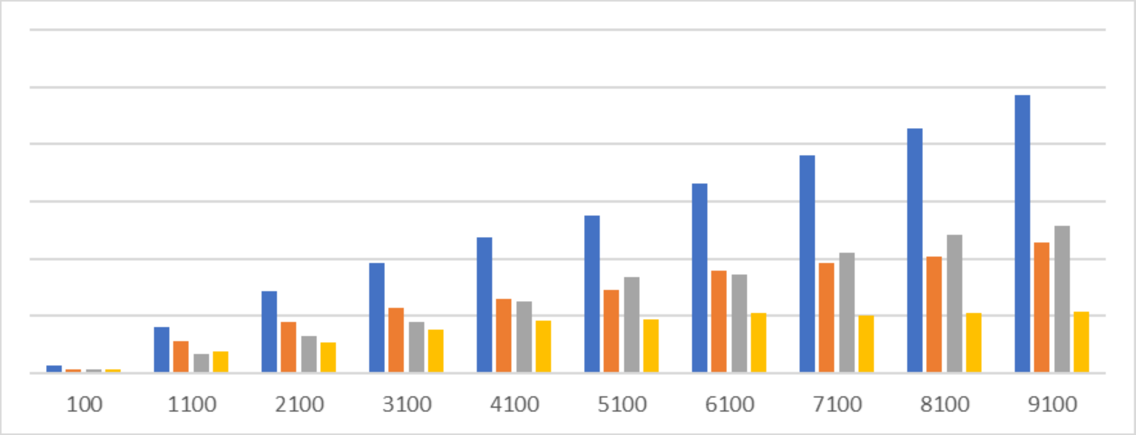


Figure 14. Trade balances in simulation scenario 6

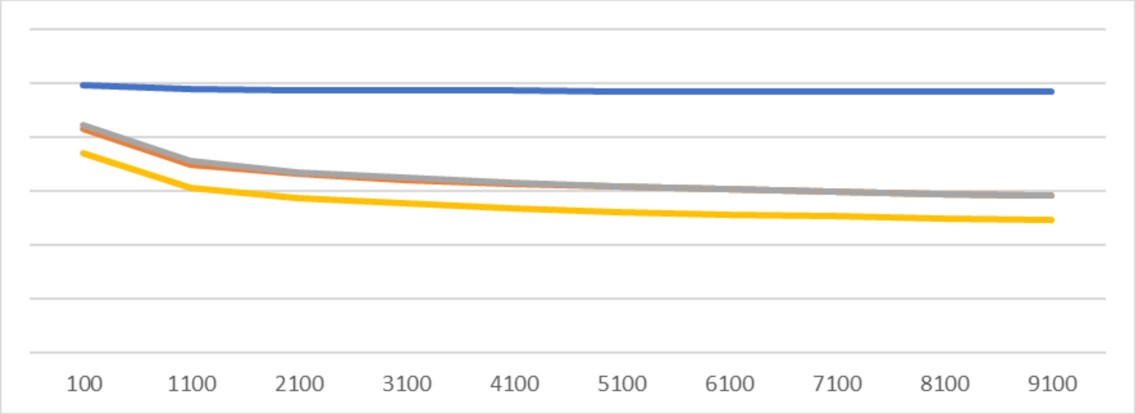


Figure 15. Stakeholder trust in simulation scenario 6

In scenario 6, one active party is not capable of sending detailed information to other parties. Relevance has an impact on the trustworthiness of the information sender, but only in relation to information detail. Therefore, the stakeholder's trustworthiness remains high, even if the information they send is of less relevance. The model is designed to take the varying capabilities of system stakeholders into account.

Furthermore, to ensure the security and openness of information shared through the system, the information is encrypted simultaneously with unique keys delivered to each recipient, as illustrated in Figure 16. *f(A*$_{key}$*)* is the encryption of the original information provided by A that results the encrypted information *A'*. For each recipient, there is a key that decrypts the information with *f'*, resulting in recipient-specific information ([*B*, *C, D*]) in Figure 16. It is noteworthy that there can also be a key or several keys for parties outside the Circle of Trust, as presented in Figure 16.

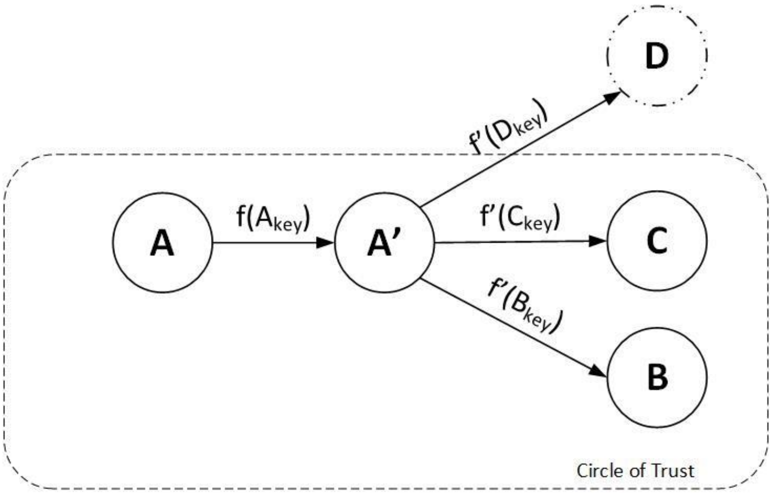


Figure 16. Recipient-specific encryption and decryption of information

According to the ElGamal-based encryption methodology presented by Huang, *f(A$_{key}$)* contains the encryption for all recipients: *f(B$_{key}$)*, *f(C$_{key}$)* and *f(D$_{key}$)* (El Gamal, 1985; Huang & Tso, 2012; Huang et al., 2015; Huang, Chen & Tso, 2015). After the keys are delivered to the recipients, the encrypted information can be accessed. And if, for instance, recipients B and C decided to compare the information received, any differences in said information could be identified, but its accuracy or reliability could not be determined.

Similarly, as a computational issue, the malicious actor would not be able to decrypt all possible solutions, and even if they were, they would not be aware which one of the results is the most accurate representation of the encrypted information. Moreover, it has been argued that even if the malicious actor could collect all the decrypted instances of the information from a certain time, it could not reliably determine which instances represent the best information.

This solution works best in time-sensitive systems where the amount of information is enormous. With infrequent exchange of high-security information, other conventional encryption methods are more useful.

The advantage of this approach is that the decryption result can be controlled during the encryption phase. Exposing all decryption solutions is a vast undertaking, and a malicious actor would not have the capability to determine which solution provides the most accurate information for which parameter within a reasonable time frame.

In some ways, the proposed system is analogous to music streaming services: a user can make a copy of a file and distribute it, but it is less complicated, cheaper, and sufficiently easy to fetch it from a common system. Similarly, in information-sharing systems, the key consideration is that participants trust the system itself, which is why the mechanisms of rule-based execution must be transparent. This helps to ensure that all stakeholders can trust that, at least to some extent, all other counterparts deliver high-quality information for the common benefit.

Although the proposed system is possible to implement to the extent defined in the dissertation scope, it is not comprehensive. In practice, this means that the necessary elements for implementation are presented, along with the applicable principles, but several details need to be worked out for the release of a more sophisticated version. For example, the approach to rule setting and the provision of rule-based contracts needs to be specified in greater detail.

While the implementation design of this system is useful at the organizational level, the concept of Circle of Trust can also be scaled down to the infrastructure level. The approach is useful when analyzing the computing nodes in a high-security environment and sensitive dataflow within the system. Malicious actors also exist at the infrastructure level, and instead of limiting the network traffic they receive, a more useful operative approach is to route deceptive data to a compromised node.

4.4. Filling the research gaps: a summary

Table 10 describes the ways in which this dissertation fills the research gaps presented in Chapter 2, Theoretical foundations, and its subchapters.

Table 10. Summary of ways in which the dissertation fills research gaps

Research objective	Research gap	Research result [Articles]
Research question 1	Knowledge management	Service model Knowledge Management as a Service [1, 2]
	Capability limitations in private clouds	Approach based on data prioritization [1, 2] Proposal for hybrid cloud infrastructure [2, 3]
	Fault tolerance and disaster recovery	Proposal for improving survivability in cloud applications [1, 2]
	Complexity of virtualization	Proposed SOA approach to future research into solutions to the underlying complexity of virtualization [1, 2]

	Security issues	Proposal for an advanced security scheme and future research [1, 2] Concept for the dynamic construction of a high-security cloud-based network [3]
Research question 2	A comprehensive model that contains the following assessments: • Threats • Vulnerabilities • Risks • Business resilience	Properties of business resilience for each component are determined [4]
	Lacks in resilience improvements: • the operative continuum • the business continuum in the short and long terms reputation	Properties of business resilience in the overall system are determined [4]
	Protection of immaterial assets and determining cost-benefit ratio.	A component criticality process is proposed and attributes determined [4]
	The protective mechanisms against persistent advanced threats.	The factor of an unknown threat is considered in the extended model [5] A contractual model is proposed for enhanced mitigative action [5]
	Security-level changes needs to be analyzed in real time	Real-time vulnerability analysis and corresponding algorithms in a dynamic environment are presented [4]
Research question 3	Theory for controlling leakage of information	Enhanced Information Sharing Management [6]
	Theory for preventing accumulation of information	
	Management scheme for shared misinformation	

4.5. Evaluation of research validity and reliability

This subchapter addresses the validity and reliability of the research comprising the dissertation. Research validity is defined as the accuracy of a measure (Rantapelkonen & Koistinen, 2016). It answers the question: Do the results represent the concept that they are supposed to measure? As described in the Methodology (Chapter 3), this dissertation applies a hermeneutical circle methodology. The hermeneutic philosophy considers the contextual relationship of the research subject (Palmer, 1969). The research is designed to progress incrementally, and new approaches are based on earlier results in a deductive manner. The hermeneutical circle is deployed by comparing the individual results of various research objectives with the context and system as a whole. This approach facilitates deeper understanding within the hermeneutical spiral, as suggested by Dilthey (1979).

This hermeneutical approach, combined with the dissertation's interdisciplinary nature, numerous theoretical domains, multiple methodologies, and several data sources suggest evaluating the validity of the research through triangulation (Patton, 1999). Carter et al. (2014) identify four types of triangulation: method triangulation, investigator triangulation, theory triangulation, and data source triangulation.

Method triangulation considers using multiple methods of data collection regarding the same phenomenon (Polit and Beck, 2012). In investigator triangulation, two or more researchers provide, in the same study, multiple observations, approaches, and conclusions. Theory triangulation addresses different theories for analysis and interpretation of data. Data source triangulation relies on varied types of data sources such as people, individuals, organizations, groups or communities to enable multiple perspectives and validation of data (Carter et al., 2014).

As explained in the dissertation design (Chapter 1,2), the six articles can be divided into three distinct sections. The triangulation used in the relevant articles is discussed in each of these sections, and taken as a whole, serves as a way of evaluating the validity of the research as a whole.

The research questions and their mapping to theoretical domains were discussed in Chapter 1. Moreover, for each primary domain, gap analysis was conducted to link the research questions to the findings. The dissertation's multiple theoretical domains and their connections to high-security ICT contexts provided several approaches to interpreting the data. Employing a variety of perspectives to examine the same material strengthens result validity (Carter et al., 2014).

The research methods used in the dissertation were introduced in Chapter 3. Each article contained at least two such methods, and from section perspective, described at least three research methods used in the investigation of each research question. Relying on a variety of methods and analyses to investigate the subject of research strengthens the validity of the results in each subsection and, thus, the dissertation as a whole.

The first section, dealt with Articles [1], [2] and [3]. In Article [3], the cowriter Jari Mannonen contributed to findings regarding the technical system architecture. This investigator triangulation through two approaches to the same subject provided a wider range of findings and strengthen the validity of infrastructure-related results that served as the basis for later findings. The data used in data source triangulation was primarily qualitative. However, quantitative calculations supporting the qualitative findings were identified in each article, and this constructed validity strengthens the validity of the qualitative results. The validity of research was furthermore evaluated and improved through empirical observations and subsequent articles that confirmed prior results.

Articles [1], [2], and [3] examined the cloud computing paradigm and predicted its market adoption. That research was conducted 2010-2012. The primary predictions presented in those initial articles have been later found to have been realized in commercial markets offering hybrid cloud service models, the management of varying security levels within a single system, advanced security measures and improved survivability.

The second section, covered Articles [4] and [5]. As mentioned before, the research conducted for Articles [1], [2], [3] and enquiries to determine the "sufficient security level" for the systems and organizations studied served as the bases for the documentation analysis to generate a theory to fulfill those requirements. As no comprehensive model for the cyber-security domain was found, the search was extended to mathematical modelling in general involving vulnerability, risk, and threat assessments. Theoretical gap analysis was conducted to help define the goals of the model. The critical infrastructure model presented by Lewis (2014) was accepted as a scientifically proven starting point and modified to the cyber-physical environment in a deductive manner.

For software algorithms, the research question, results, and validation need to be aligned (Shaw, 2003). In Article [4], the research objective was to monitor changes in dynamic security level; hence the creation of the algorithm, which was initially validated with persuasion, as system implementation was not part the scope. However, the use of the attack-tree model for algorithm evaluation presented by Fung et al. (2005) indicated that the results aligned with the study's theoretical foundations. Since the algorithm addresses the feasibility of real-time security-level monitoring, the persuasive approach is justified (Kelly, 1980; Shaw, 2003).

Article [5] was based on the model created in Article [4]. Observation of cyber incidents had indicated some defects in the model, and extensions to it were constructed in an inductive manner. That said, the model created is quantitative and designed to support qualitative problem-setting and findings. Relying on several systems and incidents and therefore multiple data sources to test the model indicates strong result validity based on data source triangulation as well as the model's applicability in different environments.

Investigator triangulation can be seen as having been utilized in Article [5], as cowriter Dr. Markus Häyhtiö contributed to findings from supply chain, private-public-partnership, and resource management perspectives. Approaching the concept of business resilience involving supply chains, subcontracting, and a broad commercial context had a significant impact, as the initial context was a closed single system. Extending the observations and discussion to further elements requiring consideration in turn increased the validity of results and applicability of findings.

Investigator triangulation does not apply in Article [6]. In this case, validity can be examined from the perspective of data source triangulation and recognizing the deep and constant interaction between the qualitative and quantitative data sources. The quality of shared information is measured in a qualitative manner, but receiving information from a certain source may have an impact on the trustworthiness of information sender. Trustworthiness can be modeled as a numeric value and a quantitative model created. The concept of qualitative information sharing proposed in Article [6] was tested through a simulation in which the concept took quantitative form. This ensured the validity of results in Article [6].

As discussed in the subchapter on limitations (Chapter 1.3), the source data used in this dissertation is classified as public and is thus only a subset of the material included in a high-security environment. As a consequence, there is a risk that the data used is not a sufficient representation of the features of a high-security environment. This risk is mitigated by concentrating on the phenomenon of high-security computation instead of detailed data. Corresponding research involving sensitive or critical information has been conducted in various other fields, such as the healthcare and energy sectors. Those results serve as comparisons and are utilized in articles included this dissertation. This technical comparison enhances the confidence and validity of the present results. On the other hand, since the solutions presented here are intended for use in all high-security environments, they are applicable to a greater variety of contexts, including for use by public authorities, governments, and the private sector.

In its discussion of specific methods of cyber-security attack, Article [5] presented public data that had been complemented with an interview. As the interview did not fulfill scientific requirements regarding data validity, no deep analysis or findings were based solely on the interview. However, international and independent media sources have published corresponding material including the data presented during the interview (Stubbs, Menn & Bing, 2019).

Research reliability is defined as the consistency of measures (Rantapelkonen & Koistinen, 2016): in other words, results do not vary between studies if the conditions remain the same. The reliability of the quantitative models applied in Articles

[4] and [5] is based on combination of deductive and inductive reasoning (Streefkerk, 2019; Merriam-Webster dictionary, 2021).

In Article [4], the critical infrastructure model presented by Lewis (2014) served as a scientifically proven starting point. Mathematical analysis can be used to evaluate the extensions to that model and its reliability criteria. Additional reliability was achieved through having material on actual costs of cyber incidents and inductively taking this into account in the model. Similarly, in Article [5] reliability was ensured first through inductive reasoning and then verified through deductive reasoning in other environments.

In Article [6], the reliability of the results was tested through the trade balance component simulation, as explained in Methodology (Chapter 3). Testing multiple data sets using similar scenarios, the algorithm produced consistent results. The repetitiveness of system execution and consistency of results proves the system's reliability [Middleton, 2019].

5

CONCLUSIONS

This dissertation has shown that it is possible to utilize the cloud computing paradigm in high-security environments, including military and public authority contexts. However, several constraints need to be addressed during the adoption of this paradigm: security, capability limitations, survivability, and technological complexity. In addition, in order to extract the most benefits, the users' perspective must be considered and stakeholder requirements regarding essential data provision must be defined. When adapting cloud computing for use in high-security contexts, this dissertation presented the following novel enhancements:

- A new service model concept called Knowledge Management as a Service (KmaaS) that improves the control of information and data across the entire cloud. This service model includes a frame architecture for transaction management in order to enable more advanced disaster-recovery methods. KmaaS also includes a metadata directory for processing information consistent with data content. KmaaS enables a more pervasive approach to cloud computing by hiding the complexity of the underlying technical data architecture. KmaaS ensures data consistency, redundancy, and reliability, which are essential requirements for data in a high-security context.
- KmaaS facilitates the usage of computational resources according to information content. It also provides improved data management with transactional features, as well as advanced replication control, while enabling external cloud management and theoretically unlimited computational resources in high-security environments.
- Furthermore, the dissertation examined preparatory actions and standardization requirements for cloud environments that can be used as capability and resource extensions to high-security cloud environments. In addition, a process for the dynamic construction of the cloud was proposed.

This dissertation also discussed measures for quantifying business resilience. With an eye to system vulnerability, the concept of business resilience was proposed as a way of determining the most critical system components in terms of business continuity. The attributes of business resilience were then applied to determine those components and the ways in which they interact with the overall environment. Those attributes allow for processing a component's direct and indirect costs when they are not in use. In an enhancement to previous models, the attributes also include immaterial expenses as enablers of future business. A comprehensive set of tools for determining the risk of a threat to the business and for allocating resources to the components that are the most vulnerable in terms of resilience was presented. Real-time vulnerability analysis in dynamic environments facilitated the use of business resilience attributes in dynamic constructions within high-security contexts. An awareness of information-security level after recovery from an attack or after system security enhancements was also achieved. The methodologies presented allow identification of system vulnerabilities in relation to business resilience, evaluation of what can be achieved through enhancements to the system, and lastly, allocation of limited resources to the most vulnerable components in order to achieve the best protection for the system.

Finally, this dissertation proposed a novel trust management approach to information sharing in a high-security environment where another stakeholder's cloud cannot be fully trusted. That environment was defined as a Circle of Trust. It was demonstrated that, while absolute trust never exists, information exchange is necessary to build comprehensive situation awareness. As novel approaches to trust management, this dissertation proposed the following:

- Enhanced Information Sharing Management, which utilizes modern blockchain and cryptographic technology, and
- Exploring smart contracts as a way of improving the overall approach by ensuring the integrity and confidentiality of shared information. This approach was shown to enhance privacy, data leakage prevention and data accumulation prevention, and reduce the collateral damage of deception in comparison to a traditional VPN P2P system.

6

SUGGESTIONS FOR FUTURE RESEARCH

This chapter proposes some intriguing areas for future research based on findings during this dissertation. To achieve improved mechanisms for creating an enhanced situational awareness or any cybersecure data-oriented system, information trustworthiness should be examined from at least the following perspectives:

- Optimization of trust management utilization in an information sharing context. One key challenge is creating a quality-based contract rule engine [6].
- Survivability of knowledge in the case of an unstable environment, along with advanced fault tolerance methods at the logical level in order to eliminate failures from inconsistent information flows [1].
- Detecting anomalies in dataflow and analysis of compromised nodes [3].
- Utilizing trust networks within the Internet of Things ecosystem [6].

From a general computational utilization perspective, the following concepts would also be worth studying:

- A computation for the automated redirecting of information based on content and security classification. With this approach, various distributed computing and information anonymization and/or pseudonymization schemes could be utilized. The objective would be to seek the most cost-effective locations for computation of various contents in relation to security requirements [1, 2, 3, 5].
- Automated analysis of system usage and, based on that analysis, the creation of a data source for a situation-awareness system that prioritizes resources accordingly [1, 2].

ERRATA

In Article [1], Chapter IV, A. Knowledge Management, the example duration of data transfer should be 80 seconds, i.e. 1.3 minutes.

In Article [2], Chapter 5.1, the example duration of data transfer should be 80 seconds, i.e. 1.3 minutes.

REFERENCES

Abadi, D. J. (2009). Data management in the cloud: Limitations and opportunities. *IEEE Data Engineering Bulletin*, *32*(1), 3-12.

Abdul-Rahman, A., & Hailes, S. (1998). A distributed trust model. *Proceedings of the 1997 New Security Paradigms Workshop*, 48-60.

Acquaah, M., Amoako-Gyampah, K., & Jayaram, J. (2011). Resilience in family and nonfamily firms: an examination of the relationships between manufacturing strategy, competitive strategy and firm performance. *International Journal of Production Research*, *49*(18), 5527–5544.

Adrian, H., & Cheney, B. (2015). JMD: A Hybrid Approach for Detecting Java Malware. *Proceedings of the 13th Australasian Information Security Conference*, 27.

Andress, J., & Winterfeld, S. (2011). *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners*. Elsevier.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A.,.Zahar, M. (2009). Above the Clouds: A Berkeley View of Cloud Computing. UC Berkeley Reliable Adaptive Distributed Systems Laboratory.

Baker, G. H. (2005). A Vulnerability Assessment Methodology for Critical Infrastructure Sites. *DHS Symposium: R&D Partnerships in Homeland Security*.

Bajerová, A. (2017). Impact on NATO of Cyberspace as a Domain of Operations: SWOT Analyses. CCDCOE. Retrieved 28th April 2020 from https://ccdcoe.org/library/publications/impact-on-nato-of-cyberspace-as-a-domain-of-operations-swot-analyses/

Barbacci, M. (1996). Survivability in the age of vulnerable systems. *IEEE Computer, 29*(11), 8.

Bisong, A., & Rahman, M. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications*, *3*(1).

Bitcoin (2009). Bitcoin Developer Guide. [Online]. Retrieved 19th Apr 2020 from: http://www.bitcoin.org/.

Bozdag, E., Asan, U., Soyer A., & Serdarasan, S. (2015). Risk prioritization in Failure Mode and Effects Analysis using interval type-2 fuzzy sets. *Expert Systems with Applications, 42*(8), 4000-15.

Brewer, E. (2000). Towards Robust Distributed Systems*, 2000 Symposium on Principles of Distributed Computing (PODC).*

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done? *Qualitative research, 6(*1), 97-113.

Buterin, V. (2020). A Next Generation Smart Contract & Decentralized Application Platform. Ethereum White Paper. [Online]. Available: http://www.Ethereum.org. Revisited: 19th Apr 2020.

Cambridge Dictionary. [Online]. (2021). Cambridge University Press. Retrieved 30th of August 2021 from https://dictionary.cambridge.org/ .

Cardoso, J., Luo, Z., Miller, J.A., Sheth, A. P., & Kochut, K. J. (2001). Survivability architecture for workflow management systems. *Proceedings of the 39th Annual ACM Southeast Conference,* 207-214.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J. & Neville, A.J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*. Vol. 41, No. 5, September 2014.

CCDCOE Law Branch Researchers & Kaska, K. (Eds.) (2019, May). Trends in International Law for Cyberspace. CCDCOE NATO Cooperative Cyber Defence Centre Of Excellence.

CCM Ver 4. [Online] (2021). Cloud Control Matrix Version 4. *Cloud Security Alliance.* Retrieved 31 August 2021 from https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Chen, B., Zeng, G. S., & Li, L. (2008). Attribute Delegation Authorization Based on Subjective Trust Evaluation. *2008 IFIP International Conference on Network and Parallel Computing*, 42-49.

CISCO. (2020). What Is a VPN? – Virtual Private Network. Retrieved 26 April 2020 from https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Courtney, M. (2017). States of cyber warfare. *Engineering & Technology, 12*(3), 22-25.

Delmolino K., Arnett M., Kosba A., Miller A., & Shi, E. (2016). Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In J. Clark, S. Meiklejohn, P. Ryan, D. Wallach, M. Brenner & K. Rohloff (Eds.) *Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, Vol. 9604* (pp. 79-94). Springer.

Dictionary.com. [Online]. (2020). Retrieved 28th of April 2020 from https://www.dictionary.com/browse/trustworthiness.

Dilthey, W. (1979). *Dilthey: Selected Writings*. CUP Archive.

Douceur, J. R. (2002). The sybil attack. *Electronic Proceedings of the 1st International Workshop on Peer-to-Peer Systems*, 101.

Eder, J., & Liebhart, W. (1996). Workflow recovery. *Proceedings of the First IFCIS International Conference on Cooperative Information Systems,* 124-134.

El Gamal T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, *31*(4), 469-472.

El Kettani, M., & En-Nasry, B. (2011) MidM: An Open Architecture for Mobile Identity Management. *Journal of Convergence*, *2*(2).

Endsley, M. (1988). Design and evaluation for situational awareness enhancement. *Proceedings of the Human Factors Society 32nd Annual Meeting*, 97-101.

Erdogmus, H. (2009). Cloud Computing: Does Nirvana Hide Behind the Nebula? *IEEE Software, 26*(2), 4-6.

Ferreira, A. (2019). Vulnerability analysis in critical infrastructures: a methodology. *Security and Defence Quarterly, 24*(2), 65-86.

FDF. [Online] (2021). Sotilastiedustelu, Julkinen katsaus 2021. Finnish Defence Forces 6th of May 2021. Retrieved 1st of September 2021 from https://puolustusvoimat.fi/documents/1948673/74055459/PV_sotilastiedustelu_raportti_www_FI_2021.pdf/5a4aea51-64bc-f736-bc70-6b3e4815495c/PV_sotilastiedustelu_raportti_www_FI_2021.pdf?t=1620279050410

Finnish Cyber Security Center (2014). Kyberturvallisuuskeskuksen vuosikatsaus 2014. Survey for year 2014 by Finnish Cyber Security Center. The Finnish Transport and Communications Agency.

ForMin Finland (2013). Tietoturvaloukkaus Suomen ulkoasiainhallinnossa – Ulkoasiainministeriö: Ajankohtaista. Retrieved 28th of April 2020 from https://finlandabroad.fi/web/fra/ajankohtaista/-/asset_publisher/TV8iYvdcF3tq/content/tietoturvaloukkaus-suomen-ulkoasiainhallinnos-2/384951.

Foster, I. (2002). What is the grid? A three point checklist. *GRID Today, 1*(6).

FSB [Online] (2020). Effective Practices for Cyber Incident Response and Recovery. *Financial Stability Board (FSB).* Retrieved 3rd of September 2021 from https://www.fsb.org/wp-content/uploads/P191020-1.pdf

Fung, C., Chen, Y. L., Wang, X., Lee, J., Tarquini, R., Anderson, M., & Linger, R. (2005, October). Survivability analysis of distributed systems using attack tree methodology. *MILCOM 2005: 2005 IEEE Military Communications Conference*, 583-589.

Fung, C. K., & Hung, P. C. K. (2005). System recovery through dynamic regeneration of workflow specification. *Proceedings of the Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*, 49-157.

Gal-Oz, N., Gudes, E., & Hendler, D. (2008). A robust and knot-aware trust-based reputation model. *Proceedings of the 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security*, 167-182.

Gal-Oz, N, Yahalom, R., & Gudes, E. (2011). Identifying Knots of Trust in Virtual Communities. In I. Wakeman, E. Gudes, C. D. Jensen, & J. Crampton (Eds.) *Trust Management V: IFIPTM 2011. IFIP Advances in Information and Communication Technology Vol. 358* (pp. 67-81). Springer.

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection, Part I: A state of the art. *JRC Technical Notes.*

Girard, J.P., & Girard, J. L. (2015). Defining knowledge management: Toward an applied compendium. *Journal of Applied Knowledge Management, 3*(1), 14.

Grandison. T., & Sloman, M. (2002). Specifying and analysing trust for internet applications. *Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government*, 145-157.

Grönroos, C. (2011). Value co-creation in service logic: A critical analysis. *Marketing Theory, 11*(3), 279-301.

Hariri, S., Qu, G., Dharmagadda, T., Ramkishore, M., & Raghavendra, C. S. (2003). Impact Analysis of Faults and Attacks in Large-Scale Networks. *IEEE Security & Privacy, 1*(5) 49-54.

Handel, M., (1982). Intelligence and deception. *Journal of Strategic Studies*, 5(1), 122-154.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105.

Huang, K., Chen, Y. C., & Tso, R. (2015). Semantic Secure Public Key Encryption with Filtered Equality Test – PKE-FET. *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, 327-334.

Huang, K., & Tso, R. (2012). A commutative encryption scheme based on ElGamal encryption. *International Conference on Information Security and Intelligence Control (ISIC)*, 156-159.

Huang, K., Tso, R., Chen, Y., Li, W., & Sun, H. M. (2015). A New Public Key Encryption with Equality Test. In M.H Au, B. Carminati, & CC. J. Kuo (Eds.) *Network and System Security. NSS 2015. Lecture Notes in Computer Science, Vol. 8792*, 550-557.

Huang, K., Tso, R., Chen, Y., Rahman, M., Almogren, A., & Alamri, A. (2015). PKE-AET: Public Key Encryption with Authorized Equality Test. *The Computer Journal*, *58*(10), 2686–2697.

Hulme, G. V. [Online] (2017). Tackling cybersecurity threat information sharing challenges. *CSO online, Jan 2017*. IDG Communications. Retrieved 3rd of September 2021 from https://www.csoonline.com/article/3157540/tackling-cybersecurity-threat-information-sharing-challenges.html

Hwang, K., Kulkarni, S., & Hu, Y. (2009). Cloud security with virtualized defense and reputation-based trust management. *Proceedings of the 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, 717-722.

IBM. (2019). Virtualization. IBM Cloud Learn Hub. Online. Retrieved on 26th April 2020 from https://www.ibm.com/cloud/learn/virtualization-a-complete-guide.

IEEE Taxonomy [Online] (2021), 2021 IEEE Taxonomy. *The Institute of Electrical and Electronics Engineers (IEEE).* Version 1.0. Retrieved 31st of August 2021 from https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee-taxonomy.pdf

ISO/IEC 27001:2013, Information Security Management. The International Organisation for Standardisation.

ISO/IEC 27005:2018, Information technology – Security techniques – Information Security Risk Management. The International Organisation for Standardisation.

ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity. The International Organisation for Standardisation.

ISO 31000:2018, Risk Management – Guidelines. The International Organisation for Standardisation.

Iltaf, N., Ghafoor, A., and Hussain, M. (2011). STEP-α: An Algorithmic Approach towards Trust based security in Pervasive Computing Environment. *IEEE Asia-Pacific Services Computing Conference*, 330-336.

Jaafar, F., Avellaneda, F. and Alikacem, E. H. (2020). "Demystifying the Cyber Attribution: An Exploratory Study," *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2020*, pp. 35-40

Jajodia, S., Noel, S., & O'Berry, B. (2005). Topological Analysis of Network Attack Vulnerability. In V. Kumar, J. Srivastava, & A. Lazarevic (Eds.) *Managing Cyber Threats: Massive Computing, Vol. 5* (pp. 247-266). Springer US.

Jenelius, E., & Mattsson, L. (2015). Road network vulnerability analysis: Conceptualization, implementation and application. *Computers, Environment and Urban Systems*, *49*, 136-147.

JP 3-13.4. (2012). Military Deception. *Joint Publication 3-13.4*. Joint Forces Staff College. January 2012.

Jøsang, A., & Pope, S. (2005). Semantic Constraints for Trust Transitivity. *Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modeling, Vol. 43* (pp. 59-68). Australian Computer Society, Inc.

Kandukuri, B. R., & Rakshit, A. (2009). Cloud security issues. *SCC '09: Proceedings of the 2009 IEEE International Conference on Services Computing* (pp. 517-520). IEEE.

Kang, M. G., McCamant, S., Poosankam, P., & Song, D. (2011). DTA++: Dynamic Taint Analysis with Targeted Control-Flow Propagation, *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011*. The Internet Society ISOC.

KATAKRI. (2011). KATAKRI 2011 – Information security audit tool for authorities. Version III. Finnish Ministry of Defence. Retrieved 25th of April 2020 from https://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf.

KATAKRI. (2015). KATAKRI 2015 – Information security audit tool for authorities. Version III. Finnish Ministry of Defence. Retrieved 25th of April 2020 from https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy, 7*(4), 61-64.

Kelly, E. F. (1980). Evaluation as Persuasion: A Practical Argument. *Educational Evaluation and Policy Analysis*, Sep. - Oct., 1980, Vol. 2, No. 5 (Sep. - Oct., 1980), pp. 35-38.

Kessler, G. C. (1998). An overview of cryptography. *The Handbook on Local Area Networks*, Auerbach.

Kim, W. (2009). Cloud Computing: Status and Prognosis. *Journal of Object Technology, 8*(1), 65-72.

Klimburg, A., & Tiirmaa-Klaar, H. (2011). Cybersecurity and Cyberpower: Concepts, conditions and capabilities for cooperation for action within the EU. EP/EXPO/B/SEDE/FWC/2009-01/Lot6/09, European Parliament, April 2011.

Klimburg, A. (2012). National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

Kossmann, D., Kraska, T- & Loesing, S. (2010). An evaluation of alternative architectures for transaction processing in the cloud. *In Proceedings of the 2010 international conference on Management of data (SIGMOD '10).*

Kraska, T., Hentschel, M., Alonso, G. & Kossmann, D. (2009). Consistency rationing in the cloud: pay only when it matters. *In VLDB '09*, August 2009.

Kumar, M., Dubey, K., & Pandey, R. (2021, January). Evolution of Emerging Computing paradigm Cloud to Fog: Applications, Limitations and Research Challenges. *In 2021 11th International Conference on Cloud Computing, Data Science & Engineering.*

Kumar, P., & Singh, S. B. (2015). Fuzzy Fault Tree Analysis using Level (λ, ρ) Interval-Valued Fuzzy Numbers. *Mathematical Theory and Modeling*, *5*(2).

Laari, T., Flyktman, J., Härmä, K., Timonen, J. & Tuovinen, J. (2019). #kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle. Helsinki. Maanpuolustuskorkeakoulu.

Lamanna, D. D., Skene, J., & Emmerich, W. (2003, January). Slang: A language for defining service level agreements. *Proceedings of the 9th IEEE Workshop on Future Trends of Distributed Computing Systems* (pp. 100-106). IEEE Computer Society.

Lappalainen, E. & Jormakka, J. (2004). Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa. Helsinki: Maanpuolustuskorkeakoulu.

Lee, D., Tang, C. Y., Fang, J. F., Yao, C. Y., & Lin, I. J. (1999). Parallel Iterative Methods–Pipelined Iterative Methods on Combustion Problem. In P. Chiao-ling Lin, A. Fox, N. Ecer, N. Satofuka, & J. Periaux (Eds.) *Parallel Computational Fluid Dynamics '98* (pp. 369-376). North-Holland.

Lewis, J. (2011). Cyberwar Thresholds and Effects. *IEEE Security & Privacy, 9*(5), 23-29.

Lewis, T. G. (2014). *Critical infrastructure protection in homeland security: defending a networked nation.* John Wiley & Sons.

Li, L., Liu, C., & Wang, J. (2007). Deriving transactional properties of composite-web services. In *IEEE International Conference on Web Services ICWS 2007* (pp. 631-638). IEEE.

Li, Y., Yang, H., & Xie, K. (2015). Network Node Importance Measurement Method Based on Vulnerability Analysis. In W.E. Wong (Ed.) *Proceedings of the 4th International Conference on Computer Engineering and Networks*, (pp. 1281-1289). Springer International Publishing.

Libicki, M. (2017). The Coming of Cyber Espionage Norms. *2017 9th International Conference on Cyber Conflict: Defending the Core.* June 2017.

Linthicum, D. S. (2017). Connecting fog and cloud computing. *IEEE Cloud Computing, 4(2), 18-20.*

Loui, R. & Hope, W. (2017). Information Warfare Amplified by Cyberwarfare and Hacking the National Knowledge Infrastructure. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 280-283). IEEE.

Lu, H., Chan, W. K., & Tse, T. H. (2008). Testing pervasive software in the presence of context inconsistency resolution services. *Proceedings of the 30th international conference on software engineering* (pp. 61-70).

Luo, Z., Sheth, A., Kochut, K., & Arpinar, B. (2003). Exception handling for conflict resolution in cross-organizational workflows. *Distributed and Parallel databases, 13*(3), 271-306.

Lv, H., Zhang, Y., Wang. R., & Wang, J. (2013). Graph-Based Real-Time Security Threats Awareness and Analysis in Enterprise LAN. In R. Zhang, Z. Zhang Z, K. Liu, and J. Zhang (Eds.) *LISS 2013* (pp. 1299-1304). Springer.

Maathuis, C., Pieters, W., & Den Berg, J. V. (2016). Cyber weapons: a profiling framework. *2016 International Conference on Cyber Conflict CyCon U.S.*, 1-8.

Mead, N., Ellison, R. Linger, R., Longstaff, T., & McHugh, J. (2000). Survivability Network Analysis Method. CMU/SEI-2000-TR-013, September 2000.

Medium. (2019). What Is Service-Oriented Architecture? Software Development Community. Medium. 13th March 2019. Retrieved on 26th of April 2020 from https://medium.com/@SoftwareDevelopmentCommunity/what-is-service-oriented-architecture-fa894d11a7ec.

Mei, L., Chan, W. K., & Tse, T.H. (2008). A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues. *Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference ASPCC 2008*, 464-469.

Mell, P., & Grance, T. (2009) The NIST Definition of Cloud Computing. Version 15, 7.10.2009. National Institute of Standards and Technology, Information Technology Laboratory. Retrieved on 26th of April 2020 from http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

Merriam-Webster dictionary. [Online]. (2021). Retrieved 30th of August 2021 from https://www.merriam-webster.com/dictionary/.

Mickos, J. Interview, 23rd of March, 2017.

Middleton, F. [Online]. (2019). Types of reliability and how to measure them. *Scribbr*. Retrieved 2nd of September from https://www.scribbr.com/methodology/types-of-reliability/.

Mintzberg, H., [Online]. (2017). The U.S. Cannot Be Run Like a Business. *Harvard Business Publishing*. Retrieved 30th of August 2021 from https://hbr.org/2017/03/the-u-s-cannot-be-run-like-a-business .

Moore, A., Ellison, R., & Linger, R. (2001). Attack Modeling for Information Security and Survivability. CMU/SEI-2001-TN-001, March 2001.

Morgan, C. [Online] (2021). Cyber Attacks: The Challenge Of Attribution And Response. *Cybercrime and Dark Web Research*. Digital Shadows. June 2021. Retrieved 2nd of September from https://www.digitalshadows.com/blog-and-research/cyber-attacks-the-challenge-of-attribution-and-response/

Morisse, M., & Prigge, C. (2017, August 10-12). *Design of a business resilience model for Industry 4.0 manufacturers* [Conference paper]. Twenty-third Americas Conference on Information Systems, Boston, MA, USA.

Nachira, F., Nicolai, A., Dini, P., Le Louarn, M., & León, L. R. (2007). Digital business ecosystems. European Commission.

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

Naraine, R. (2012). Nortel hacking attack went unnoticed for almost 10 years. [online] ZDNet. Retrieved 28th or April 2020, from http://www.zdnet.com/article/nortel-hacking-attack-went-unnoticed-for-almost-10-years.

NATO. (2007). CYBERWAR Related Definitions. North Atlantic Treaty Organization (NATO). AC/322(SC/2-NC3TS)L(2007)0002 - NU, April 2007.

NATO. (2017). Warsaw Summit Key Decisions. North Atlantic Treaty Organization (NATO). Fact Sheet. 6th of February 2017.

NATO. (2020). North Atlantic Treaty Organization. [Online]. Retrieved 28th April 2020 from https://www.nato.int/.

NCSC-FI [Online] (2021). National Cyber Security Centre – Finland. Retrieved 3rd of September 2021 from https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management

NDB (2020) LLP: Statement on Auditing Standards No. 70 (SAS 70). Retrieved 28th of April 2020 from http://sas70.com/sas70_overview.html.

Newsome, J. & Song, D. X. (2005, February). *Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software* [Conference paper]. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA.

Ng, I. C., Maull, R., & Yip, N. (2009). Outcome-based contracts as a driver for systems thinking and service-dominant logic in service science: evidence from the defence industry. *European Management Journal, 27*(6), 377-387.

NIST FIPS PUB 199. (2004, February). Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 199.

NIST FIPS PUB 200. (2006, March). Minimum Security Requirements for Federal Information and Information Systems. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 200.

NIST SPEC PUB 1500-201. (2017, June). *Framework for Cyber-Physical Systems, Vol. 1: Overview.* National Institute of Standards and Technology (NIST) Special Publication 1500-201.

Onwubiko, C. and Onwubiko, A. (2019). Cyber KPI for Return on Security Investment. *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA),* 2019, pp. 1-8.

Palmer, R. (1969). *Hermeneutics: Interpretation Theory in Schleiermacher, Dilthey, Heidegger, and Gadamer.* Northwestern University Press.

Patton, M.Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Sciences Research*, 34, 1189–1208.

Polit, D.F., & Beck, C.T. (2012). Nursing research: Generating and assessing evidence for nursing practice. *Philadelphia, PA: Lippincott Williams and Wilkins.*

Prunckun, H. (2019). Counterintelligence Theory and Practice. *Security and Professional Intelligence Education Series (SPIES).*

Rantapelkonen, J. & Koistinen, L. (2016). *Pohdintoja sotatieteellisistä käsitteistä.* Helsinki: Maanpuolustuskorkeakoulu.

Rauscher, K. F. & Yaschenko, V. (2011). The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations. *EastWest Institute and Information Security Institute of Moscow State University*, April 2011. Issue 1.

Reuters. (2009). Timeline: Key dates in the history of Nortel. Reuters Technology News, 14.1.2009. Retrieved 28th of April 2020 from http://www.reuters.com/article/us-nortel-timeline-sb-idUSTRE50D3N120090115

RFC1661. (1994). The Point-to-Point Protocol (PPP). Network Working Group. July 1994. Retrieved on 26th April from https://tools.ietf.org/html/rfc1661.

Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I. M., …Galan, F. (2009). The reservoir model and architecture for open federated cloud computing. *IBM Journal of Research and Development, 53*(4), 4-1.

Rohith. C., & Batth, R. S. (2019). Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and its Repercussion. *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, (pp. 640-645). IEEE.

Saha, D., & Mukherjee, A. (2003). Pervasive computing: a paradigm for the 21st century. *Computer, 36*(3), 25-31.

SANS Institute. [Online] (2021) Retrieved 31st of August 2021 from https://www.sans.org/emea/.

Sauvé, J., Marques, F., Moura, A., Sampaio, M., Jornada, J., & Radziuk, E. (2005, October). SLA design from a business perspective. *Proceedings of the International Workshop on Distributed Systems: Operations and Management DSOM 2005* (pp. 72-83). Springer.

Sevis, K. N. & Seker, E. (2016, June 13-14). *Cyber warfare: terms, issues, laws and controversies* [Conference paper]. 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), London, UK.

Shaw, M. (2003). Writing good software engineering research papers: a minitutorial. *Proceedings of the 25th International Conference on Software Engineering (ICSE '03)* (pp. 726–736). IEEE Computer Society.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE internet of things journal*, 3(5), 637-646.

Silas, S., Ezra, K., & Rajsingh, E. (2012). A novel fault tolerant service selection framework for pervasive computing. *Journal of Human-centric Computing and Information Sciences, 2*(5).

Siljander, P. (1988). Hermeneuttisen pedagogiikan pääsuuntaukset. Main orientations in Hermeneutic pedagogigcs. Oulun yliopiston kasvatustieteiden tiede-70 kunnan tutkimuksia 55. Oulu: Oulun yliopisto.

Stajano F. & Clayton R. (2011) Cyberdice: Peer-to-Peer Gambling in the Presence of Cheaters. In B. Christianson, J. A. Malcolm, V. Matyas, & M. Roe (Eds.) *Security Protocols XVI. Security Protocols 2008. Lecture Notes in Computer Science, Vol. 6615*. Springer.

Stonebraker, M., Madden, S., Abadi, D. J., Harizopoulos, S., Hachem, N., & Helland, P. (2007). The end of an architectural era: It's time for a complete rewrite. *Proceedings of the 33rd International Conference on Very Large Data Bas*es (pp. 1150-1160).

Straub, J., & Traylor, T. (2018). Introduction of a Maritime Model for Cyber and Information Warfare. *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, (pp.25-29). IEEE.

Streefkerk, R. [Online]. (2019). Inductive vs. deductive reasoning. *Scribbr*. Retrieved 2nd of September from https://www.scribbr.com/methodology/inductive-deductive-reasoning/.

Stubbs, J., Menn, J., & Bing, C. (2019, June 26). Inside the West's failed fight against China's 'Cloud Hopper' hackers. Reuters Exclusive. Retrieved 19th of April 2020 from https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

Finnish Security and Intelligence Service. (2019). National Security Review. The Finnish Security and Intelligence Service. 5th of December 2019.

Tavares, T., Teodoro, G., Kurc, T., Ferreira, R., Guedes, D., Catalyurek, U., ... & Saltz, J. (2007, May). An efficient and reliable scientific workflow system. *Seventh IEEE International Symposium on Cluster Computing and the Grid (CCGrid'07)* (pp. 445-452). IEEE.

TechTarget. (2020). Definition, service-level agreement (SLA). TechTarget. Updated January 2020. Retrieved 26th of April 2020 from https://searchitchannel.techtarget.com/definition/service-level-agreement

Tolga, I. (2019). Whole-of-Government Cyber Information Sharing. CCDCOE. Tallinnn 2019. Retrieved 28th of April 2020 from https://ccdcoe.org/uploads/2019/06/Cyber_Info_Sharing_Ihsan_Tolga_CCDCOE_June_2019-.pdf.

Truong, H., Dustdar, S., Götze, J., Fleuren, T., Müller, P., Tbahriti, S.,Ghedira, C. (2011). Exchanging Data Agreements in the DaaS Model. *IEEE Asia-Pacific Services Computing Conference* (pp. 153-160). IEEE Computer Society.

Tseng, F., Chou, L., & Chao, H., (2011) A survey of black hole attacks in wireless mobile ad hoc networks. *Journal of Human-centric Computing and Information Sciences, 1*(4).

TUVE. High-Readiness Network. The State Security Networks Group Finland. Retrieved 25 April 2020 from https://www.erillisverkot.fi/en/services.

UK Cabinet Office, National security and intelligence, HM Treasury, & Hammond, P. (2017). National Cyber Security Strategy 2016 to 2021. UK Cabinet Office, London. 11 Sep 2017.

US-CERT. (2017). U.S. Department of Homeland Security:Alert report. Retrieved 27th of May 2017 from https://www.us-cert.gov/ncas

US-CERT. (2020). U.S. Department of Homeland Security:Alert report. Retrieved 28th of April 2020 from https://www.us-cert.gov/ncas.

US JCS. (2018). Cyberspace Operations. Joint Publications Operations Series: Joint Publication 3-12. United States Joint Chiefs of Staff. 8.6.2018.

US JCS. (2020). DOD Dictionary of Military and Associated Terms. US Department of Defense Terminology Program. United States Joint Chiefs of Staff. January 2020.

US White House. (2017). National Security Strategy of the United States of America. The White House, Washington D.C., December 2017.

VAHTI. (2016) Information security guidelines for business continuity. Latest version 2/2016. Ministry of Finance. Retrieved 25th of April 2020 from https://www.vahtiohje.fi/web/guest/home.

Vargas, J. & González, D. (2016). Model to assess supply chain resilience. *International Journal of Safety and Security Engineering, 6*(2), 282-292.

Vaquero, L., Rodero-Merino, L., Caceres, J., & Lindner, M. A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review, 39*(1), 50-55.

Wang, L., Tao, J., Kunze, M., Castellanos, A., Kramer, D., & Karl, W. (2008). Scientific Cloud Computing: Early Definition and Experience. *IEEE International Conference on High Performance Computing and Communication*s (pp. 825-830). IEEE.

Wang, X., Sang, Y., Liu, Y., & Luo, Y. (2011) Considerations on Security and Trust Measurement for Virtualized Environment. *Journal of Convergence, 2*(2), 19-24.

Xia, H., Jia, Z., Ju, L., Li, X., & Zhu, Y. (2011). A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules. *2011 IEEE/ACM International Conference on Green Computing and Communications (GreenCom)* (pp. 124-130). IEEE.

Xiong, L., & Liu, L. (2003, June). A reputation-based trust model for peer-to-peer e-commerce communities. *CEC 2003. IEEE International Conference on E-Commerce, 2003* (pp. 275-284). IEEE.

Yeo, C. S., & Buyya, R. (2006). A taxonomy of market-based resource management systems for utility-driven cluster computing. *Software: Practice and Experience, 36*(13), 1381-1419.

Yle Uutiset. (2014). Supo: Ulkoministeriö joutui kaksi kertaa vakoilun kohteeksi. Retrieved 28th of April 2020 from http://yle.fi/uutiset/3-7332824.

Zeng, Y., & Xiao, R. (2015). A networked approach to dynamic analysis of social system vulnerability. *Journal of Intelligent and Fuzzy Systems, 28*(1), 189-197.

Zhou, Z. X., Xu, H., & Wang, S. P. (2011). A Novel Weighted Trust Model based on Cloud. *Advances in Information Sciences and Service Sciences*, *3*(3) 115-124.

ORIGINAL PUBLICATIONS

I

2011 IEEE. Author manuscript in accepted version,
published with permission. If citing, please use:
Klaus Zaerens
Enabling the Benefits of Cloud Computing in a Military Context
2011 IEEE Asia-Pacific Services Computing Conference, Jeju Island, 2011, pp. 166-173.
https://doi.org/10.1109/APSCC.2011.42

2011 IEEE Asia -Pacific Services Computing Conference

Enabling the Benefits of Cloud Computing in a Military Context

Klaus Zaerens
Department of Military Technology
National Defence University
Helsinki, Finland
Klaus.Zaerens@iki.fi

***Abstract*— Cloud computing has been a topic of keen interest in recent years, having been referred to as "the emerging paradigm for the last five years", "the most promising computational platform" and "the prevailing technique for next ten years". There has been a lot of discussion as to what new opportunities it can bring to markets, what benefits it can offer, and what system development possibilities it enables for software development. In this paper we discuss cloud computing in a military context. We define the key features and characteristics of the cloud in public authority environments. We address the most essential problems and obstacles to be considered before the benefits of cloud computing can be fully enabled therein. As a solution to problems with the adoption cloud computing in public authority environments, we propose a new service model called Knowledge Management as a Service, which also improves usability. The discussion and views presented in this paper can be adopted in any organization with doubts concerning the sensitive and classified contents of current ICT systems in cloud computing.**

Keywords: Cloud computing; Service models; Administrative Data Processing; Military

I. INTRODUCTION

Cloud computing is at the peak of its hype cycle. However, the business world and research have not progressed at the same pace. The business world has acknowledged the benefits of cloud computing with regard to the cost-effectiveness of IT infrastructure and computing. Expectations are also high for new cloud computing markets [1,2]. It is widely believed that cloud computing will be the prevailing technology for the next five years. The technology itself is not new, but the maturity of old technologies has enabled their combination into a paradigm now presented as cloud computing. In the business world, there is a desperate hunt for clients and applicable environments and applications to make good on the paradigm's claims: cost-effectiveness, scalability and fault-tolerance. Cloud computing is gaining critical mass and creating a market for itself. At the same time as business vendors are securing their market share, various research groups are still struggling to come to an accurate definition of cloud computing and identify the potential problems it entails.

There has been some discussion of and projects related to the use of cloud computing technology in the military. Naturally, the systems that have been publicly presented have not contained any real military mission-critical data, such as combat data. The benefits of cloud computing that can be achieved in these kinds of systems are the same as those that can be achieved in any business: cost-effective computing and a decrease in the total costs of ownership (TCO).

In this paper, we will discuss issues and problems to be considered when implementing cloud computing in core authority systems. We define the key features and characteristics of such a cloud environment. We also characterize the environment's limitations and provide examples of corresponding measurable parameters. We will narrow our observations to military systems in which the need for computational capacity is high and the reliability of information is always critical.

As a solution to problems with the adoption of cloud computing in public authority environments, we propose a new service model called Knowledge Management as a Service, which also improves usability.

The paper proceeds as follows. First, we will examine the essence of cloud computing by defining its relevant terminology, characteristics and principles, as well as the benefits of the technology within the scope of a military context. Next, we address the main problems or obstacles that prevent these benefits from being enjoyed in a military context. Lastly, we propose possible solutions or indicate future work to be done to overcome the obstacles described. We will conclude with key findings and a description of the future of cloud computing in the military context.

II. ABOUT CLOUD COMPUTING

The point of cloud computing is to enable the use of IT infrastructure more cost-effectively and offer greater pervasiveness. Cloud computing has derived characteristics from different technologies, paradigms and architectures, such as distributed computing, grid computing, pervasive computing, service oriented architecture, utility computing, Internet computing and global computing. Because of this, it has not been clear that we are dealing with a whole new paradigm. Paradigm comparisons have been made especially with grid computing, utility computing and pervasive computing [1,3,4]. We share the views of Wang and von Laszewski that cloud computing is definitely a distinct paradigm from those mentioned above.

There has been also a lot of discussion about an accurate definition of cloud computing. The definitions presented vary more or less according to the organizational, business or operational environment or interests [1,3,4].

978-0-7695-4624-7/11 $26.00 © 2011 IEEE
DOI 10.1109/APSCC.2011.42

III. CLOUD COMPUTING CHARACTERISTICS AND BENEFITS IN PUBLIC AUTHORITY ENVIRONMENTS

In this paper we extend the definition of cloud presented by the NIST (National Institute of Standards and Technology) [5].

A cloud is considered an enormous, scalable system. It is always available, so customers can use its resources on an on-demand basis. A cloud should also be easy to use. It is location- independent and accessible through the network. The complexity of the underlying technology is hidden from the end-user. The primary characteristics of cloud computing in public authority environment in general and especially in military environment are listed in Table I.

In the systems of public authorities or government agencies, the usage of clouds is more restricted than usual. With confidential content, a scenario where the consumer doesn't actually have any control over the location where data is processed is unacceptable. Despite virtualization, data is always processed on some physical server that is subject to the laws of the country in which it is located. Especially in military systems, it is crucial to know at least where data is processed and what organizations and administrative authorities have access to the data.

Cloud computing is claimed to be cheaper than having an onsite network system. This argument is based on the fact that the organization does not have to buy servers of its own; they simply pay for the use of resources that exist in the cloud. If the organization builds its own computational infrastructure, the system must be scaled so that relatively infrequent peak loads can be processed [6]. If an organization chooses not to underprovision their system, their hardware layer will be excessively capable. The result is that the system is expensive and will be idle most of the time. In the cloud paradigm, an organization uses the resources on an on-demand basis and can expect to always have enough resources. At times of peak load, the system's resources in use scale up, and once the peak is over, the resources in use scale down. Scaling up doesn't necessarily cost any more than basic use. In the cloud there are no costs of ownership. This is why outsourcing infrastructure to the cloud tends to be very tempting to many corporations. From the cloud resources' vendor's point of view, this kind of scaling improves the utilization of physical hardware when the cloud is large and serves numerous customers. In addition, the larger the cloud, the smaller the hardware acquisition costs, and with technological homogeneity in operations, the total costs per operation are smaller than the organization owning its own onsite hardware. This leads to cheaper vendor prices for customers and so on.

Examining cloud computing characteristics in private clouds can be accomplished by examining the overall benefits of cloud computing in private clouds. Private clouds roughly resemble private networks. The system scales within the hardware of the system. The hardware can be leased instead of owned, but multi-tenancy at the service, data or application level is usually limited. Savings from the decrease in TCO are indirect and enabled by better utilization of existing hardware.

TABLE I. CLOUD COMPUTING CHARACTERISTICS IN A PUBLIC AUTHORITY ENVIRONMENT.

Characteristic	Description
Data processing	Unlimited computational capabilities and storage of the cloud enable processing of greater amounts of data.
On-demand self-service	Consumers connect to the cloud and request resources from the cloud as needed. The cloud infrastructure and services comply with consumer demands.
Security	Consumers' access to resources and data is strictly controlled, monitored and limited by access rights.
Broad network access	The cloud can be accessed over the network by standard mechanisms from any location with any kind of device.
Excessive knowledgebase	All relevant information from various sources is available to consumers at all times.
Resource pooling	The computing resources support multi-tenancy. Physical and virtual resources are dynamically assigned and reassigned according to consumers' demands. A given arbitrary consumer does not necessarily have any control over or knowledge of the exact locations of resources.
Rapid elasticity	Cloud capabilities can quickly scale in and scale out. To consumers, capabilities appear to be unlimited.
Traceability	Every action by a consumer or in a service in the cloud must be traceable.
Survivability	The cloud system must be fault tolerant. It should automatically recover to an operational state from different disaster scenarios.
Measured Service	Cloud systems automatically control and optimize resources. Resource usage can be monitored, controlled and reported.

The main benefits for the military lie in the usage of SOA-based applications in a virtualized platform, which gives leverage to the utilization of existing hardware. Furthermore, in private clouds, the technical homogeneity of the system improves manageability and operating costs. With standardized and consistent platforms, it is possible to develop automated maintenance routines that deliver savings in the long run.

At first glance, it seems that the benefits of pay-per-use don't apply in a cloud bounded by organizational limits. However, monitored and measured resources and usage control mechanisms enable optimization of resources within the organization and guarantee service levels for individual departments or divisions.

The other benefits of cloud computing are related to the underlying technology. Homogeneity within the service layer facilitates better manageability. Service orientation and decoupling are essential features for geographic distribution of systems and resilient computing [7].

Virtualization, distribution and scalability improve the reliability of cloud systems and offer better fault tolerance and a solid platform for advanced disaster-recovery techniques.

IV. Cloud computing service models

Service models in general imply where the cloud is used. The service models relevant in authority environments are listed in Table II. Hardware and Data as a Servcice (HaaS and DaaS) are low-level services for the customers' specific needs. The DaaS service model is usually presented in the service model hierarchy at the same level as Platform as a Service (PaaS). It is described as data provider service that in practice refers to direct database connections. This low-level presentation ensures data redundancy, consistency and accessibility. It also allows us to avoid the problems arising from the loose coupling and stateless features of Software as a Service (SaaS). With DaaS as a separate service model, we want to emphasize the importance of information management in systems that contain confidential data. Infrastructure as a Service (IaaS) refers to fundamental computing resources, such as networks, storage or processing as a whole. IaaS hides the details of HaaS and DaaS. PaaS hides the details of infrastructure and offers a programming environment and tools to the customer. SaaS hides the details of the infrastructure and the programming environment and offers customers a service pool that can be accessed by any kind of device platform. By combining services, it is possible to create and deploy new applications. Knowledge Management as a Service (KMaaS) is proposed as a high-level service for a customer. It provides a view of all information essential to the customer. The technology, applications or location of data are not relevant. KMaaS enables easy access to the resources and services of the cloud. We discuss KmaaS in greater depth later in this paper.

TABLE II. Cloud computing service models in a public authority environment.

Cloud Service Model	Description	Customer level
Knowledge Management as a Service (KMaaS)	The customer can access knowledge in a more pervasive way.	Personnel (e.g. Operations manager)
Software as a Service (SaaS)	The customer can use the provider's applications over a network	Unit in an organization (e.g. Operations center)
Platform as a Service (PaaS)	The customer can deploy customer-created applications to a cloud	Division in an organization (e.g. Operations division)
Infrastructure as a Service (IaaS)	The customer can rent processing, storage, network capacity, and other fundamental computing resources from cloud.	Organization (e.g. operations department)
Data as a Service (DaaS)	The customer can store and access data. Service ensures consistency and redundancy. Typically DaaS is an implementation of a database.	Organization (e.g. operations department)
Hardware as a Service (HaaS)	This is a lower-level service than IaaS. The customer can specify precisely the type of resources of services needed. For example a service can include a server or a firewall.	Organization (e.g. operations department)

V. Cloud computing deployment models

The deployment models that are commonly recognized are public clouds, private clouds, community clouds and hybrid clouds (see Table III). A public cloud is open to the general public or to a partnership of several industry groups. A public cloud is owned by an organization selling cloud services. A private cloud is dedicated to a single organization. A cloud can be located on the organization's premise or offsite. The community cloud infrastructure is shared by several organizations and supports a specific community that has a shared interest, such as a policy or mission. A hybrid cloud is a composite of two or more clouds (private, community, or public). In this model, the clouds remain independent but share a standardized interface, which enables the portability of services.

Applying service models in private clouds does not differ from applying them in other cloud deployment models. PaaS and IaaS are important models in the adoption of legacy systems. However, to gain long-term benefits, it is essential that new applications and software are developed according the Service Oriented Architecture (SOA) standard and used in production as SaaS.

The demand for control of the physical data location in the cloud restricts the use of public clouds as a deployment model in the military context. A private cloud is best for organizations that value features like security, compliance, governance and interoperability. A community cloud can be considered, if every party in the community and the cloud vendor can be trusted in terms of confidentiality. A community cloud may consist of different authorities' environments; from the military aspect, it might be useful to have access to its resources via a hybrid cloud. In addition, we argue that the interface to resources in the external cloud should be one-way: the private cloud sees itself as part of the hybrid cloud, but the external cloud has limited (or no) visibility to resources in the private cloud.

TABLE III. Cloud computing deployment models.

Deployment Model	Description
Private Cloud	Enterprise owned or leased. Reminiscent of an organization's private network.
Community Cloud	Shared infrastructure for a specific community
Public Cloud	Sold to the public, mega-scale infrastructure. One cloud can include numerous vendors.
Hybrid Cloud	Composition of two or more clouds

VI. Problems and obstacles

As stated earlier, the technology used in cloud computing is not new; it is simply a new combination of old technologies. That is why a cloud environment inherits every technical problem from its original master technologies. It is stated that the new combination of technologies solves or makes old problems less significant. This argument has not been proven in practice, but theoretically, in a virtualized environment, automated scaling techniques can decrease the impacts of failures or exceptions and improve a system's overall fault tolerance.

One of the presumed benefits of cloud environments is their large size: as a matter of fact, the idea is to have a system in which resources are not limited. Theoretically, it is impossible to have a fully controlled test environment that is similar to a production environment. Of course we can predict how a system or an application will behave, but new problems may arise after the boundaries of a test environment have been exceeded. For example, at some parts in the cloud there may be poor network connections or limited bandwidth, or the cloud could also be so large that fetching critical data results in intolerable latency or an unmanageable amount of computing nodes.

The main driver for cloud computing is business needs. Challenges may also be business related instead of technical. For example, a customer accesses the cloud from a location where the computing load is already heavy. It is possible that, over some period of time, a certain customer's service level agreement (SLA) is breached although the cloud is fully functional. It is obvious that the real problems that have the potential to occur have not yet been fully understood and cannot be verified until the paradigm is implemented in practice.

There are numerous articles and blog posts about technical problems and lists of obstacles that must be overcome before cloud computing can conquer the world. Below, we point out the five most critical problems that must be resolved before the benefits of the paradigm can be exploited fully in operational and tactical military systems. With regard to these problems, a characterization of limitations in a public authority environment and examples of corresponding measurable parameters are listed in table IV.

TABLE IV. CHARACTERIZATION OF LIMITATIONS IN A PUBLIC AUTHORITY ENVIRONMENT.

Limitation	Example of parameters
Knowledge timeliness	• Age of information • Toleration limits for age of information
Knowledge correctness	• Error margin of information
Knowledge reliability	• Probability of incorrect information
Latency for computation	• Bandwidth • Data size • Amount of computing nodes • Service propagation • Computational variables (MIPS, processors) • Utilization of services
Latency for service	• Availability of services • Idle time of services • Service propagation
Fault tolerance	• Usability • Recovery time • Downtime / month
Complexity of the cloud	• Number of layers • Number of vendors • Number of interfaces in architectural topology
Authorization	• Number of logical interfaces • Number of users • Number of user roles • Number of different device types • Number of computing nodes, networks, vendors

A. *Knowledge management*

Knowledge itself is the most critical issue in modern warfare. The party that owns the knowledge has the advantage. Knowledge can take the form of observations as well as commands or directives. The essential requirements for knowledge are consistency, redundancy, reliability, timeliness and availability. The demand for up-to-date knowledge shifts towards a demand for real-time knowledge when situations are rapidly changing over extremely short periods of time. Interesting issue arises if a prediction model is implemented to process data in a rapidly changing environment. Then the demand for availability of real-time knowledge can be relaxed, but increasing the error margin for the correctness of knowledge is compromised.

Knowledge management can also be considered data management from a technical point of view. The actual data that instantiates the abstract term "knowledge" has different features, depending on the producer of the data, the user of the data and the data content itself.

Another, more practical example of data management problems is real-time processing of applications during operational situations on the battlefield; in these instances, the system must be able to process huge amounts of data. The main problem is how to share up-to-date data with all who are connected to the application at all times, or replicate data to different physical locations within the network [8].

Cloud computing is presented as an infinitely scalable solution for data processing thanks to its exploitation of grid computing technologies. The benefits of cloud computing for overall system performance cannot be contested, but in a military context it still requires centralized data storage or a shared-nothing application architecture. In a shared-nothing architecture, computational units in the system have little or no common data. The data architecture has to be well planned and situations where replication is needed must be minimized to achieve an effective system. However, the usual technical data transfer rate in a private network is 100 MBit/s. 1 GB of data takes 4,000 seconds to transfer, which is about 66.5 minutes. It is obvious that a replication rate that slow cannot be tolerated in real-time systems. In other words, the data transfer is effective only with small amounts of data.

This kind of data problem is significant if one thinks about the broad network access feature of a cloud. In a military context, we could have a use case where a portable device connects to the cloud after long radio silence due to the commencement of a mission. Typical to this kind of situation is a low bandwidth rate (due to the wireless connection) and a huge amount of data to transfer (operational and tactical information). It is clear that after action in the field, the transferring of knowledge relevant to the mission must be a rapid process.

B. Capability limitations in private clouds

As stated earlier, cloud computing has theoretically unlimited computational scalability and decreases the costs of infrastructure by improving hardware utilization. In the context of private clouds, this kind of unlimited computational scalability is an illusion. Private clouds always have boundaries that prevent external connections and protect vital information. In other words, in terms of hardware and computational performance, the private cloud in general does not differ from a private network. Grid technology and different virtualization schemes harness the existing infrastructure in a more effective way and improve the utilization of existing hardware. The problems are guaranteeing that the most important information has privileges to computational resources at all times and accessing more computational capability for the private cloud when the load is at its greatest: in other words, how to bend the borders of the private cloud.

Let us use a military operational system as an example. In times of peace, most of the system's computational resources are idle. When a crisis escalates, it is obvious that computational resources are needed. It is important to ensure processing of the most vital operational data.

C. Fault tolerance and disaster recovery

One absolute demand for military systems is fault tolerance. The more critical the system in question, the less acceptable any downtime is. In addition, the more important the system is for success of the military operation, the more certainly the system will be the target of hostile actions.

The system should preserve and maintain critical knowledge and protect it from unauthorized users at all times. If an adverse event occurs in some part of the system, it should not affect availability of services or the assigning of computation resources.

D. Complexity of virtualization

The cloud environment is presented as easy to use for consumers. New virtualization techniques are used to conceal the underlying technical architecture. The virtualization also enables the scalability of the cloud environment. Data, resources and service management in a virtualized environment that scales up and down must have rigid control virtualization techniques that ensure dynamic provisioning; in addition, the transparency of location, data and services add logical complexity to the overall cloud system architecture. This kind of complexity naturally makes the origins of possible failures harder to find and resolve. In military context the cost of time consumed in detecting the root cause or finding and isolating the actual failure can become too expensive if some critical manual operation fails. The increasing complexity of system increases also the amount of difficulties to control the physical location of data. The consequence might be that data transfer time becomes too great for consumer specifically if operation demands real time data.

The demand for an easy user interface should be retained, while simplifying complexity to minimize the costs of operation.

E. Security issues

According to an IDC Enterprise Panel in August 2008, security is the most important issue in adopting a cloud model. The most central anxieties concern user and data isolation management, data multi-tenancy, encryption needs and compliance.

Implementing a cloud infrastructure as a private cloud solves most of the usual security-related problems in authority environments. In this case, then, the same security issues apply as in private networks. Security issues become slightly more challenging in the case of hybrid clouds. In a hybrid cloud, the same security demands for sensitive data and user control must be in effect in an external cloud as in a private cloud, regardless of security management models and vendors.

One of the golden goals in cloud computing is to use computational resources in a more pervasive way. This means that the user has access to cloud resources from anywhere [9, 10]. If we examine the origins of pervasive computing, we find an interesting possibility for the soldiers of the future. In the original pervasive computing paradigm, a given device can connect to a network's resources and services at any time and from any location [9]. The device and network environment negotiates the limitations and computational resources to be used. Imagine collecting operational information automatically via some kind of device that is a part of every soldier's equipment. In return commands, guidance and directives can be delivered from the back-end system. In this kind of system, new security issues arise concerning the devices connected to the back-end system. How can a military organization prevent that end-user device or the information that it receives and sends from falling into the wrong hands?

VII. Overcoming obstacles

In this section, we propose some possible approaches to overcoming the problems and obstacles stated in previous section. Some of possible solutions are related to the old technologies from which cloud computing has evolved.

A. Knowledge management as a service

Organizations whose operations and functions are distinctively information-centric need a new set of services or a whole new service layer in order to take advantage of cloud computing in a more pervasive way. We propose a new service model concept for the cloud, called Knowledge Management as a Service (KMaaS). It differs from DaaS in having additional built-in services through which data can be processed in a more intelligent way. As described earlier, DaaS is quite low level and data storage-centric. KMaaS expands DaaS with a more abstract point of view. The relationship between KMaaS and other service models is illustrated in Fig. 1. In Fig. 1, Hardware as a Service (HaaS) is presented as a point of comparison to DaaS.

In KMaaS, data is accessed via a metadata directory. In the metadata directory, additional properties, such as privileges, location information (source and storage) and timestamp (for preventing old information) are attached to information. The important possibility arising from this kind of metadata directory technique is information management in relation to the producer of the data, the user of the data or the data content itself.

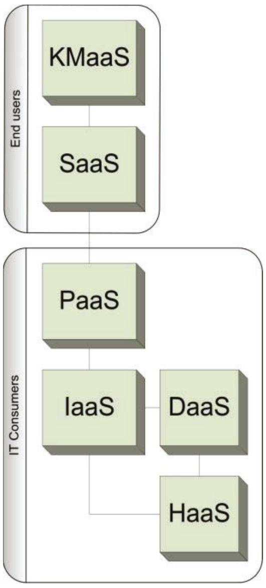


Figure 1. Service models in relation to consumers

In proposed concept, KMaaS has a rule engine and a rule repository in order to process data as instructed by the metadata directory. KMaaS has a built-in security model that controls authorization issues according to metadata directives and data handling procedures that fetch data and process it at the available locations. KMaaS is responsible for data redundancy, so replication control is built-in and automated. Fig. 2 illustrates the KMaaS framework architecture.

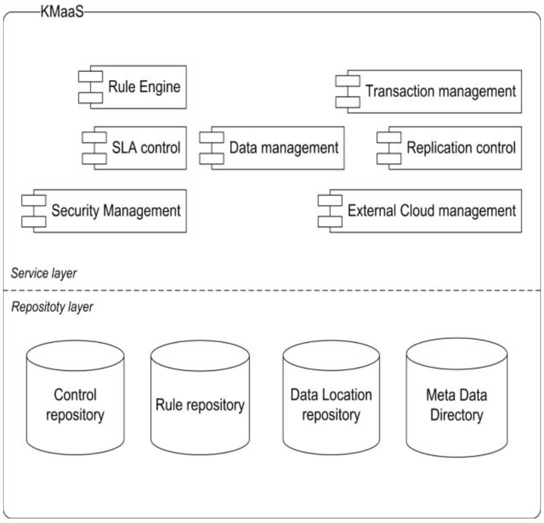


Figure 2. The logical architecture of KMaaS

On the other hand, in decision support systems, commands and directives must be undeniable across the cloud. The amounts of data processed are usually relatively small, but consistency, reliability and redundancy must be emphasized. This kind of information processing must have a data management system similar to the one we have used in the context of databases or workflows. It has been claimed that this kind of transactional management is not likely to be deployed in clouds in the near future [8]. We claim that transactional features are essential to adopting cloud environments for critical operational and tactical military systems. This is why KMaaS has a built-in framework that enables transactional features for processing information. However, this kind of transactional framework in cloud environments still needs some work at the conceptual level.

In the proposed concept, we facilitate dynamic computational behavior according the knowledge processed, data prioritization and authorization of knowledge. With replication control, we can improve the management of data redundancy. With transactional features we achieve improved data consistency, reliability and security as well as advanced recovery techniques. External cloud management enables service-level agreements between service providers and hybrid clouds in public authority environments. This significantly increases the availability of computational resources.

In military context KMaaS represents the interface to reliable, consistent and redundant data. The consumer can rely that the essential data for operation is available without time delays regardless the underlying system architecture.

B. Data prioritization

A hybrid cloud encompassing a community cloud used by national authorities can be the answer to capability limitations during crisis. This expands and transforms the problem a little: How do we determine which data or tasks can be processed within the community cloud? A community cloud is not as secure an environment as private cloud, but during a crisis, the possible risks might be tolerable. The decisions are easier if the Department of Defense is itself the community cloud provider and investments in it are processed similarly as with any other purchases of military equipment.

But whether the question is what data is processed outside the private cloud or what data is processed at all, a more advanced form of data management by data classification or prioritization is needed. This might be achieved by mechanisms originally developed for managing SLA. Some interesting and useful research has already been conducted [11, 12, 13]. Still more work has to be done to ensure that the most critical computational tasks are computed regardless of the overall utilization rate within the system. After all, data prioritization and a controlling system will be added as a supported function in the KMaaS service model.

Data prioritization and classification have a more fundamental impact in cloud environments. It must be recognized that the infrastructure of new, information-centric cloud software needs to be developed in a more information-aware way.

C. Improving survivability in cloud applications

As mentioned earlier, survivability and fault tolerance are very critical issues to be managed in a military context. Several distinct approaches must be considered in improving fault tolerance, such as knowledge management-related data architecture and recovery techniques, and infrastructure-related service distribution and network topology.

The physical distribution of hardware, data and services is essential in a military context. The cloud must be structured in independent sections. One requirement of a cloud section is to be able to maintain full operational capability in case of failure in some other section of the cloud. Sections are aware of communications costs among sections and automatically reroute a communications channel if needed. From a management point of view, a section must be possible to be separated from the cloud and potentially shut down.

Exception handling techniques are a more software-based approach to ensuring system survivability [14, 15]. This solution is associated with the information management examined earlier. Transactional management of data enables developing advanced recovery techniques when data reliability, consistency and redundancy are high-priority issues [8, 16, 17].

Another issue related to knowledge management is data architecture. Data replication costs can be intolerable. These kinds of obstacles can be overcome by investigating data architecture within the cloud. A project called H-Store has been trying to solve this issue [18]. The basic idea is to physically maintain data so that the transfer distances are as small as possible. However, master data storage must be available in case of outage in “the best section”.

D. Solutions to the underlying complexity of virtualization

Virtualization adds logical complexity to a system. The homogeneous nature of a cloud implies that automated processes can be found to decrease the number of administrative tasks. However, more research should be conducted in the field of configuration and data management in virtualized environments in order to exploit all possibilities.

For application and service developers, the underlying problems ought to be hidden. Service or application cloudability becomes a demand for application and service development. The term “cloudability” can be defined as an characteristic of a software implementation that (referring to the NIST definition) takes full advantage of the cloud paradigm, by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability [5].

E. Advanced security

For flexible provisioning of resources within the cloud, security and identity management must inevitably be unified within the cloud environment. The development of provisioning, data and support services have improved fault tolerance and on-demand security controls [13,19]. On the other hand, encryption needs, user and data isolation, data masking and multi-tenancy are still challenging.

We propose that user identity, security and isolation management be handled by centralized services, as in traditional private networks. In case of absolute data isolation, we also propose a centralized approach unless data can be managed by shared-nothing architecture.

In order to achieve the most secure infrastructure, it is important to recognize that security implementations must be extended to software development [5]. Features supporting identity and security management can be considered a demand for cloudability.

In ensuring security in the hybrid cloud deployment model, we propose that a hybrid cloud have a one-way connection. In this case, security management is more controlled and access to the private cloud is handled as within an organization’s private network. It is important that users demand resources from and always connect to a primary private cloud. If more resources are needed, the private cloud’s resource manager requests resources from an external cloud according to the preset SLA [13]. The manager of the private cloud has full control over the data that needs to be processed and has the necessary information on confidentiality of data. This procedure ensures resource transparency to the end user and prevents leakage of sensitive data to external infrastructure.

Obstacles to achieving this futuristic vision of more pervasive connectivity in a military context still remain. Problems with client devices that are automated and even online will need more work to resolve. It is clear that the main security management methods have little to offer in terms of securing this kind of equipment. In the worst-case scenario, devices could open a back door to the cloud system. More research has to be done and new, creative out-of-the-box solutions are needed.

VIII. Conclusions

In this paper we examined the cloud paradigm within the military context. We stated that the core operational and tactical systems must be bounded by the limits of a private cloud. Yet we noted that hybrid clouds might bring more capability to the overall system.

We identified the five primary obstacles to adopting cloud environments in a military context and examined possible solutions to overcoming them. We proposed a new service model concept called Knowledge Management as a Service (KMaaS), which improves the control of information and data across the entire cloud. This service model includes a frame architecture for transaction management in order to enable more advanced disaster-recovery methods. KMaaS also includes a metadata directory for processing information consistent with data content. KMaaS enables a more pervasive approach to cloud computing by hiding the complexity of the underlying technical data architecture. KMaaS ensures data consistency, redundancy and reliability, which are essential requirements for data in a military context.

With KmaaS, we facilitate the usage of computational resources according to information content. We also achieve improved data management with transactional features as well as advanced replication control, while enabling external cloud management and theoretically unlimited computational resources in public authority environments.

References

[1] L. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner. A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39(1), January 2009, pages 50-55

[2] H. Erdogmus. Cloud Computing: Does Nirvana Hide behind the Nebula? IEEE Software archive, 26(2) March 2009, Pages: 4-6.

[3] L. Wang, J. Tao, M. Kunze, A. Castellanos, D. Kramer and W. Karl. Scientific Cloud Computing: Early Definition and Experience. IEEE International Conference on High Performance Computing and Communications, 2008, Pages: 825-830.

[4] L. Mei, W.K. Chan, T.H. Tse. A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues. IEEE Asia-Pacific Services Computing Conference, 2008, pages 464-469.

[5] P. Mell and T. Grance. The NIST Definition of Cloud Computing. Version 15, 7.10.2009. National Institute of Standards and Technology, Information Technology Laboratory. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

[6] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zahar. Above the Clouds: A Berkeley View of Cloud Computing. UC Berkeley Reliable Adaptive Distributed Systems Laboratory, February 10, 2009.

[7] W. Kim. Cloud Computing: "Status and Prognosis". Journal of Object Technology, vol. 8, no. 1, January-February 2009, pages 65-72.

[8] D. Abadi. Data Management in the Cloud: Limitations and Opportunities. IEEE International Conference on Data Engineering (ICDE 2009), 32(1), March 2009, Vol. 32 No. 1, pages 3-12.

[9] D. Saha and A. Mukherjee. Pervasive computing: a paradigm for the 21st century. IEEE Computer, 36(3): 25–31, 2003.

[10] H. Lu, W.K. Chan and T.H. Tse. Testing pervasive software in the presence of context inconsistency resolution services. Proceedings of the 30th international conference on Software engineering 2008, Leipzig, Germany, Pages: 61-70.

[11] D. Lamanna, J. Skene, and W. Emmerich. SLAng: A language for service level agreements. Proceedings of the 9th IEEE Workshop on Future Trends in Distributed Computing Systems. IEEE Computer Society Press, 2003, pages 100–106.

[12] J. Sauve, F. Marques, A. Moura, M. Sampaio, J. Jornada, and E. Radziuk, "SLA design from a business perspective," in Lecture Notes in Computer Science. Springer Berlin/Heidelberg, 2005, pages 72–83.

[13] B.R. Kandukuri, V.R. Paturi and A. Rakshit. Cloud Security Issues. IEEE International Conference on Services Computing, september 2009, pages 517-520.

[14] J. Eder, W. Liebhart, Workflow recovery. Proceedings of the 1st IFCIS Conference on Cooperative Information Systems, June 1996, pages 124-134.

[15] Z. Luo, A.P. Sheth, K.J. Kochut, and B. Arpinar. Exception handling for conflict resolution in cross-organizational workflows. Technical Report, LSDIS Lab, Computer Science, University of Georgia, April 2002.

[16] T. Tavares, G. Teodoro, T. Kurc, R. Ferreira, D. Guedes, W. Meira Jr, U. Catalyutrek, S. Hastings, S. Oster, S. Langella, and J. Saltz. An efficient and reliable scientific workflow system. IEEE International Symposium on Cluster Computing and the Grid (CCGRID 2007), March 2007, pages 445-452.

[17] L. Li, C. Liu, and J. Wang, Deriving transactional properties of composite web services. IEEE International Conference on Web Services (ICWS2007), July 2007, pages 631-638.

[18] M. Stonebraker, S. R. Madden, D. J. Abadi, S. Harizopoulos, N. Hachem, and P. Helland. The end of an architectural era (it's time for a complete rewrite). In Very Large DataBases, Vienna, Austria, 2007.

[19] L.M. Kaufman. Data Security in the World of Cloud Computing. IEEE Security and Privacy, 7(4), July/August 2009, pages 61-64.

II

2012 IJCSE Republished, with permission, from:
Klaus Zaerens
Gaining the Profits of Cloud Computing in a Public Authority Environment.
Int. J. Computational Science and Engineering, special issue on “Advanced Challenges and Research Trends in Cloud and Grid Interoperability,” 2012.
https://doi.org/10.1504/IJCSE.2012.049748

NOTIFICATION

Due to copyright laws the pages 109–119 (Article II) (including pictures) have been removed from this electronic version.

Please contact the Library of the National Defence University for a full printed version of this dissertation!

III

2012 Republished, with permission, from:
Zaerens, K., Mannonen, J.
Concept for the Construction of a High Security Environment in a Public Authority Cloud.
Lecture Notes in Electrical Engineering, Springer-Verlag, September 6, 2012.
https://doi.org/10.1007/978-94-007-5076-0_48

Concept for the Construction of High Security Environment in Public Authority Cloud

Klaus Zaerens[1], Jari Mannonen[2]

[1] National Defence University, Helsinki, Finland
Klaus.Zaerens@iki.fi
[2] Logica Suomi Oy, Karvaamokuja 2, 00380 Helsinki, Finland
Jari.Mannonen@Logica.com

Abstract. The economical pressure decreases budgets in the public sector which in turn increases the pressure for developing novel innovations to ensure adequate computational capabilities and resources in every operative scenario. Total costs of ownership prevent the construction of datacenters which are capable enough when the requirements for computational capabilities are greatest. In this paper, we propose a concept for the evaluation, standardization and deployment of cloud environments and public networks in order to dynamically extend the high security public cloud environment.

Keywords: High Security, Network, Cloud computing, Public Authority.

1 Introduction

Building a high security cloud infrastructure and support for service model layers is time-consuming and requires a great number of decisions and contracts with hardware and software suppliers and environment providers. In addition, infrastructure is usually scaled for the estimated use of resources. However, computational infrastructure must be scaled so that the relatively infrequent peak loads can be processed [1]. If it is decided that a cloud system is not underprovisioned, the hardware layer will be excessively capable. Resource pooling and elasticity of computational resources can be achieved in most of the clouds provided today. New problems emerge when there is more data to be computed than one cloud can process and the essence of information or operations processed require ultimate security. This kind of a situation can occur in a public authority environment during a natural disaster or a similar crisis; or in the military context during a threat to national security; as well as in smaller scale in the private sector with excessively survivable systems or classified development projects. It is obvious that especially in the public authority context it is not possible to make preparations for the highest peak of resource consumption described above. During peak loads, the amount of data is huge and it exponentially increases over a small timescale at the operational level. At that time it would be too late to build a network capable enough to meet the resource requirements. It is also necessary that computational resources are geographically available where needed and that the expansion of resources is controlled. Therefore, predictive actions must be executed both during the

James J. (Jong Hyuk) Park et al. (eds.), EMC Technology and Service,
LNEE 181, pp. 401–408, DOI: 10.1007/978-94-007-5075-3_48,

early preparations phase of network infrastructure and in the planning phase of operations performed when composing a secure public authority network. These predictive actions must be targeted at the existing computational system environments, such as commercial clouds infrastructures and datacenters. In this paper, we propose a solution to enable and harness the theoretically unlimited computational resources for public authority use, as well as a standardization method needed and actions to be performed during this process.

This paper proceeds as follows: First, we will introduce the process on preparatory actions for enabling an extendable high security private cloud. Next, we propose a standardization method needed with existing cloud environments in order to expand the cloud environment when capability requirements increase. Lastly, we propose a process needed in the expansion. We will conclude with key findings.

2 Preparatory Actions for Enabling Extendable High Security Private Cloud

As has been discussed in paper [2], the demand for controlling the physical data location in the cloud restricts the use of public clouds as a deployment model in security authority and especially in military context. However, if we determine the physical boundaries of the possible cloud environment in existing public clouds before building the actual private cloud, this restriction can be relaxed. In other words, as the requirements for computational capabilities and resources increase, we extend the private cloud infrastructure in the existing public cloud hardware to meet the new requirements. This expansion of the network must geographically focus on the area of activity where privacy and security can be ensured.

In addition to geographical issues, multiple other properties of possible cloud extensions must be considered in evaluating their suitability for a high security cloud. These properties are listed in table 1. It is essential to focus on elasticity and latency properties of possible clouds. Elasticity ensures the adaptation of high security control policies as well as connectivity to the core cloud. Latency properties are indicative of the performance of operations and of possible bottlenecks in data transmission.

Table 1. Properties to be considered in evaluating the suitability of cloud infrastructure for extendable high security cloud environment.

Property	Description
Geographical location of the network infrastructure	The network should be physically located in the area of public authority jurisdiction.
Elasticity of the network infrastructure	The network infrastructure must support elasticity and dynamical adaptation of new control policies. The physical network connection must be easily disconnected and changed to be used with secure cabling.

Secured maintenance and supply	Network infrastructure maintenance should be secured at all times, and the supplied techonology should be universal, replaceable and repairable. The distribution of electricity should also be secured and the readiness of reserve power ensured.
Clustered cabling between cloud environments	Cabling between central cloud environments must be fault tolerant. Cabling must be constructed so that it will not introduce a single point of failure. Two physical clouds are cabled with two separate cables which are routed geologically by different paths.
External cloud latency time	The external latency time refers to latency between the core public authority cloud and the extended cloud.
Transformation time to high security cloud	Transformation time refers to the time it takes for the core cloud to adopt a new external cloud. This is the time it takes for an external cloud to be converted into a compatible one and connected to the high security private cloud.
Virtualized node level minimum requirements (cpu/memory/disk)	The minimum requirements for one node within an extended cloud. This depends on the applications which are planned to be implemented in the secure cloud infrastructure.
Application requirements for virtual node	Software requirements for the nodes in the virtual machine, that is, the required OS, system software, extensive language support (PHP, Java, etc.) and possible database support
Node subdomain support and configuration time	Some of commercial clouds contain the support by default if required within a secure cloud. Configuration time refers to the time needed for a node to convert from an external cloud to a high security cloud.

Cloud extensions can be used for different tasks by different organizations. By defining these purposes of computation, exact requirements for the cloud extension can be determined. In predicted high activity areas the focus should be on geographical dimensions of the extensions so that a pervasive approach can be ensured for the authority and data transmission latencies can be tolerated [3]. Computational and geographical requirements narrow down the possible network topology and the infrastructure that can be selected for the extensions of the secure cloud. After the cloud environments used in the extensions of the secure cloud have been selected, requirements of standardization are set for the corresponding cloud providers. In the final state, cloud providers have met the defined requirements and extendibility can be tested and confirmed. The extendibility of cloud extensions must be ensured regularly. At each phase of preparatory actions documentation and reports must be updated. Written documentation forms the basis for making decisions on how to extend high security at a time of extensive computational needs. The process described is illustrated in figure 1. The requirements set for cloud providers will be discussed in the next chapter.

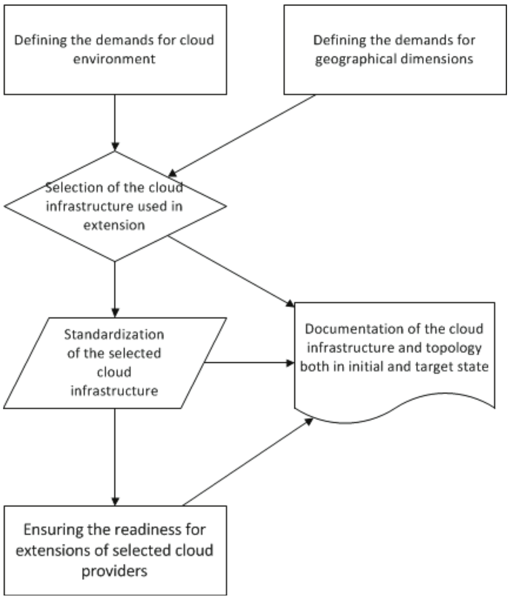

Defining the demands for cloud environment
Defining the demands for geographical dimensions
Selection of the cloud infrastructure used in extension
Standardization of the selected cloud infrastructure
Documentation of the cloud infrastructure and topology both in initial and target state
Ensuring the readiness for extensions of selected cloud providers

Fig. 1. The process for preparatory actions.

3 Requirements for Standardization of a High Security Public Authority Cloud Environment

In order to construct a high security cloud for sudden resource requirements on top of an existing cloud infrastructure it must be ensured that the existing clouds have similar features among each other. This is enabled by setting consistent standardization requirements for the clouds used in the construction. In this chapter, we propose standard properties to be set as requirements for those cloud infrastructures which are selected to the target cloud infrastructure. This standardization enables support for the actual process in which the secure cloud is constructed.

In this paper, we adopt survivable cloud network characteristics in the public authority environment presented in paper [2]. Survivability and fault tolerance are very critical issues to be managed in the public authority context. Several distinct approaches must be considered in improving fault tolerance, such as knowledge management-related data architecture and recovery techniques as well as infrastructure-related service distribution and network topology. However, these characteristics need to be extended in order to meet the requirements of a sudden network expansion. The requirements are listed in table 2.

The requirements ensure the elasticity and readiness of the network infrastructure, as well as acceptable operational performance during the normal operation before the extension. The actual requirements are determined according to the cloud environment needed; for example, the military has different special requirements than other public authorities, such as the police forces. In Finland requirements for high security networks are specified at the ministry level [4].

The standard minimum requirements define the minimum level cloud requirements for the cloud to be connectable with the high security cloud environment. The physical characteristics should meet the requirements of the security requirements. This includes secured maintenance and supply as well as constructional structure of the facilities. The Statement on Auditing Standards No. 70 (SAS 70) can be used as an initial requirement for the physical security of a datacenter [5]. Internal latency times should be kept within required levels. Spin up and spin down times of nodes should also meet the standardization requirements. These spin up and down times affect the elasticity of the network infrastructure. In the survivable and high security cloud environment, the activation time of the cloud and the spin up time of the nodes are more crucial than the spin down time. Depending on the applications which are implemented in the cloud, it is possible that the spin down time becomes more crucial; for instance, if the cloud environment is running at its peak performance levels and computing power is needed to run some other high priority application. However, the spin up time concept can be taken further to include the adoption time of the whole extendable cloud to be used as a part of a high security cloud. The adoption time of the cloud is in fact the time that is needed to convert a connectable cloud to be used as a part of a secure cloud.

Table 2. Requirements of high security cloud for a cloud environment used as an extension of computational capabilities

Requirement	Description
Section-based network topology	Nodes must be grouped into sections (e.g. switched fabric topology).
Section isolation and independency	Sections should not be dependent on the resources of other sections or parts of networks. A section includes its own data and content management functions and service repositories.
Operation automation	Sections contain a support for automated administrative operations.
Ubiquitous manual management and control	It is possible to access cloud and section management and control at any section.
Failure detection	Features for the detection of failures in the local and neighbouring nodes
Advanced recovery	A section can automatically recover from failure and is capable of adjusting its own configuration according to the changed environment.
Fault tolerance	Shutdown of any node, server or section does not affect the rest of the network.
Trust management between server nodes	Continuous trust analysis of the neighbouring nodes
Support for transaction management	Support for transaction management at a high level service model such as Knowledge Management as a Service (KMaaS) or at low-level service models ensuring reliability, redundancy and consistency

Support for data replication	Data replication management support operates at the infrastructure level and is low-level support ensuring data transfer according to user requirements and needs.
Cloud datacenter external connectors	The datacenter connection must be duplicated from the different parts of the datacenter. If one external connector is broken, it must not affect the others.
Cloud datacenter electricity requirements	Electric power supply must be secured and readiness of reserve power ensured.
Physical characteristics of a cloud datacenter	Physical requirements of the datacenter must be within required standards. This includes the requirement for constructional structure of facilities and locations (e.g. altitude from sealevel, thickness of walls, geological environment).
Secure datacenter connections	The physical connection of the datacenter must be secure, that is, the cables must be secured and possibly doubled fully between the datacenters.
Cloud security infrastructure	The cloud extension must implement the same security policies than the core security cloud.
Internal cloud latency times	The data throughput rate in the cloud
Datacenter typing	The adopted cloud extension can be used within the public authority cloud in two ways: for delivering only the necessary computing power or as an interface for the operative connection point.
Node spin up time	The maximum time for starting a node in high security cloud
Node spin down time	The maximum time for shutting down a node in high security cloud
Node adoption time	The maximum time it takes for a node to convert into a node that is compatible with the high security cloud
Cloud adoption time	The maximum time for conversion and availability of a predefined group of nodes which are adopted to high security cloud
Node level storage requirements	The special requirements of data storage for nodes and minimum I/O latencies per node

4 Process for Dynamic Construction of Secure Cloud

In this chapter we propose a process for defining steps for the construction of a secure cloud. The cloud is constructed using the existing cloud infrastructure. To enable this, standardization and preparatory actions presented in previous chapters are needed. Usually the process of extending a public authority secure cloud environment is initiated due to some unexpected event. The process is illustrated in figure 2.

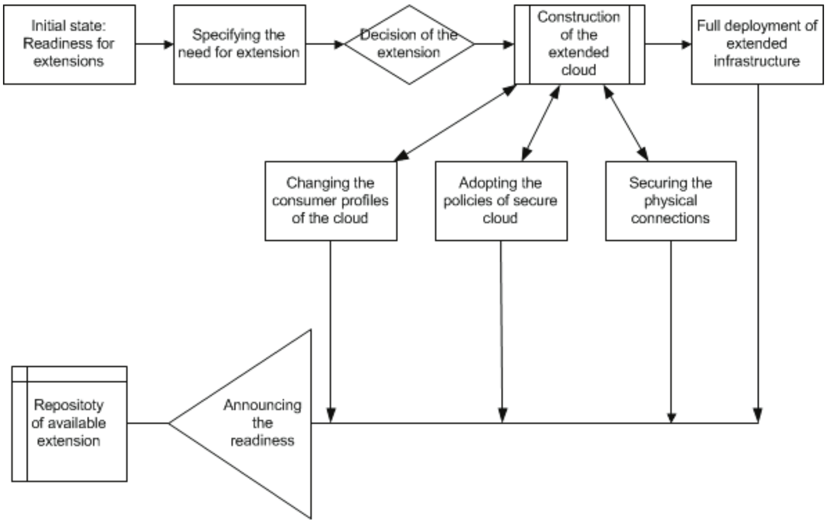

Initial state: Readiness for extensions
Specifying the need for extension
Decision of the extension
Construction of the extended cloud
Full deployment of extended infrastructure
Changing the consumer profiles of the cloud
Adopting the policies of secure cloud
Securing the physical connections
Repositoty of available extension
Announcing the readiness

Fig. 2. Process for Dynamic Construction of Secure Cloud.

In the initial state of the process, the readiness for possible extensions is ensured and tested. Requirements for the extension need to be determined: is there a need for data storage, pervasive connection or pure computation capability and what the number of needed resources is. Also the geographical location of the capabilities must be specified. After that the decision on necessary cloud extensions can be made according to the description of available cloud environments. At the construction phase the selected environments restrict traditional consumers from using cloud resources, adapt the policies of the high security network and secure the physical connections to the core public authority cloud. At each step of the phase the available configuration must be informed to the core cloud in order to dynamically start using the resources of the extended cloud. The deployment phase lasts as long as a decision on disassembling the extension is made.

5 Related work

There is a lot of current research concerning the improvement of security in cloud environments. Most of the approaches discuss security issues within the cloud. There are discussions about how two separate and different cloud infrastructures would ensure high security computational resources in hybrid cloud as stated in the NIST definition[6]. Considerations similar to ours are presented by Bisong et al. [7], Rochwerger [8] and Hwang [9]. However, all approaches have their limitations with regard tothe ultimate high security requirements.

6 Conclusions

In this paper, we have proposed preparatory actions and requirements for the standardization concerning cloud environments which can be used as capability and resource extensions to a high security cloud environment. We also proposed a process for the dynamic construction of the cloud.

Testing the readiness of extendibility of the selected clouds needs to be studied in more detail. It might not be possible to test full scale simulations before extensive computational capabilities are needed.

Standards and processes presented in this paper can be adopted in any environment where a separate private cloud environment needs to be built according to some SLAs. This approach enables us to develop tools for producing dynamic or temporary private clouds according to specific needs and demands.

Acknowledgements. This work has been partially supported by Logica in Finland (http://www.logica.com/) especially by Jan Mickos and Mikko Jylhä.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zahar, M.: Above the Clouds: A Berkeley View of Cloud Computing. UC Berkeley Reliable Adaptive Distributed Systems Laboratory, February 10, 2009.
2. Zaerens, K.: Gaining the Profits of Cloud Computing in a Public Authority Environment. Int. J. Computational Science and Engineering (IJCSE 2012), Special Issue on "Advanced Challenges and Research Trends in Cloud and Grid Interoperability".
3. Kim, W: Cloud Computing: "Status and Prognosis". Journal of Object Technology, vol. 8, no.1, January-February 2009, pp. 65-72.
4. Finnish Ministry of Finance: Hallinnon Turvallisuusverkkohanke TUVE (Security network program for administration), http://www.vm.fi/vm/fi/05_hankkeet/024_tuve/index.jsp.
5. NDB, LLP: Statement on Auditing Standards No. 70 (SAS 70), http://www.sas70.us.com/what-is/what-is-sas70.php.
6. Mell, P. and Grance, T.: The NIST definition of cloud computing. September 28, 2011. National Institute of Standards and Technology, NIST SP - 800-145.gg
7. Bisong, A. and Rahman, S.: An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.
8. Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I., Montero, R.; Wolfsthal, Y., Elmroth, E., Caceres, J., Ben-Yehuda, M., Emmerich, W. and Galan, F.: The Reservoir model and architecture for open federated cloud computing. IBM Journal of Research and Development, July 2009, vol.53, no.4, pp.1-11.
9. Hwang, K, Kulkareni, S. and Yue Hu: Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement. Dependable, Autonomic and Secure Computing, 2009. DASC '09, December 2009, pp.717-722.

IV

2015 Republished, with permission, from:
Zaerens, K.
Business Resilient Vulnerability Analysis for a Dynamic High Security Environment
Proceedings of the 2015 18th International Conference on Network-Based Information Systems.
September 2015, pp. 242–249.
https://doi.org/10.1109/NBiS.2015.39

2015 18th International Conference on Network-Based Information Systems

Business Resilient Vulnerability Analysis for Dynamic High Security Environment

Klaus Zaerens
Department of Military Technology
National Defence University
Helsinki, Finland
klaus.zaerens@iki.fi

***Abstract*— Vulnerability analysis methods have gained more interest in recent years, due to the publicity of international cyber attacks on critical infrastructure, emerging hacktivism and business reconnaissance. This shift has sparked discussion on the costs of risk management in software development. In this paper, we discuss vulnerability analysis in the context of critical systems: systems in which an operative outage endangers the continuity of the organization. As a solution to the expenses of improved information security, we define a concept termed *business resilience*, which offers a general reference point for relevant improvements to a system. In this context, business refers to any profit-centered element of an organization. We present an approach to determining the criticality of an identified threat to the business. We also propose a methodology for utilizing business resilience properties in dynamic environments, such as the high security networks used by the military. The discussion and views presented in this paper can be adopted by any organization concerned about sensitive and classified contents stored and communicated in current ICT systems in the context of cloud computing.**

Keywords—Vulnerability analysis; Risk Management; Survivability; Attack tree; Military

I. Introduction

Survivability and software vulnerabilities have been a top discussion in military systems for over twenty years. As technology evolves, threats to systems become more diverse and harder to identify. This has inspired researchers to model environments and convert threats into a computable format. There are various definitions of a threat, but we approach the definition specifically from the survivability point of view. Barbacci introduced survivability as "A system class that is able to execute the task in a reasonable time, even if significant parts are paralyzed because of an attack or damage" [1]. Extrapolating from this, we define a threat as an event that endangers survivability.

In this paper, we will discuss resource optimization when implementing vulnerability analysis in core authority systems and define the key properties of such analysis. We also characterize algorithms for conducting the analysis on a real-time basis in a dynamic environment. We will narrow our observations to military systems, in which the need for computational capacity is high and the reliability of information is always critical.

Economic risk management is the optimization of resources in relation to identified threats and consequential damages. Systems cannot ever be fully secured upon construction because of limited resources, such as finances, expertise, time and ever-evolving polymorphic environments. As a solution to the challenge of modelling in the environment of public authorities, we propose a new concept called *business resilience*, which also improves knowledge on information security in the system as a whole.

The paper is organized as follows. First, we will examine the essence of vulnerability analysis by introducing relevant research in the field, defining the relevant terminology, characteristics and principles, as well as the benefits of the methodology within the scope of a military context. Next, we will discuss concept of business resilience and its key properties. Lastly, we propose algorithms for implementing business resilience in a dynamic, high-security environment. We will conclude with key findings and a description of the future of business resilience in the military context.

II. About Vulnerability Analysis and Related Work

Vulnerability analysis is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Modelling the critical infrastructure and identifying the most severe vulnerabilities are key tasks for the authorities responsible for national security. One motivation behind vulnerability analysis is to have a measurable approach to policy making. It answers the question of which components should be made more resilient to attacks and determines the probability of a successful attack on a component. The combination of component vulnerabilities and attack probability makes it possible to quantitatively evaluate the vulnerability of a sector. And yet the analysis is only as comprehensive as the model.

There has been a lot of research on attack, vulnerability and risk analysis. Some studies are based on network specifications [2, 3, 4, 5], some exploit graph representations [2, 6, 7] and perhaps the most popular approach is utilizing tree constructions, like attack trees or fault trees [2, 8, 9, 10]. Vulnerability analysis is closely related to survivability analysis and research [11, 12, 13]. There are also more comprehensive approaches that combine several methodologies, like model-based vulnerability and the risk

978-1-4799-9942-2/15 $31.00 © 2015 IEEE
DOI 10.1109/NBiS.2015.39

analysis method for critical societal infrastructure like the one presented by Lewis [14]. It makes use of network modelling as well as fault tree analysis. Instead of analyzing the system environment of the components, we can approach data contents via dynamic taint analysis (DTA) [15, 16, 17]. It is an extremely powerful method for detecting vulnerabilities in applications, like the one Herrera presented for Java malware [17].

In this paper we adopt the approach presented by Lewis as a starting point, because of its scalability from critical network infrastructure to the individual system component. Its simplicity and practicality allow for additional methodologies and tools to enhance the generated risk-assurance level. The main steps of model-based vulnerability analysis and risk analysis are [14]:

1. Listing of assets. Identifying all the components of the system.
2. Network analysis. Categorizing and analyzing relationships between the components. Identifying the most critical component.
3. Fault tree analysis. Building a tree representation of the vulnerabilities to create a fault or failure in a component. With vulnerability probabilities, the likelihood of failure occurring in a component can be estimated.
4. Event tree analysis. The outputs of the previous step are input into an event tree. The event tree contains all possible events obtained by single and multiple combinations of faults. With this step, assurance of all relevant vulnerabilities is enhanced.
5. Event matrix analysis. The number of processed events can be reduced using an event matrix, by enumerating the single and double faults in the event tree.
6. Risk assessment and resource allocation. Determining optimal allocation for funding to improve component resistance to vulnerabilities.

In Lewis' approach, the various system components are determined and, for each one, the possible faults and threats are identified. A component is listed if the possibility of threat to different components multiplies during a single attack. This possible multiplication of threats is processed using event matrix analysis, which threats all threats as equal [14]. The only distinction is the probability of the occurrence, not the severity of the possible damage [14]. Lewis presents a method for determining the costs of improving security with a relative percentage per single threat, but it considers reduction in attack probability for only one component at time.

As we stated before, vulnerability analysis has been a very important method in the military context. It has been considered a methodology with which vulnerable targets can be identified and preventive action against threats can be taken. It has guided process management as well as the system software built to support it. In dynamic high security environments, it improves awareness of current security levels [18]. However, one challenge has been the computing resources needed to analyze the constantly changing environment and providing sufficient security with limited resources. In the next section, we propose a set of properties to be applied using vulnerability analysis technology. They allow us to identify the components or parts of the system that should be secured in order to use budgets most effectively.

III. Vulnerability Analysis Conducted by Business Resilience

Cyber attacks or cyber warfare are very popular topics in today's media. These discussions usually center around the identity of the perpetrator, the type of attack, and how the attack could have been prevented. This last topic in particular can be an item of interest long after the attack or incident itself has ended, and the discussion can go on for a long duration if the attack has caused inconvenience for lots of people. The problem with this kind of discussion is that it usually concentrates on reactive actions and the technological details of attack prevention. The discussion can be inconvenient to the business being targeted, and such antagonistic discussion can be one of the original goals of the malicious actor. Little attention is typically paid to the real damage caused by the attack and why the systems should be protected in the first place. The consequence of technically oriented discussion is that future security improvement investments for the systems of the targeted corporation are possibly exaggerated, and only against limited types of attacks that have gained media awareness.

Despite public discussions, it is widely known that systems cannot be secured fully against attacks. The more efforts are made to secure a system, the higher the expense. Investment costs increase exponentially in relation to the level of protection achieved in the overall system. Systems that have little or no protection can be more secured with little investment. Similarly, improving overall security in a high-security system typically requires significant investments.

Moreover, the organization shouldn't forget why the system is being protected. An implementation technology or method of possible attack or cyber war is never a reason in and of itself for improving system security. Systems always have a reason for existence, determined by business use. The criticality of the system is directly related to the how crucial the system is for the business and how few failures of the system can be avoided without compromising the business. This means that the significance of the system must be evaluated according to the business impact caused by compromised knowledge, compromised sensitive personal information, system outage or failure. Moreover, the type of damage for the business must also be noted and taken into consideration. Cyber threats can cause enormous direct and indirect damages. Interruption of business operations causes loss of revenue and income. Recovery of operations can cause expenses for a significant amount of time, up to several years. Loss of reputation causes direct and indirect expenses. Cyber attacks may cause legal fees, fines and/or sanctions. Loss of immaterial capital, such as research and development investment, will cause expected cash flow reductions. Exposure of sensitive business or customer data will cause direct and indirect expenses, as well as reduction of cash flow and loss of reputation.

We propose a concept called *business resilience* to determine a system's security tolerance. We define the concept of business resilience as ability for the business to survive the loss of immaterial and material capital due to significant parts of the information system environment being paralyzed or exposed to the public at large due to a cyber attack or collateral damage in the cyber environment. With business resilience, we can determine comprehensive improvement of tolerance against the risks for the organization. The main goal of this determination is to gain sufficient security levels against identified threats with the resources available.

A. *Properties of Business Resilience*

The properties for determining information security, sustainability and business resilience in a given system are listed in Tables I and II. Business resilience is quantified by the financial key ratios of the business. We have not included balance sheet values in this paper, in order to maintain the simplicity of the model, which is nevertheless comprehensive. For a sufficient approximation, the key ratios revenue and cash flow must be considered. The resilience limit is defined as the financial value that the business can tolerate in direct losses during an attack. In other words, it answers the questions of how long a business can remain unavailable and what kinds of expenses the corporation can afford to dedicate to recovery activity before bankruptcy strikes. Reputation means the business reputation that might be lost because of the unsuccessful prevention of an attack, or the publicity of exposed contents. It might cause a loss of credibility and decrease in customer base. Reputation can be determined as a financial value function over time, meaning the value of reputation loss changes over time. The initial reputation loss will be high when the attack and system vulnerabilities are publicized. With successful countermeasures and prevention of increased damage, the cost of reputation losses can be curtailed. On the other hand, if the attack is continuous, sensitive data is leaked to the public at large, or prevention of the attack fails, reputation losses increase. We assume that this continuous function represents the situation that the attack continues and prevention fails. Naturally, the value of reputation loss can be reduced by carefully planned information delivery to the public.

Business resilience is the financial tolerance of the components that are compromised. At the business level, the collection of business components is evaluated through various properties. The properties for each component are described in Table II.

To avoid and decrease the losses of a cyber attack, risk can be transferred of shared. Risk transfer is directed at a component. In the business context, the total amount of transferred risk is the sum of all transferred risk in components. It should be noted that, for example, insurance against cyber attacks is a component of this model. Nevertheless, it would be unusual for a corporation to be able to transfer risks entirely. All risks cannot be avoided, naturally. Residual risk must be accepted. The determination of the quantity of the residual risk is difficult to evaluate. A suitable approximation is achieved by analyzing and forecasting the possible change in cash flow due to cyber attack. In our model, this can be calculated by summarizing the lost revenue of all components compromised by the attack and comparing that to the corporation's cash flow. When the resilience limit equals total lost revenue subtracted from the remaining cash flow, the continuity of the business is endangered.

TABLE I. PROPERTIES OF BUSINESS RESILIENCE IN OVERALL SYSTEM

Property	Value type	Description
Revenue	Financial value	Key ratio on the income statement
Cash flow	Financial value	Key ratio on the income statement
Limit of resilience	Financial value	The limit of losses that can be tolerated before bankruptcy
Reputation loss	Function of financial value over time	Estimated value of the reputation loss due to an attack
Business components	Array of components	Individual component properties are described in Table II
Total transferred risk	Financial value	The total amount of transferred or shared risk
Information security investment budget	Financial value	Investment budget for information security improvement

The last property at the business level is the investment budget that can be used to improve information security. This property determines the possibilities for improving tolerance against cyber attacks. The technique for determining how the investment can be optimized and allocated to different components is discussed in section 3B.

In Table II, we describe the properties of each business-critical component. For each component, a short description of its role is provided, along with its significance for the business. Business criticality is the numerical value of criticality for the business. The method for determining business criticality is described in section 3B.

Business operation is the downtime of the business and the loss of revenue in all lost business operations due to unavailability of the component. Immaterial capital, such as patents and IPRs, is the value of unique market assets (for example, business secrets that offer an advantage over competitors). Customer data loss is the value of customer data that is lost, corrupted or exposed. This data includes business secrets, and may also include sensitive data, such as personal information or credit card data. Sensitive data means data contents of the system that have business value (for example, research results or product costs).

The probability of success upon threat may vary in each component of the system, and the real cost that the threat produces is its impact and damage to all the components it impacts. This dictates that when investing in system security, threats to the system must be considered and the organization must decide what kind of real risks it is able or willing to acknowledge. We state that the probability of successful attack against business resilience is the probability of a threat succeeding in any component as presented in (1) where F_i is the set of components that are influenced by the threat *i*. $F_i = \{comp_j\}$, where the system component j is influenced by the threat *i*. Therefore $P(F_i\ comp_j)$ denotes the probability of a successful attack on component by threat *i*. We consider the threats as nondependent on each other; each is considered an individual threat during an attack.

$$\mathrm{P}(threat\ i) = \mathrm{P}(F_i\ comp_1) + \ldots + P(F_i\ comp_j) - \mathrm{P}(Fi\ comp_1 + \ldots + comp_j) \qquad (1)$$

The risk function *R* represents the overall probability that some of the identified threats will succeed in the system in some component. It is defined as

$$R =_n f(\mathrm{P}\ (threat\ i_1), \ldots , \mathrm{P}\ (threat\ n\ ))_s \qquad (2)$$

wherein *n* represents the total number of threats and *s* the total number of components. We simplify the above approach to represent it in a more manageable form. We state that it is sufficient to represent *R* as a summation function where the risk R_j for component *j* is the sum of all probabilities of threats influencing that component, as in

$$R_n = \sum\nolimits^{n}_{i=1} \mathrm{P}(threat\ i). \qquad (3)$$

The collection of identified threats is connected to the component. Each threat has some probability for success, and the evaluated cost is for reducing the probability of success by one percent. The methods of calculating the threats are discussed in more detail in section 3C. On a component level, the minimum cost of security enhancement can be determined by a minimum cost of security improvement as

$$\min\ (c_i * R_i) = \min\ (\sum\nolimits^{n}_{i=1} c_i * \mathrm{P}(threat\ i)), \qquad (4)$$

where c_i is the cost of reducing threat vulnerability *i* by 1% [14] and $i \in [1, n]$. Risk can also be transferred via contract to, for example, a service provider, the customer, a subcontractor or an insurance company.

TABLE II. PROPERTIES OF BUSINESS RESILIENCE FOR EACH COMPONENT

Property	Value type	Description
Component description	String description	Component name, description and role in system
Business criticality	Normalized value [0..1]	Criticality of the component in relation to business
Cost of investment	Financial value	Development costs of the component
Estimated lost revenue	Financial value	Expected direct costs if the component is not available due to an attack
Recovery costs	Financial value	Estimated cost for the recovery of the component
Immaterial properties	Financial value	Estimated value of business advantage in relation to competitors. Value of immaterial capital that is bound to the component
Sensitive data content	Financial value	Estimated value of confidential data that is tied to the component.
Customer data content	Financial value	Estimated value of confidential customer data that is tied to the component.
Risk	Probability	Estimated risk that any of the identified threats will succeed and cause the component to be unavailable
Threats	Array of identified threats	Identified threats to the component and the probability of attack succession and cost of probability reduction by 1%
Minimum cost of security improvement	Financial value	The minimum cost for risk reduction by 1%
Transferred risk	Financial value	The amount of component risk transferred or shared

Fig.1 presents the relationship between business resilience and components and threats. The arrows from attacks to component illustrate the risk that a successful attack presents, and the arrows from component to business operations describe the criticality of the component. The weight of the arrows defines the relative criticality among other arrows. The business resilience here is the tolerance for faults during component outage caused by a successful attack. The risk of outage can be transferred, enhancing business resilience. Reputation illustrates the credibility of business operations as seen by the public.

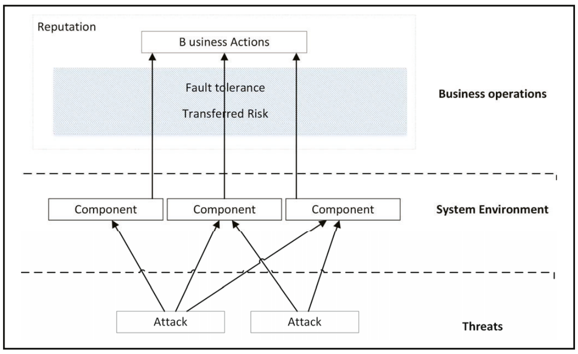


Fig. 1. Illustration of the relationships between business resilience, components and threats.

In the following section, we describe a simple method for determining component criticality. It is an approximation of the subjective interpretation of strategy, but it allows the corporation to focus a limited investment budget on the most crucial components.

B. Determining the component criticality

As stated before, we argue that a reduction of optimal risk level or the probability of reaching the critical point in the system is relevant only when it is reasonable in terms of the system as a whole. To evaluate this reasonability, we propose a simplified method of quantifying criticality. The attributes that determine the business criticality for each component are listed in Table III. The value for determining the business criticality to be applied in each component can be found in the properties of the component (Table II). A good convention for determining the system as a whole is to proceed top down, to start with larger parts and break those down into more detailed components. This helps focus on the relevant information. Within Table III, we can see that different attacks have different financial impacts. The investment value is the financial value of the component that can be considered lost because of an attack; it refers to the time necessary to pay back the investment calculations that will not to be actualized. The value of the lost revenue is the immediate financial damage and the impact of the attack. The recovery expenses are the costs actualized in order to restore the system to pre-attack levels. The value here is not considering the timeline of the recovery. Recovery costs can be also caused by replacement of the component. In terms of immaterial impact, the value of the lost component can be considered the amount of investment, or with unpublished patents, the loss of future productivity or income.

TABLE III. MATRIX OF ATTRIBUTES THAT DETERMINE COMPONENT CRITICALITY.

Impact	Investment value	Value of lost revenue	Recovery expenses
Business operation		x	x
Immaterial capital	X	x	
Customer data		x	x
Sensitive business data		x	x

We determine the overall criticality of the component by normalizing the summarization of lost expenses *v* (investment value, lost revenue, recovery expenses) for the component. During normalization, the most critical component is given the value 1, and the rest are valued in relation to this maximum value. We do not consider security enhancements to a component as investments. That is, the value of a component in relation to business resilience does not increase by investing in safety measures. This is because the cost of outage does not change directly. However, the recovery time or expenses might be altered due to a security investment, which also changes the criticality of the component. The criticality of component C_j is represented by

$$C_j = v_j / \max (v_j), \tag{5}$$

where $j \in [\ 1,\ S\ ]$ and S indicates the set of components in the system.

Multiplying the criticality attribute of a component with the risk faced by the component (3), we can prioritize the urgency of component improvement. The closer the product gets to 1, the more urgent the improvement is.

C. Charasteristics of Business Resilience

In this section, we examine the characteristics of business resilience in more detail and present approaches to making investments in information security as profitable as possible. We adapt the approach Lewis presented in his model based on vulnerability analysis of the threats to the components, because as we have stated, the components are the units that ensure business continuity. Instead of focusing on individual threats when improving the system protections, we consider the component to be improved itself. In practice, instead of estimating the costs of countermeasures against one threat, we consider the cost of a better component or the continuity of the system after attack.

Continuing with a business resilience approach makes it possible to address the cumulative impact of the threat. In large attacks, one threat vector affects multiple components. On the other hand, some large attacks may cause limited or no damage in one component in terms of business continuity. Usually it is too expensive to build a separate preventive mechanism for each component, when the costs of the attack are limited to a small proportion of the expenses. In such cases, the risk can be deemed acceptable. But more importantly, the threat must be analyzed in terms of the business damage it causes. This being the case, we cannot bypass the components affected by the attack. The real financial damage of a single attack is the sum of all damaged components and their cumulative costs.

We propose that the distinction in terms of threat is always the actual impact on business, which differs from the original model presented by Lewis. This fact supports a business resilience approach, meaning those components that are most essential to business continuity are improved first with enhanced protection against attacks.

Applying a business resilience approach stresses the criticality attribute of the component. We agree with Fung et al. that the system as a whole is as strong as its weakest link [19]. Moreover, we assume that the system should be always being protected against common and commonly known general attacks, and that malicious actors behave with economic interests at heart. Fung et al. propose a difficulty level in their attack model which states that attackers tend to find the easiest way, the one that needs least effort to be exact, to cause the greatest damage in a certain attack type [19]. Moreover, the probability of a successful attack is not as relevant as the damage, because we can be sure that in general there are more malicious actors than we can protect our system from. Consequently, the weakest components, when measured in terms of business resilience, must be fixed first. The mathematical downside of this approach is that the most probable and expensive threats might suffice with an inadequate level of security, and we accept that some attacks may occur. However, we argue, that the criticality factor will ensure that the most fundamental and crucial threats are taken into sufficient consideration. And as stated before, t systems cannot ever be built to be entirely attack-safe.

The business resilience of the system determines that if all business-relevant components of the system are unavailable, the business will cease to exist after certain time. The relative portion of the resilience *PR* determined by a component can be evaluated by the values of all components, as in

$$PR_j = v_j / \sum{}^{s}_{j=i} (v_j), \tag{6}$$

where *s* indicates the amount of components in system. The total sum of all component values must be always smaller than the business resilience. Otherwise, a single attack can irrevocably damage the operative business or reputation of the organization. In a public authority, this means that the credibility of the authority may be questioned and the safety of citizens be compromised. Ways of improving the overall resilience of the system can include procuring insurance or improving the information security of the selected component or all components. In the latter case, the simplest approach to improving the system is to apply the improvements (4) to single component. However, this approach relies on local optimization and instant improvements reliant on limited financial resources. Improving one component does not necessarily give protection against the threat at large. This is why a threat must be addressed collectively based on all the components it affects.

The total financial value of a threat towards our system can be calculated by summarizing the component values that are impacted by the threat if successful. We simplify the calculation to emphasize the threat value, determining that a successful attack, all components that are influenced by successful attack are summarized in a total value v_i, as

$$v_i = \sum F_{vi}, \tag{7}$$

wherein F_i contains all the components influenced by the threat and v represents the value of the component on the set. In order to determine the vicinity for the value of threat, we compare it to the entire business resilience BR of the system as relative value of threat RV_i

$$RV_i = v_i \,/\, BR \tag{8}$$

Security actions should take place if total value of the threat approaches the business resilience value (ie. $RV_i \approx 1$). We also argue that if the success probability of threat is greater or equal to the relative value of threat, the threat should be considered a risk and an action plan to avoid the risk are developed.

The alteration in the system always affects the composition of vulnerability, the threat set with probabilities and the role of each component in the overall system. This is why after every change in components, vulnerability must be evaluated again. The methodology Lewis presented is comprehensive, yet too heavy for real-time analysis in a dynamic environment. We propose a modified attack-tree approach to solving this challenge. We describe this approach in greater detail in the next section.

IV. Real-Time Vulnerability Analysis in Dynamic Environment

In a dynamic high-security environment, it is impossible to continuously perform every critical infrastructure protection step from scratch as described in the previous sections. We propose a lighter and more computative method that can be executed after various changes are made to a set of components. These changes include improvement of and reduction of security of the component, new components in the overall system (for example the addition of new nodes to network) and disabling some components from the network (for example if they are compromised in attack). We extend the attack-tree methodology presented by Fung and Hung [8]. The attack-tree methodology was developed for distributed SOA (Service Oriented Architecture) environments where services are employed to fulfill a system objective [8]. In our military context, services are components of the system environment and can be services, network nodes or critical systems. In the following section, we observe how business resilience attributes are handled within a changing environment. We limit our discussion to static environment with static set of threats.

A. The Impact of Business Resilience to Intrusion Modelling

In an attack-tree methodology, the system is inspected from the attacker vantage point. The success of the attack is the success of a top-level goal [19]. An AND operation implies that the attack must succeed against all branches of the tree in order to cause the system to fail [19]. The most cost-effective way to improve total security against an AND operation is to improve security in the branch where improvement is cheapest. Similarly, an OR operation implies that only one of the branches must be successfully attacked for the attack to succeed [19]. It also means that in order to improve overall information security, the security level must be improved in every branch of the OR operation.

In a dynamic environment, the vulnerability setting of the system can change rapidly due to intrusion or executed countermeasure. We combine the dynamic construction of a high-security environment with automatic and constant vulnerability analysis. We utilize the business resilience properties in AND, OR and LEAF operations presented by Fung and Hung [8]. This way we achieve a more survivable and resilient environment against attacks or damages. Fig. 2 presents a sample attack tree construction in relation to a process diagram.

It is important to be aware of the resilience level of the environment after the change. We present four algorithms for modelling the change in business resilience: initialization, resilience change in a component, adding a new component to the system and excluding a component from the system. In order to gain a good grasp of security performance, it is relevant to identify the location of the new component and its influence on the resilience of neighboring components. At the leaf level, there is a single operation or a component whose failure has an impact on system execution. A leaf is the level that addresses costs and impacts. The higher levels of the tree decrease or increase total resilience, depending on the operation.

Algorithm 1. Algorithm to initially identify resilience level

```
First round with all leaves

Calculate component risk
Calculate component value
if component value > current maxvalue then
    maxvalue = component value

Second round with all leaves and nodes recursively

if node is LEAF
    Calculate criticality with maxvalue
    Calculate improvementUrgency = risk * criticality
    if improvementUrgency > current maxImprovementUrgency then
        maxImprovementUrgency = component improvementUrgency
if parenting node is AND operation
    node value = max(value of direct descendants)
    node risk = max(risk of direct descendants)
    node criticality = max(criticality of direct descendants)
if parenting node is OR operation
    node value = sum(values of direct descendants)
    node risk = sum(risks of direct descendants)
    node criticalities = sum(criticalities of direct descendants)
```

The computational cost of calculation is at most $3n(n+1)$, where n is a total amount of leaves. In practice this means that there are always at most two leaves as siblings. As we can see, the cost is a polynomial, and to decrease the computative power needed in real-time for this analysis, we suggest that the initial baseline for the resilience be calculated first. It can be made, for example, on a Lewis model step three, where the fault tree is built.

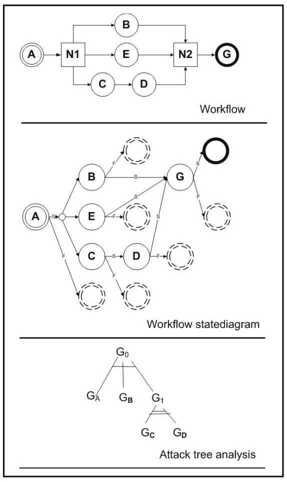


Fig. 2. Sample attack-tree construction in relation to workflow diagram

In algorithm 2, the added component is always considered a leaf. It is assumed that the parent of the added component is not a leaf. It should be determined how the component is added to system, ie. through an AND or an OR operation.

Algorithm 2. Algorithm for determination of resilience after addition of a component

```
With added component
  Calculate component risk
  Calculate component value
  If component value > current maxvalue then
    maxvalue = component value
    set maxValueIsChanged to true
    Calculate criticality with maxvalue
    Calculate improvementUrgency = risk * criticality
    if improvementUrgency > current maxImprovementUrgency then
      maxImprovementUrgency = component improvementUrgency

    if  maxValueisChanged = true then
      For each leaf calculate criticality and improvementUrgency
      For each parenting node calculate properties similarly in initialization
        phase
    else
      With all parents of added component
        If parenting node is AND –operation
          node value = max(value of direct descendants)
          node risk = max(risk of direct descendants)
          node criticality = max(criticality of direct descendants)
        If parenting node is OR –operation
          node value = sum(values of direct descendants)
          node risk = sum(risks of direct descendants)
          node criticalities = sum(criticalities of direct descendants)
```

It is worth noting that calculating the risk to an added component can impact the total probability values of the threat. In other words, the addition of a component can have significant changes to the overall system, perhaps justifying re-evaluation of the whole system .

Algorithm 3. Algorithm for determination of resilience after excluding a component

```
With all parents of excluded component
  if excluded node has one sibling node then
    Exclude parent node and attach sibling to the parent of parent
  if parenting node is an AND operation
    node value = max(value of direct descendants)
    node risk = max(risk of direct descendants)
    node criticality = max(criticality of direct descendants)
  if parenting node is an OR operation
    node value = sum(values of direct descendants)
    node risk = sum(risks of direct descendants)
    node criticalities = sum(criticalities of direct descendants)
```

The value of the excluded node can contain the maximum value of the system. However, it is not necessary to calculate the whole system at this point, because relative criticalities still remain. We argue for excluding components as a result of an attack, and after recovery, adding components back to the system. The max values are calculated during additions to the system. We propose that one component not be overvalued in comparison to the overall system, and new components added to the system should not exceed the max value of previous components.

Algorithm 4. Algorithm for determination of resilience after change in survivability of a component

```
With altered component
  Calculate component risk
  Calculate criticality by with maxvalue
  Calculate improvementUrgency = risk * criticality
  if improvementUrgency > current maxImprovementUrgency then
    maxImprovementUrgency = component improvementUrgency

With all parents of altered component
  If parenting node is AND –operation
    node risk = max(risk of direct descendants)
    node criticality = max(criticality of direct descendants)
  If parenting node is OR –operation
    node risk = sum(risks of direct descendants)
    node criticalities = sum(criticalities of direct descendants)
```

Restructuring the tree can be completed by adding and excluding nodes and leaves appropriately. We argue that the algorithms presented are suitable for a dynamic environment, because changing, adding or excluding a component requires at most 3*k* operations, where the *k* is the level of hierarchy for the processed component. In those rare situations that addition changes the existing maximum value of all components, the criticalities of whole system need to be recalculated. This does not happen in normal operative execution, but during significant change to the system. In this instance, the analysis should be re-evaluated in every case. With the presented algorithms, we gain the most important properties of the system for the two top levels. The properties are total resilience value, risk and criticality for a portion the entirety of the components of a system.

When improving system survivability, it is most convenient to have AND operations in critical components [19]. In practice, this means that component services should be coupled. It can be expensive to build backup systems for every operation in a large-scale environment. However, in high-security systems, it is necessary to be able to turn off the compromised component or system segment. This exclusion of damaged or compromised component guarantees operability, though with limited resources.

V. Future work

As the next step, we propose implementing a real-time vulnerability analysis and resilience determination algorithms in a high-security cloud environment. We have planned on improving the algorithms by expanding them with system recovery features in order to improve the survivability of a system. The survivability of the system and overall information security against certain types of attacks can be improved cost-effectively by having a selection of countermeasure tools available to combat attacks. This means the ability to diminish or eliminate the source of the threat is less expensive than building exaggerated and oversized security mechanisms. This approach changes the formulation of the vulnerability analysis from a purely defensive to more active defense.

Another track under research is to have these survivability enhancements seamlessly deployed into a software development process. The advantage of this is that the costs of building security mechanisms for the system during the construction phase is significantly less than adding them to a completed system already in production. We use this model to quantify the sufficient level of security and review the actualization in each development phase.

We are also building a model which determines the change of business resilience over time in relation of the system technology in use, threats and system reputation.

VI. Conclusions

In this paper, we examined vulnerability analysis within the military context. We proposed a concept called business resilience to determine the most critical components of the system in relation to business continuity. We identified the attributes of business resilience and examined how to determine them and how they interact with overall environment. The attributes allow for processing the direct and indirect costs of the component for the business when they are not in use. In an enhancement to previous models, the attributes also include immaterial expenses as enablers of future business. We presented a comprehensive set of tools for determining the risk of a threat to the business and for allocating resources to components that are the most vulnerable in terms of resilience. We argue that improvements to information security in high-security systems must be considered in terms of the attributes of business resilience in order to allocate resources efficiently.

With real-time vulnerability analysis in dynamic environments, we facilitate the use of business resilience attributes in dynamic constructions in high-security contexts. We also achieve an awareness of the information security level after recovery from an attack or after security enhancements to a system. We have limited the observations on how to detect malicious attacks or how the component security is enhanced, but we presented algorithms to determine the overall business resilience of the system after such events. The methodologies presented allow us to identify the vulnerabilities of the system in relation to business resilience, to evaluate what can be achieved with enhancements to the system, and lastly, to allocate limited resources to the most vulnerable components in order to gain best protection of the system.

Acknowledgments

This work has been partially supported by CGI in Finland (http://www.CGI.com/), with particular support from Jan Mickos. His contributions to determining the concept of business resilience are appreciated.

References

[1] M. Barbacci, “Survivability in the age of vulnerable systems”, IEEE Computer, 29, 11(1996), page 8.

[2] S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, and C. S. Raghavendra, “Impact Analysis of Faults and Attacks in Large-Scale Networks”, IEEE Security & Privacy, pp.49-54, 2003.

[3] S. Jajodia, S. Noel and B. O’Berry, “Topological Analysis of Network Attack Vulnerability”, Managing Cyber Threats, Massive Computing Volume 5, 2005, Springer US, pp.247-266.

[4] Y. Li, H. Yang and K. Xie, ”Network Node Importance Measurement Method Based on Vulnerability Analysis”, Proceedings of the 4th International Conference on Computer Engineering and Networks, 2015, Springer International Publishing, pp.1281-1289.

[5] Y. Zeng and R. Xiao, “A networked approach to dynamic analysis of social system vulnerability”, Journal of Intelligent and Fuzzy Systems, Vol.28, No.1, 2015, pp.189-197.

[6] E. Jenelius and L. Mattsson, “Road network vulnerability analysis: Conceptualization, implementation and application”, Computers, Environment and Urban Systems, Vol. 49, January 2015, pp.136-147.

[7] H. Lv, Y. Zhang, R. Wang and J. Wang, “Graph-Based Real-Time Security Threats Awareness and Analysis in Enterprise LAN”, LISS 2013, Springer Berlin Heidelberg, pp 1299-1304.

[8] C.K. Fung and P.C.K. Hung, “System recovery through dynamic regeneration of workflow specification”, Proceedings of the Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, Washington, DC, 2005, pp149-157.

[9] P. Kumar and S. B. Singh, “Fuzzy Fault Tree Analysis using Level (λ, ρ) Interval-Valued Fuzzy Numbers”, Mathematical Theory and Modeling, Vol.5, No.2, 2015.

[10] E. Bozdag, U. Asan, A. Soyer and S. Serdarasan, “Risk prioritization in Failure Mode and Effects Analysis using interval type-2 fuzzy sets”, Expert Systems with Applications, Volume 42, Issue 8, 15 May 2015, pp.4000-4015.

[11] N. Mead, R. Ellison, R. Linger, T. Longstaff and J. McHugh, “Survivability Network Analysis Method”, CMU/SEI-2000-TR-013, September 2000.

[12] A. Moore, R. Ellison and R. Linger, “Attack Modeling for Information Security and Survivability”. CMU/SEI-2001-TN-001, March 2001.

[13] J. Cardoso, Z. Luo, J.A. Miller, A.P. Sheth and K.J. Kochut, “Survivability architecture for workflow management systems”, Proceedings of the 39th Annual ACM Southeast Conference (ACM-SE'01), Athens, Georgia, May 2001, pp 207-214.

[14] T.G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley-Interscience, 2006.

[15] J. Newsome and D. X. Song, “Dynamic taint analysis for automatic detection, analysis, and signaturegeneration of exploits on commodity software”, In Network and Distributed System Security Symposium (NDSS), San Diego, February 2005.

[16] M. G. Kang, S. McCamant, P. Poosankam and D. Song, “DTA++: Dynamic Taint Analysis with Targeted Control-Flow Propagation”, *NDSS*. February 2011.

[17] H. Adrian, and B. Cheney, "JMD: A Hybrid Approach for Detecting Java Malware", Proceedings of the 13th Australasian Information Security Conference (AISC 2015). Vol. 27. 2015.

[18] K. Zaerens and J. Mannonen, “Concept for the Construction of High Security Environment in Public Authority Cloud”, Lecture Notes in Electrical Engineering, Springer-Verlag, pp. 401-408, September 2012.

[19] C. Fung, Y. Chen, X. Wang, J. Lee, R. Tarquini and M. Anderson, “Survivability analysis of distributed systems using attack tree methodology”, Military Communications Conference, 2005, pp. 583 – 589.

V

2015 Republished, with permission, from:
Häyhtiö, M. and Zaerens, K.
Comprehensive Assessment Model for Critical Infrastructure Protection,
Management and Production Engineering Review, 8(4), December 2017

Management and Production Engineering Review
Volume 8 • Number 4 • December 2017 • pp. 42–53
DOI: 10.1515/mper-2017-0035

A COMPREHENSIVE ASSESSMENT MODEL FOR CRITICAL INFRASTRUCTURE PROTECTION

Markus Häyhtiö, Klaus Zaerens

National Defence University Helsinki, Finland

Corresponding author:
Markus Häyhtiö
National Defence University Finland
Defence Acquisition
Helsinki, Finland
phone: +358-(0)45-1200304
e-mail: markus.hayhtio@kolumbus.fi

Received: 5 July 2017
Accepted: 16 November 2017

Abstract

International business demands seamless service and IT-infrastructure throughout the entire supply chain. However, dependencies between different parts of this vulnerable ecosystem form a fragile web. Assessment of the financial effects of any abnormalities in any part of the network is demanded in order to protect this network in a financially viable way. Contractual environment between the actors in a supply chain, different business domains and functions requires a management model, which enables a network wide protection for critical infrastructure. In this paper authors introduce such a model. It can be used to assess financial differences between centralized and decentralized protection of critical infrastructure. As an end result of this assessment business resilience to unknown threats can be improved across the entire supply chain.

Keywords

critical infrastructure, supply chains, capability management, risk management, cyber, service.

Introduction

The history of international trade is long. The role of globalization has steered development toward increasing global alignment of activities across countries, operations and market offerings [1]. Importance of international trade is tremendous for modern economies. A study conducted by the Bertelsmann Foundation's Global Economic Dynamics program [2] reveals the fact that one of the largest beneficiaries of the global trade was Finland with the annual gain in the income per capita of about €1500.

Despite the fact that international trade has deep roots, its significance has never been as great as it is now. Clear, positive effects of globalization as a mechanism to spread wealth cross borders have made it possible to create a web of enterprises that work closely together across the globe. But there is a downside to this: a global network of organizations working together increases the possibility of risks due to their dependency on inter-discipline information.

Protection of the critical components of the supply chain has to cover critical, recognized nods and most important production systems and their subsystems. Then again, as Lewis [3] points out, actors participating in supply chain management are commercial companies whose main purpose is to run commercially viable operations. Therefore Critical Infrastructure Protection (CIP) is not their first priority, but still an essential part of business due to its financial importance. Also, international trade expands its web so widely, that regional conflicts or crises are seldom a concern for other countries from any other point-of-view than commercial. These actors have streamlined their operations to the point that no back-up systems exist [3].

The supply chain systems' operations' four functions have to be analyzed across organizations. According to Beer [4], these four functions are implementation, coordination, control and intelligence.

In detail, these functions consist of:

1. Implementation consists of daily operations, which enable production of physical products and services.
2. The coordination function consists of the regulating system (task, authority, responsibilities), which is used to manage production operations.
3. The control function consists of supervision and management of the operations related to the implementation and coordination of production of physical goods and services.
4. Intelligence consists of functions relating to the adaptation of environmental changes.

Each one of these functions is built and run as a set of predefined processes. These processes are vulnerable to both uncertainties and risks. The protection of critical infrastructure requires thorough assessment of vulnerabilities and risks at process and individual component levels. Additionally, cross-functional operations require a set of abilities, which enable efficient management of operations and minimization of vulnerabilities and risks. As stated earlier, there is a need to assess all the parts of the business domain's supply chain and reflect the results to the pre-determined outcomes. Capability management as a management tool gives a clear structure for the definition process of risks. This provides a general picture and helps to concentrate on the relevant risks [5].

There are 2 research questions the authors are trying to answer in this paper:

1. What are the potential financial benefits of concentrating on prevention compared to the protection of the total supply chain?
2. Which capability indicators affect supply chain CIP operations?

The functionality of the model is assessed by collecting information from the actualized attacks against a recognized component, assessing and analyzing the time this attack was effective and analyzing its effects on the component's functionality.

A significant element in the analysis is the attack vector. The purpose of attack vector analysis is to assess how increased observation capability could minimize the attacker's effect on the target component, and compare the costs between centralized observation and systems wide observation. This enables cost benefit analysis between centralized and out-sourced service provision.

One has to notice that even though the attacker is stopped in time 0, there is the possibility of severe reputation loss, which has possible negative financial effects, even though the threat did not become a reality.

All the elements affecting CIP are illustrated in the Appendix 1.

The paper proceeds as follows. First, we will examine the uncertainty in the service networks and describe the elements of domain assessment in CIP. Next, we address the problem of unknown threat that exists in contractual environment of CIP. Lastly, we propose an approach for improving business resilience to overcome the problems described. We will conclude with key findings and a proposition of the future research.

Uncertainty in the service networks

Uncertainty is defined as "the difference between the amount of information required to perform the task and the amount of information already possessed by that organization." [6, p. 5] With risk we refer to the possible outcomes of an action, specifically to the loss that might be incurred if a given action is not taken [7]. A risk combines two attributes i.e. probability and impact. Probability is a measure of how often a detrimental event, which results in a loss, occurs. Impact refers to the significance of that loss to the organization. The level of risk is then perceived as the likelihood of occurrence of a detrimental event and the significance (impact) of that event [8, p. 397). Time should be considered as a variable in each analysis, and the effect time has on vulnerability and risks should be analyzed thoroughly.

There are a few assumptions we have to make in order to discuss the matter. The first assumption is that a structure of network organizations and processes is referred to as a service ecosystem. It describes the inter-functional and multidiscipline nature of service oriented industries and operations. The second assumption is that supply chain management is a part of the service industry. In their widely cited article, Vargo and Lush [9] introduce a theory of service dominant logic, the main point of which is a transition from goods based exchange to an economy based on more specialized skills and knowledge. The authors follow the approach of the Nordic School of Marketing [10] and Service-Dominant Logic (S-D logic) [9]. This approach was selected due to its emphasis on end-user preferences, which is a widely accepted method of developing and researching services.

At the core of the S-D logic is the shift from an emphasis on the traditional goods based, tangible resources to dynamic resources, which act together with other resources. Vargo and Lusch [9] refer to these resources as operand and operant resources, respectively. Because supply chain management is highly dependent on the IT-infrastructure, there is an obvious need to manage the capabilities for running the whole system of supply chain value creation. As Vargo and Lusch state, these arrangements need coordination and co-creation.

One of the foundational premises (FPs) of service dominant logic (S-D) is:

> *"Value co-creation is coordinated through actor-generated institutions and institutional arrangements" [9, p. 7].*

Thus, the third assumption the authors make, is that much of the supply chain management is run and managed through automated systems without social interaction. Despite this fact, these automated systems are created by humans, whose approach to the system is connected to the social environment it is developed in. This approach, which is widely used among the social sciences, is interested in the relationships between individuals and larger groups.

Social networks have significant importance to the success of supply chain operations. Uncertainty is defined, managed and accepted within the boundaries of a specific social network. Therefore every organization can reduce uncertainty by obtaining possession of critical assets and forming ties with stakeholders who are more specialized in a specific operation within their social network [11].

A systems based approach to one's identity introduced by [12] has been a topic influencing both educational and social sciences. This topic cannot be ignored when researching an area as complex as supply chain management, since we are not immune to the effects of either the cultural or social environments surrounding us.

Risk management strategies are not as straightforward as they may seem to be at first sight. Firstly, because supply chains are, as stated earlier, dependent on several systems, there is a need to analyze each system thoroughly in order to assess the correct approach to the risks and vulnerabilities of each of the systems. Secondly, time should be considered as a variable in each analysis, and the effect time has on vulnerability and risks should be analyzed thoroughly.

Domain assessment

Critical infrastructure is divided into three levels. The most important level consists of the information technology industry, energy sector and water supply industry. The second level consists of the banking and finance sector, and the chemical industry sector. The third level is formed by the armaments industry, postal- and distribution services, agriculture and food supply chains, health care, and search and rescue services [3, 13]. Domain assessment should be divided into three time-related phases: observation, comprehension and prediction [14].

The four functions of the supply chain systems' operations have to be analyzed across the domains the organizations operate in. Our approach has been adapted from the principles introduced by Skyttner [15].

The first and the most important assessment covers the way capabilities are managed within recognized, critical management areas. During the assessment work, the organization's ability to create valid input information, which enables necessary vulnerability analysis, has to be covered. Secondly, there has to be the capability to store that valid information in a way that meets the requirements for the protection of critical infrastructure. Thirdly, the capability to manage the organ, which uses the valid information, has to be assessed. Fourthly, an organization has to have the capability to predict and create scenarios, which require valid information. And lastly an organization has to have the capability to manage feedback information, and most of all, manage the pre-determined operations based on the scenarios.

In the second domain, an organization's capability to manage the contractual environment by using the methods, which take in to account the needs of end-user and the needs of the whole of the supply chain as a system, has to be assessed.

In the third domain, an organization's capability to manage the carrying capacity and capability to secure the alternative methods of transportation and suppliers of vital goods and services for the organization has to be assessed.

In the fourth domain, an organization's capability to manage the alternative and existing data transportation methods under all conditions has to be assessed.

In the last domain, the enhancement of the capability to react to rapidly changing political, social, environmental, legal and technological changes has to be assessed. This relates more to the first domain. The connections between functions and domain are illustrated in Appendix 2.

But how do we define a relevant risk in each of the domains? How do we decide which part of the supply chain creates a critical node? How do we divide a system and its sub-systems into manageable components, without sacrificing the overall purpose of the system? How do we define the capabilities, which need to be met? How do we prevent a situation in which the "tail wags the dog", meaning that the risk preventing process defines the outcome and not vice versa? There has to be a managerial approach, a methodology, which sets a framework for capability management.

The initial goal of domain assessment is to define and create capabilities, which enable recognition of an attack and reduce the attacker's ability to operate in the target component. Observation and protection are reactive functions, which affect the overall costs.

Contractual environment

The capability to manage contractual environment processes requires a set of pre-defined capabilities. As Anteroinen [16, p. 13] states:

> *"...capability is the ability or power to achieve a desired operational effect in a selected environment and to sustain this effect for a designated period".*

This definition does not determine how the objective should be achieved. The definition also takes into account how domain operations are run.

In the assessment of relationships between the domains and functions the authors limited their scope. During the research the scope was limited to domain 2 ("capability to manage contractual environment") and to function 2, which defines the management and supervision of the production process.

In the modern network based service chains, the commercial co-operation between the actors in the service supply chain is regulated with contracts. Contract management is divided into two major approaches. The first one concentrates on the structural design of the agreed transaction. The main focus of this approach is on the written contracts between different participating parties. These agreements are legally binding by nature [17, p. 241].

The second approach is more concerned with the relationships between the actors participating in the commercial co-operation. The main factor, participating parties rely on, is trust, which works as a safeguard for coordination and control functions. The upside of participants in this approach is the positive outcome of the transaction in spite of the existing and possible vulnerability [18, p. 395).

There are existing studies, which combine these two approaches, but their results are not clear-cut. One of the main reasons behind these results is the complexity of the contracts in the framework of trust. Even though one of the basic principles of S-D logic emphasizes institutional arrangements, it does not define which one of the approaches should be used for contractual management.

As the authors stated, the supply chain for a service ecosystem consists of several systems and subsystems. The capability to manage all the interrelating contracts within an ecosystem can become extremely expensive if the structural approach is used. Also, just a trust-based approach is hardly acceptable. We are after all researching the critical infrastructure, whose vulnerability cannot be protected only with the element of trust.

There are also examples of reciprocal-trust relationships which are based on the mutually positive out-comes, based on the actions active parties make [19]. This model does not take into account the possible role of third parties trying to take advantage of the two parties, who have created a reciprocal-trust relationship. Also, the reciprocal altruism introduced, among others by Trivers, [20] already in 1971 demands several and repeated interactions with known actors.

These contractual choices are obviously linked to the industry in question, which affects the criticality of the industry and possibly the already existing relationships between the actors within the industry. Contractual management should also consider the time-related phase observation, comprehension and prediction the critical process is related to. The four organizational functions – implementation, coordination, control and intelligence – need a thorough assessment from the contractual management point of view as well. These decisions are affected by the cultural, political and economic factors, as the main theories of international trade illustrate.

Contractual environment and an unknown threat

We approach the challenges in a contractual environment by observing two real life cases. In both cases we present partially successful cyber-attacks and discuss the deficiencies of situational awareness in a business ecosystem. The described sophisticated attacks were successful because of their unidentified nature and development resources behind new technology. Since there is always the possibility for an unknown threat, we endeavor to present a model managing the risk it produces.

The chapter is organized as follows. First we define the concept of an unknown threat. After that we present the two cyber-attack cases, and finally we analyze the cases in relation to contractual environment.

Unknown threat

An unknown threat is defined as a threat, which is not previously known, there is a theoretical background for the existence of this threat, there are no previously known counter measures against the threat or there are no known identification methods for the threat.

These threats include:

- 0-day vulnerabilities,
- tailored, effective based malicious operations,
- complex attacks against the targeted physical part of the component/system,
- APTs, Advanced Persistent Threats that combine all of the above and include significant resources for transforming the behavior of malicious activity.

Case of Industrial Espionage

Our first case contains a modern industrial espionage. The target of the attack was the immaterial capital of a large enterprise in the manufacturing sector that operates in the Nordic geo region. The details of the attack are classified. The information used here is retrieved through an interview with Jan Mickos [21], Vice-president, CGI Finland Security Advisory (May 23, 2017), and can also be viewed in public sources.

Attack description

The perpetrators of the attack campaigns are referred to as ”APT 10” and “APT 29”, which are explained in more detail [22] and [23]. The technical methodology used in the attack was fairly common. Previously known malware was slightly altered so it would not be exposed by normal antivirus scanners nor would it be blocked by technical security protection solutions. The adversary used a lot of time, resources and effort to cover the tracks of their actions and hide from defensive scanners and monitors. One particular feature of the attack was the ability to change the maneuvers, which ensured the stable progression of the attack towards its goal.

The attack was also special in its tactical dimension. It was aimed indirectly at the target via a common ICT service provider. This enabled two advantages. First, it is nearly impossible for an ICT service provider to identify malicious actions, since the traffic in the command and control (CnC) channel was hidden under the normal noise of enterprise activity. Second, even if the targeted enterprise would have noticed any abnormalities, it has no visibility or jurisdiction to the technical environment of the ICT service provider. As a side effect to the primary target, the attacker was able to create an entry point into other customers’ systems through the same ICT service provider.

Time dimension of the attack

The attack was exposed in the target environment in 2016. In a forensic investigation, the first traces of CnC were found to be from 2013. Any information from before this could not be reconstructed. It took around four months to block the attacker from the targeted system after exposure. That time was used for identifying the coverage of the attack, creating sufficient counter measures and collecting enough information for forensic analysis.

During the four years of attack, the attacker gradually collected information from the target environment, increased the compromised systems and components and proceeded towards the target. It is assumed that the attacker did not reach the ultimate target.

After successful coordination of counter measures and blocking the vulnerabilities of the systems it has been noticed, that the attacker has resumed a similar campaign towards the target enterprise via another service provider. This implies two results. First, the unknown threat has changed into a known threat and exposing new attempts are significantly faster. Secondly, a motivated attacker does not quit trying to reach the ultimate goal after the first obstacle. Instead, the attacker searches for another vulnerable component to continue the original campaign.

Speculating on the possible consequences of an attacker reaching the goal of immaterial capital, we can take the famous Nortel case as an example. The attack on Nortel proceeded unobserved for ten years [24]. In practice, the attacker was in control of the whole ICT environment of Nortel. As an indirect consequence of losing the immaterial capital and exposing business plans to competitors, the market value of Nortel dropped 98% in only two years, ending up in Canada’s greatest bankruptcy of all time [25].

Case WannaCry Campaign

Quite a recent example of a cyber-attack is from May 2017; the case is called WannaCry ransom ware [26].

This campaign had several unprofessional features and because to them, direct damages were relatively small. However, indirect damages were notable. It disrupted normal functions of several critical infrastructure systems all over the world, including hospitals and traffic. It was fortunate for the societies that the attackers’ goal was only to deploy ransom ware and collect ransom instead of destroying the compromised ICT systems or stealing the information that was accessed.

In the scope of this paper, WannaCry campaign had two interesting features. The first interesting feature was the speed of contamination of the systems. The previous example campaign was active for several years. This campaign was only active for days. The progress speed was so rapid that the analysis and counter measures of a single system took too much time to be effective. The blocking actions were only successful because of information exchange between security specialists across organizational and geological boundaries, and centralized blocking actions.

The second interesting feature was the methodology used in the campaign. It utilized the technology developed by the National Security Agency, USA (NSA), which was leaked to the public earlier. Despite that the mechanisms were known before the attack, there was a large amount of compromised systems worldwide. As a consequence, one can never trust or assume that the supply chain or the subcontractor has implemented the full preventive toolset for known threats. Furthermore, it is evident that the unknown threats are even less likely being monitored.

Analysis of the case

In both cases, the attack was blocked by centralized and coordinated actions. To obligate the supply chain node or the subcontractor to monitor systems preventing advanced and persistent type campaigns is nearly an impossible task. Only the one, that manages the environment as a whole and understands the possible goals of an attacker and also carries the business risk, can evaluate the differences and abnormalities of actions in a complex system environment.

We have also observed from empirical data of less public campaigns that the value of damage changes with time as follows [21]:

- the financial/business damage development follows a time-based logarithmic formula:
  - time 0 is the attacker's penetration into the component/system,
  - time 1 is the time the actual damage driven action begins,
  - between 0 and 1 the attacker prepares the actual damage enabling action, such as intelligence and creation of necessary command functions,
  - onward from time 1 there is increasing damage to the component in relation to the maximum value of the component to the whole business value of the operations;
- the value of damage increases exponentially in the relation to time:
  - effects in the individual component reflect to the whole system and increase the overall damage and financial loss.

Improving business resilience to unknown threats

Inspired by the case example presented in the previous chapters, the purpose of the improvement of resilience to unknown threats is to create a model, which tries to take into account the previously unrecognized threat to the specific business. The approximation in the model is based on the previous work by Zaerens [27], which showed the necessity to analyze financial impacts of threat prevention.

In this assessment, the authors are limiting their research to the main owner of the business. Also, an individual component under the research is not necessarily a technical phenomenon or a part of the IT-system. Depending on the business environment, the component can be a technical phenomenon, a business concept or a business driven phenomenon such as customer value creation. The main owner in the model is a company/function, which offers the final product to the end-user.

The observations in the model are based on either the sensor-based observation or on the log-based observation. Based on this definition, the only restriction to observation is the components ability to create material for analyzing purposes. This material is produced by the sensor and it can be technical, automatic or based on human interaction.

Each system component has to have a sensor, which collects information for observation purposes. This is illustrated in formula 1, a cluster of components in the system $sens_j$ in which $j \in [1,\ S]$ and S equal the amount of components in the system.

The sensor's ability to observe the threat can be assessed by using relative probability $1/w$, where w equals the coverage of information relating to the unknown threat.

In the worst case scenario, information is not collected at all and the possibility to react to the threat is non-existent. Threat observation is divided into ten operations within four previously introduced functions; the operations are managed as a part of operations management, using recognized capabilities.

The sensor's capability to reduce the unknown threat is presented in formula 2 developed by Zaerens in his previous research (Zaerens, 2015)

$$R_n = f(P(\text{threat}\, i_1 * (1/w_{\text{sens[1]}})), \ldots, \\ P(\text{threat}\, n_s * (1/w_{\text{sens[s]}}))).$$

In order to clarify the topic, the authors defined the attack vector as a function, whose purpose is to fulfil the threat. The assumption is that the attack vector has a linear relationship with the threat. This excludes surveillance activities, whose purpose is to define possible existing vulnerabilities in the target component.

Sensor activity is a constant, on-going function, which requires continuous sensor development in order to manage threat observation. This demands investments from the sensor throughout its lifecycle. This life-cycle cost is usually estimated to be 10 % of the initial investment. This enables life-cycle estimation as follows:

$$c_{\text{sens}} = d(1 + 0,1tw),$$

in which d – initial investment, t – time, w – a relative data collection ability in a specific sensor.

Even though these formulae increase a sensor's effectiveness against the threat, they do not take the costs, which are related to data analysis, into account. Obviously threat reduction is possible only, if the collected data collected from the sensor is analyzed. To simplify our approach we assume that the collected data contains sufficient data for exposing the attack.

Decentralized component based analysis can be described as a system where a real-time function of some predefined rule catches an anomaly or an exception. Component based cost analysis can be calculated using the following formula 4

$$h_{\text{sens[w]}},$$

in which h – cost of the analysis by individual component w used.

We assume that the size of the rule set in component analysis does not affect the actual cost of the analysis. The effectiveness of component based analysis is reduced, if the area under observation is not restricted and its interphases to business processes are not defined adequately. Moreover, the real time observation significantly decreases the possibility for detecting attacks that have been going on for a long duration (e.g. APT type of campaigns).

Financial effects of the centralized approach can be calculated using the following formula 5. This concentrated analysis estimates information from several sensors and their interdependencies. The cost of the analysis is not solely based on the amount of sensor; it is based on average threat coverage

$$C_{\text{analysis}} = h\left(\left(\sum_{i=1}^{\text{sens[n]}} w_{\text{sens[i]}}\right) \Big/ n + \sum_{i=1}^{\text{sens[n]}} i\right),$$

in which h – cost of the analysis, n – amount of sensors.

The effectiveness of the analysis increases when the amount of information from sensors increases.

Instead of centralized monitoring, having each component implemented with its own monitoring capability, the total cost of analysis of the system is the sum of all sensor and analysis costs from each partial component in the system. It is evident that even if the amount of sensors would be greater in some of the outsourced components, the overall effectivity of analysis significantly lacks business related information. Therefore the cost-effectivity ratio is better for centralized systems rather than distributed systems.

Discussion

Dialogue between the supply chain stakeholders does not jeopardize the risk management procedures of a supply chain, quite the opposite. It creates a solid base for understanding the system's stakeholders and their needs throughout the different life cycles of a supply chain. Maglio, Srinivasan, Kreulen, and Spohrer [28] envision that service scientists could begin to understand service systems by identifying stakeholders and their needs, opportunities and problems in the environment. Theories behind the service science need to be analyzed during development work. It should be done due to the fact that capability management requires open multidiscipline dialogue between different disciplines and functions.

Looking at the five operational domains, it becomes evident, that the assessment of an individual domain, process or a single actor's CIP capability is not adequate. There is a need to find those processes, which have the largest number of interfaces with each of the domains and the whole ecosystem. This should be the end result of an effective, centrally controlled surveillance activity.

As our research indicates, comprehensive, systems-wide protection can become extremely expensive. There are two questions, which arise from this conclusion. The first question is: who is responsible for the investments holistic protection demands? Secondly, what is the alternative cost for ecosystem-wide protection? One can ask if a main company should invest in tracking and control functions, instead of a "bullet proofed", ecosystem-wide active protection.

The role of a contractual agreement should be seen as an assumption of the future state of the CIP, not as a boundary between the actors participating in the service supply chain. Contractual agreements should be formed following the principles used in the performance based logistics (PBL).

In the PBL, responsibility of the product/service system management is on the supplier of the system, unlike in the traditional end-user – supplier relationship [29]. PBL is in use in military context and it is "a contractual mechanism".

Berkowitz explains that

> *"...[a] contractual mechanisms will include long-term relationships and appropriately structured incentives with service providers..., to support the end user's (warfighter's) objectives."* [30, p. 5].

This approach does not contradict with the idea of the centralized surveillance and monitoring system. Centralized monitoring and surveillance activities should be used to secure both adequate CIP and a source for the PBL incentives. Also, requirements based PBL emphasizes the positive sides of the structural and trust based contractual management. The existing incentives encourage a service provider to fulfil pre-determined service goals, as research by Doerr, Lewis and Eaton [31] has shown, because these benefits are accountable and reliably measurable.

Limitations of the study

As mentioned before, this paper is limited according the public information available. Attacked organizations are reluctant to comment the success rates or the damage impact of attacks even if they are known. This ensures the preservation of their reputation and trust relations in the economic systems they participate in. The damages of successful attacks, that are publicly known, are underrated without exception [32, 33]. It is notable that attacks are not made public, unless a third party brings the information to attention.

Recommendation for future research

An interesting research area would be to model the progression of an attack in relation to time. This enables the analysis of the timeframe in which the attacker could theoretically reach the business's critical information after entering the system. This kind of a model would assist in estimating the available time for countermeasures or the collection of forensic information and analysis of attack progression.

Conclusions

Combining the systems wide approach and explaining the theoretical background behind the various models creates a comprehensive model, which assists in critical infrastructure protection. It shows that individual supply chains are a collection of extremely complex systems and subsystems backed up with sometimes contradicting theories and practices.

Current global trading operates in an environment, which is highly vulnerable to abnormalities in all parts of the supply chain. During a value creation process, an IT-infrastructure (a cyber-system) is dependent on five basic components:

1. input information, which reflects the reality of the surrounding world,
2. stored data of the existing reality to help decision making processes,
3. information stimulating the "organ" (human, machine), which in turn affects and stimulates the system,
4. data referring to the desired future state of the system,
5. feedback information regarding the desired outcome of the system or parts of the subsystem [34, p. 11].

All of the organizational functions – implementation, coordination, control and intelligence – across the system and relating subsystems are dependent upon the five components presented above. Each of the five components is subject to vulnerability and risk. This requires a description of the capabilities, which are needed to manage both functions and basic components of system wide vulnerability and risk management. Without these descriptions there is no possibility to calculate the financial effects of CIP.

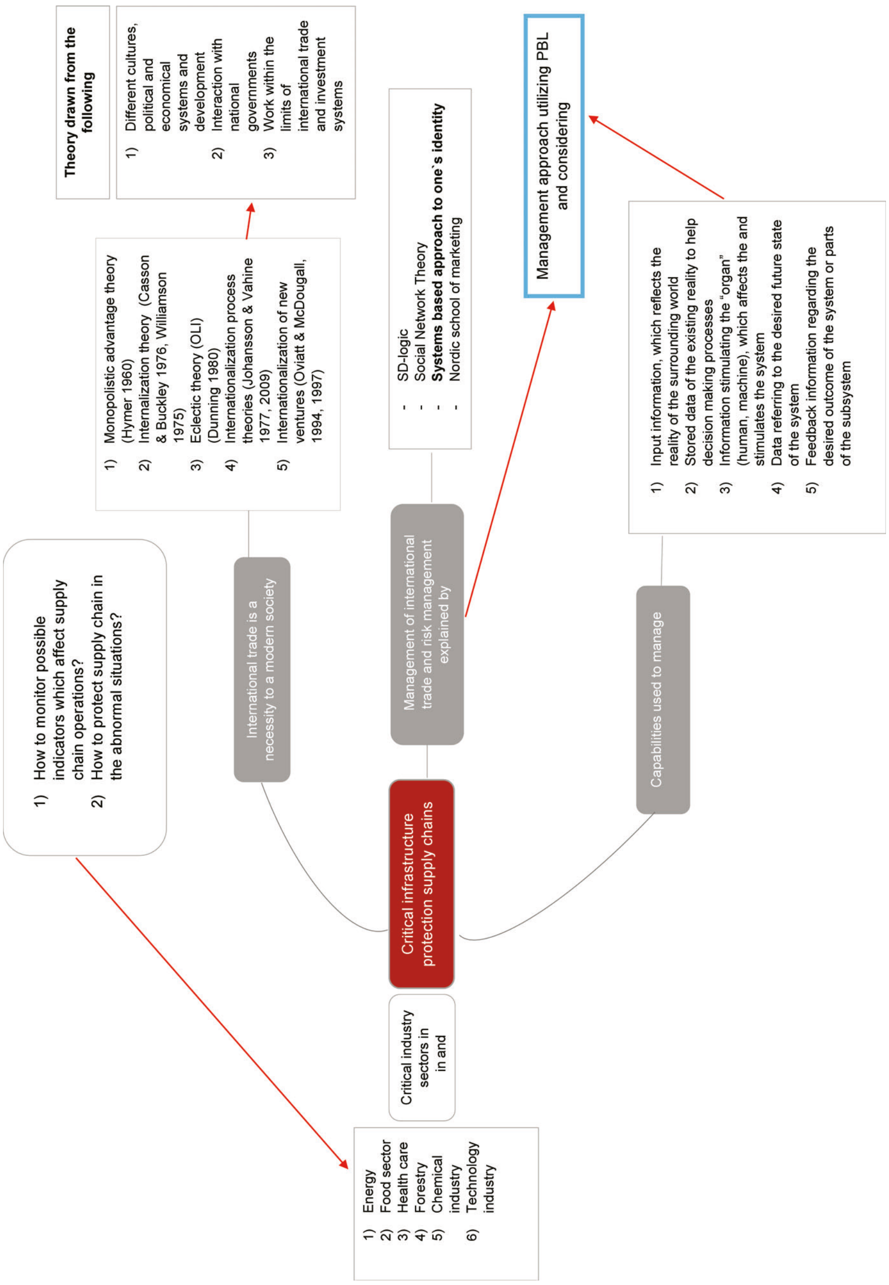
Because a supply chain consists of a large number of multinational actors, each one of these players is potentially a critical node due to efficiency requirements defined by financial requirements. But unless an individual node affects pre-determined critical processes in the critical domain, a total collapse of the supply chain is not foreseeable. But there is a need for a systematic method, which enables the assessment of entire systems and their subsystems.

The authors have come to the conclusion, that the principles of cyber protection illustrated by i.a. Kuusisto [34], can be followed in commercial supply chain management. The following IT-infrastructure capability areas should be monitored, protected and secured thoroughly only if the benefits are on a financially acceptable level:

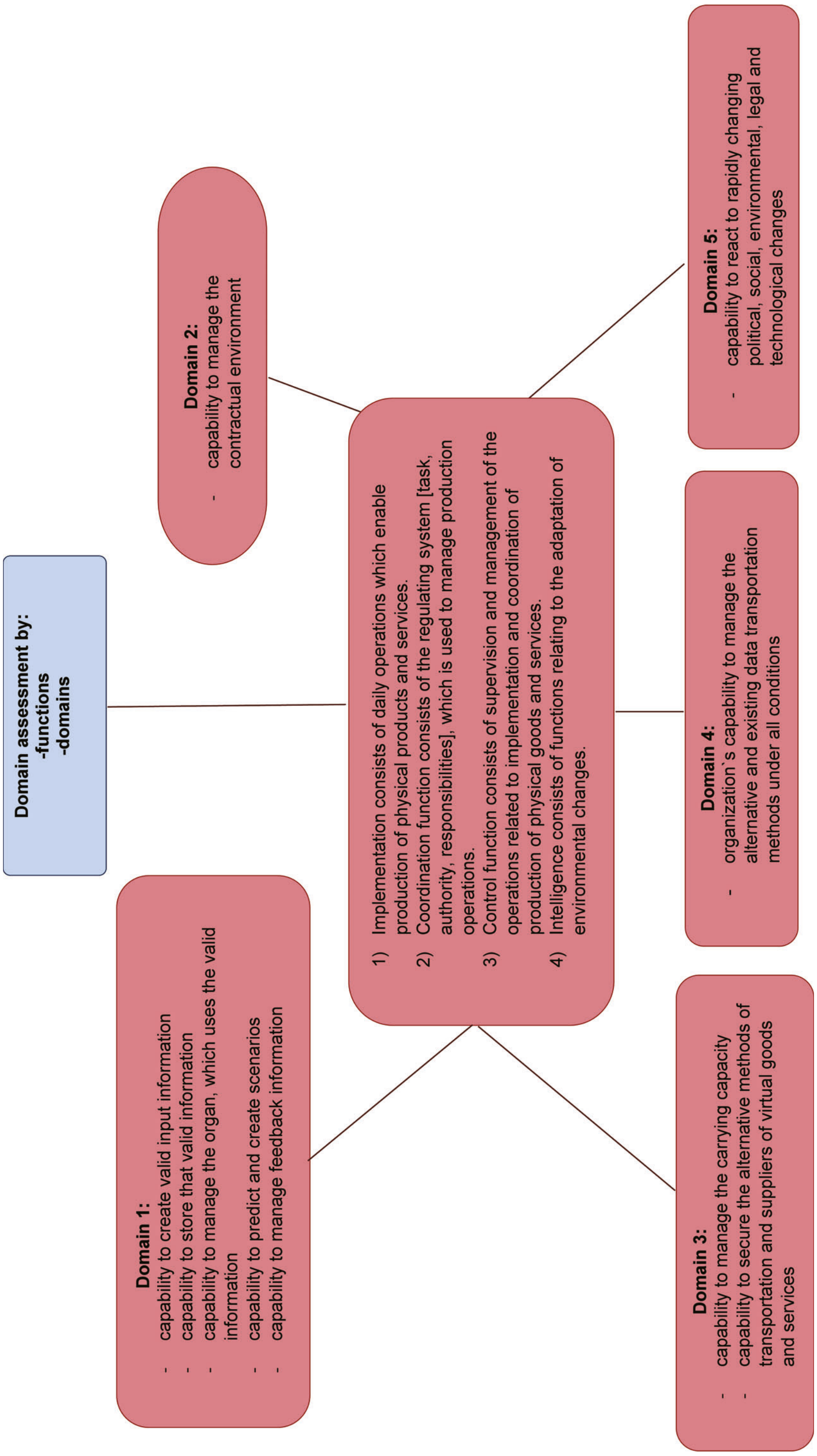
1. the capability to create valid input information, which enables necessary vulnerability analysis,
2. the capability to store said valid information in a way that it meets the requirements for the protection of the supply chain,
3. the capability to manage the organ, which uses the valid information,
4. the capability to predict and create scenarios, which require valid information,
5. the capability to manage feedback information and most of all, manage the pre-determined operations based on the scenarios.

In this paper we examined the domain assessment within the critical infrastructure protection. We stated that business ecosystem environment that contains supply chains or subcontracting is vulnerable for unknown threat. Yet we noted that distributed ecosystem can increase the resilience in operation with careful contractual management. We described the model that quantifies the key elements that are used in observing the malicious intrusions to business system. We also proposed what needs to be taken into consideration in enhancing more resilient business ecosystem.

Appendix 1. Framework for Critical Infrastructure Protection


Critical infrastructure protection supply chains
Critical industry sectors in and
1) Energy
2) Food sector
3) Health care
4) Forestry
5) Chemical industry
6) Technology industry
1) How to monitor possible indicators which affect supply chain operations?
2) How to protect supply chain in the abnormal situations?
International trade is a necessity to a modern society
1) Monopolistic advantage theory (Hymer 1960)
2) Internalization theory (Casson & Buckley 1976, Williamson 1975)
3) Eclectic theory (OLI) (Dunning 1980)
4) Internationalization process theories (Johansson & Vahine 1977, 2009)
5) Internationalization of new ventures (Oviatt & McDougall, 1994, 1997)
Theory drawn from the following
1) Different cultures, political and economical systems and development
2) Interaction with national governments
3) Work within the limits of international trade and investment systems
Management of international trade and risk management explained by
- SD-logic
- Social Network Theory
- Systems based approach to one`s identity
- Nordic school of marketing
Management approach utilizing PBL and considering
Capabilities used to manage
1) Input information, which reflects the reality of the surrounding world
2) Stored data of the existing reality to help decision making processes
3) Information stimulating the "organ" (human, machine), which affects the and stimulates the system
4) Data referring to the desired future state of the system
5) Feedback information regarding the desired outcome of the system or parts of the subsystem

Appendix 2. Domain Assessment model



Domain assessment by:
-functions
-domains

1) Implementation consists of daily operations which enable production of physical products and services.
2) Coordination function consists of the regulating system [task, authority, responsibilities], which is used to manage production operations.
3) Control function consists of supervision and management of the operations related to implementation and coordination of production of physical goods and services.
4) Intelligence consists of functions relating to the adaptation of environmental changes.

Domain 1:
- capability to create valid input information
- capability to store that valid information
- capability to manage the organ, which uses the valid information
- capability to predict and create scenarios
- capability to manage feedback information

Domain 2:
- capability to manage the contractual environment

Domain 3:
- capability to manage the carrying capacity
- capability to secure the alternative methods of transportation and suppliers of virtual goods and services

Domain 4:
- organization`s capability to manage the alternative and existing data transportation methods under all conditions

Domain 5:
- capability to react to rapidly changing political, social, environmental, legal and technological changes

This work has been partially supported by CGI Finland (http://www.CGI.com/), with particular support from Jan Mickos. His contribution to determining the analysis on unknown threats is appreciated.

References

[1] Laanti R., Gabrielsson M., Gabrielsson P., *The globalization strategies of business-to-business born global firms in the wireless technology industry*, Industrial Marketing Management, 36, 8, 1104–1117, 2007.

[2] Bertelsmann Foundation, *Globalization Gains for Developed Countries Outpace Those for Emerging Nations* Retrieved June 15, 2016, from http://www.bfna.org/article/globalization-gains-for-developed-countries-outpace-those-for-emerging-nations

[3] Lewis T.G., *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons, 2014.

[4] Beer R.D., *A dynamical systems perspective on agent-environment interaction*, Artificial Intelligence, 72, 1, 173–215, 1995.

[5] Teller J., Kock A., Gemünden H.G., *Risk management in project portfolios is more than managing project risks: a contingency perspective on risk management*, Project Management Journal, 45, 4, 67–80, 2014.

[6] Galbraith J.R., *Designing complex organizations*, Addison-Wesley Longman Publishing Co., Inc., 1973.

[7] Liesch P.W., Welch L.S., Buckley P.J., *Risk and uncertainty in internationalisation and international entrepreneurship studies*, Management International Review, 51, 6, 851–873, 2011.

[8] Zsidisin G.A. et al., *An analysis of supply risk assessment techniques*, International Journal of Physical Distribution & Logistics Management, 34, 5, 397–413, 2004.

[9] Vargo S.L., Lusch R.F., *Service-dominant logic: continuing the evolution*, Journal of the Academy of Marketing Science, 36, 1, 1–10, 2008.

[10] Grönroos C., *Marketing as promise management: regaining customer management for marketing*, Journal of Business & Industrial Marketing, 24, 5/6, 351–359, 2009.

[11] Hoffman M.L., *Empathy and moral development: implications for caring and justice*, Cambridge University Press, 2001.

[12] Bronfenbrenner U., *Ecology of the family as a context for human development: research perspectives*, Developmental Psychology, 22, 6, 723, 1986.

[13] Horsmanheimo S., Kokkoniemi-Tarkkanen H., Kuusela P., Tuomimäki L., Puuska S., Vankka J., *Kriittisen infrastruktuurin tilannetietoisuus*, Valtioneuvoston Selvitys- ja Tutkimustoiminnan Julkaisusarja, 19, 2017.

[14] Endsley M.R., *Toward a theory of situation awareness in dynamic systems*, Human Factors: the Journal of the Human Factors and Ergonomics Society, 37, 1, 32–64, 1995.

[15] Skyttner L., *General systems theory: problems, perspectives, practice*, World Scientific, 2005.

[16] Anteroinen J., *Enhancing the development of military capabilities by a systems approach*, Maanpuolustuskorkeakoulu, 2013.

[17] Lyons B., Mehta J., *Contracts, opportunism and trust: self-interest and social orientation*, Cambridge Journal of Economics, 21, 2, 239–257, 1997.

[18] Rousseau D.M., Sitkin S.B., Burt R.S., Camerer C., *Not so different after all: a cross-discipline view of trust*, Academy of Management Review, 23, 3, 393–404, 1998.

[19] McCabe K.A., Rigdon M.L., Smith V.L., *Positive reciprocity and intentions in trust games*, Journal of Economic Behavior & Organization, 52, 2, 267–275, 2003.

[20] Trivers R.L., *The evolution of reciprocal altruism*, The Quarterly Eeview of Biology, 46, 1, 35–57, 1971.

[21] Mickos J., Interview, March 23.

[22] BAE systems threat research blog. Retrieved June 3rd, 2017 from: http://baesystemsai.blogspot.se/2017/04/apt10-operation-cloud-hopper_3.html. [Accessed 3 Jun. 2017].

[23] FireEye, *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*, FireEye Threat Intelligence, Special Report, 2015.

[24] Naraine R., *Nortel hacking attack went unnoticed for almost 10 years*, [online] ZDNet. Retrieved June 3rd, 2017, from http://www.zdnet.com/article/nortel-hacking-attack-went-unnoticed-for-almost-10-years, 2012.

[25] Reuters, *TIMELINE: Key dates in the history of Nortel*, Reuters TECHNOLOGY NEWS, 14.1.2009. Retrieved July 1st, 2017 from http://www.reuters.com/article/us-nortel-timeline-sb-idUSTRE50D3N120090115.

[26] US-CERT, *U.S. Department of Homeland Security: Alert Report*, Retrieved May 27th, from https://www.us-cert.gov/ncas, 2017.

[27] Zaerens K., *Business Resilient Vulnerability Analysis for Dynamic High Security Environment*, 18th International Conference on Network-Based Information Systems, 2015.

[28] Maglio P.P., Srinivasan S., Kreulen J.T., Spohrer J., *Service systems, service scientists, SSME, and innovation*, Communications of the ACM, 49, 7, 81–85, 2006.

[29] Randall W.S., Pohlen T.L., Hanna J.B., *Evolving a theory of performance-based logistics using insights from service dominant logic*, Journal of Business Logistics, 31, 2, 35–61, 2010.

[30] Berkowitz D., Gupta J.N., Simpson J.T., McWilliams J., Delayne L., Brown B., Sparks T., *Performance Based Logistics*, Center for the Management of Science and Technology, Huntsville, AL, 2003.

[31] Doerr K., Lewis I., Eaton D.R., *Measurement issues in performance-based logistics*, Journal of Public Procurement, 5, 2, 164, 2005.

[32] ForMin Finland, *Tietoturvaloukkaus Suomen ulkoasiainhallinnossa – Ulkoasiainministeriö: Ajankohtaista*, Retrieved June 3rd, from http://formin.finland.fi/public/default.aspx?contentid=291701&contentlan=1&culture=fi-FI, 2013.

[33] Yle Uutiset, *Supo: Ulkoministeriö joutui kaksi kertaa vakoilun kohteeksi*, Retrieved June 3rd, from http://yle.fi/uutiset/3-7332824, 2014.

[34] Kuusisto T., *Kybertaistelu 2020*, Julkaisusarja 2: Asiatietoa, No. 1/2014.

In the appenpendices

Buckley P.J., Casson M., *Future of the multinational enterprise.* Springer, 1976.

Dunning J.H., *Toward an eclectic theory of international production: some empirical tests*, Journal of International Business Studies, 11, 1, 9–31, 1980.

Henriques I., Sanjay Sharma, *Pathways of stakeholder influence in the Canadian forestry industry*, Business Strategy and the Environment, 14, 6, 384–398, 2005.

Johanson J., Vahlne J.E., *The Uppsala internationalization process model revisited: from liability of foreignness to liability of outsidership*, Journal of International Business Studies, 40, 9, 1411–1431, 2009.

VI

2018 IEEE. Author manuscript in accepted version,
published with permission. If citing, please use:
Klaus Zaerens
Concept for Controlled Business Critical Information Sharing using Smart Contracts
2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018, pp. 1-8.
https://doi.org/10.1109/CSNET.2018.8602824

2018 2nd Cyber Security in Networking Conference (CSNet)

Concept for Controlled Business Critical Information Sharing using Smart Contracts

Klaus Zaerens
Department of Military Technology
National Defence University
Helsinki, Finland
Klaus.Zaerens@iki.fi

***Abstract*— Trust management has been a topic of keen interest in recent years. There has been a lot of discussion as to what new opportunities it can bring to markets, what benefits it can offer, and what system development possibilities it enables for software development. In this paper we discuss trust management and business critical information sharing in a definite group of stakeholders called Circle of Trust. We examine the key features of the Circle of Trust in military environments. We address the most essential problems and obstacles to be considered before the benefits of Circle of Trust can be fully enabled therein. As a solution to problems with the information transfer management, we propose a novel conceptual approach which ensures the privacy of the data source and transparency of information sharing utilizing the blockchain technology and modern cryptographic solutions. In addition, the concept presented enables the quantitative information trade and objective control mechanism for contractual liabilities within the consortium. The discussion and views presented in this paper can be adopted in any organization with doubts concerning the sensitive and classified contents of supply chain management or current ICT systems.**

Keywords*— *Trust management, Information Sharing, Security Management, Cryptography, Military

I. Introduction

Importance of trust management is increasing as the Internet is more open for access, different collaboration environments have become more common and social networking affects our decision making. The relevance of trust management is gradually becoming more significant, but the multilateral nature of the concept, generally trustworthy parties and large data sets with high response time requirements have kept commercial activators and applications away from production use in public authority environments [1].

Public authorities in security field have sought and developed numerous means to improve cooperation by ICT solutions [1]. Different kind of collaboration tools and environments has been deployed and integrations between systems and data storages have developed. It is obvious that concepts like semantic knowledge processing, connectivity and social networking enables improved cooperation between authorities. However, these concepts also cause new challenges. Openness can be hard to manage in highly secured environment. Also processing and sharing the critical operative information increases hostile interest on system environment.

In public authority environment the trust in other stakeholder is unreserved in relation to profession and officiality. In collaboration and cooperation context, participating authorities compose virtual community with only trusted parties [2]. We call this kind of consortium a Circle of Trust. Within the Circle of Trust, the participant shares information in a way that the other participants will improve their success in operations. This enhances the overall performance of the virtual community from which every participant gain benefit.

The special case of information sharing is to delegate operative situational data for improving situational awareness in the Circle of Trust. This kind of collaboration improves the accuracy of the individual awareness in each actor and enriches the awareness of all actors within operation. This cooperation enables better communications, safe procedures and more effective actions in operations throughout participating authority organizations.

In this paper, we will discuss issues and problems to be considered when implementing Circle of Trust concept in core authority systems. We define the key characteristics of such a high security environment. We will narrow our observations to military systems in which the need for computational capacity is high and the reliability of information is always critical. In military environment we must ensure data flow correctness, traceability and survivability. In this paper we discuss on a situation where a trusted node forfeited credibility and we should control the information or knowledge the node receives from our trusted network. As a solution to problems with the adoption of Circle of Trust in high security environments, we propose a novel Enhanced Information Sharing Management approach based on blockchain technology that manages the delivery of information within the closed Circle of Trust and improve the security of overall system by reducing the risk of information being compromised.

II. Situational Awareness and Trust Management in Military Context

Improving situation awareness has become more critical in public authority operations and especially in military context. The possibilities and utilizations of situation awareness have

978-1-5386-7045-3/18/$31.00 ©2018 IEEE
XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

increased together with technical evolution. Sensors and mobile devices increase the effectivity of collecting data from locations that traditionally have been difficult to access. More data can be collected and stored than previously, which enables view on situation to be more truthful, accurate and comprehensive.

Most of the severe challenges on improving situation awareness are related to refinement of significant information from huge amount of data, unstable data transfer connections and especially in field operations, limited data capacities [1]. Data correctness, reliability, redundancy and timeliness have also been discussed in several publications [1]. Less discussion has been addressed to trust evaluation of the data source or the security issues on delegating the situational data to recipients with different trust levels. This aspect is relevant in military environment where there is always possibility for a malicious actor receiving confidential information or sending unreliable data to decision making process.

In this paper we adopt the definition of trust presented by Grandison and Sloman because of the simplicity yet complete enough. According to Grandison and Sloman, trust is a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context [2]. Moreover, in this paper we limit our observation on computative trust management. Widely accepted features on computative trust management include subjectivity, the expected probability and relevance [3, 4].

In military context participants of the trust relation are bound to a role. A participant represents some actor or unit within an organization. Unit has a task and a goal and special expertise specified by the organization. In this environment, two interacting actors from different units trust the represented role of the other not the actor itself. Yet the trustworthiness between two roles can be fixed on process level, the individual actor might have specific preferences, interests or experience which affects to quantitative trust. Similarly, data providers such as sensors can be modelled as an actor in trust relation and represented by an ownership of an organizational unit.

III. Circle of Trust Characteristics and Benefits in Military Environments

In this paper we define Circle of Trust as a consortium of a specified subject with only trusted parties. It means that each participant has sufficient amount of trust to other participant in relation to the subject. The sufficient can be considered as readiness for deliver and receive knowledge unconditionally without risking own operative ability. The motivation for creating the consortium is to construct a united force to gain improved capability in operations with the same goal. For achieving the goal it is essential to have an open and transparent information exchange between the participants. To sustain the circle, all parties should have indirect or direct benefit from collaboration and cooperation with each other. The participants rely operative enhancement that they gain from the participation of the circle. Enhancement can be for example improvement of efficiency in operative actions or overall reduction of operative costs. In practice the actions can be trading situational information between participants. Moreover, we argue that the Circle of Trust formed by combining the public authorities from different countries is the only real possibility to improve the situational awareness in order to operate successfully in cyberwar. Malicious actions in cyberwar are conducted always from international level and often routing is hiding the origins of the actor. Resolving the actor needs international collaboration with openness of information. We should not forget that defending from malicious action on solely national level can be only reactive by nature. That is why countermeasures are effective only when performed also on international level. The information collected by international consortium can help to identify the existence of malicious actor and to detect false information from the attacked systems.

The example of Circle of Trust is illustrated in Fig. 1. In Fig. 1 *A* represents us as a situational information provider. *B* and *C* are recipients of our information. Arcs represent the direction of information. Because information trading should happen in both directions, arcs are represented also from the recipient to provider. Each arc contains two parameters *s* for situational information and *w* for the weighted trust between information provider and recipient. It is notable, that if for example $w_{AC} \neq w_{AB}$ then $s_{AC} \neq s_{AB}$. In practice this means, that the situational information provided by the provider is not the same unless the trust relation between provider and recipient were exactly the same. It can also be noted that the trustworthiness of the recipient is in direct relation to the correctness and completeness of the situational information provided by the information provider.

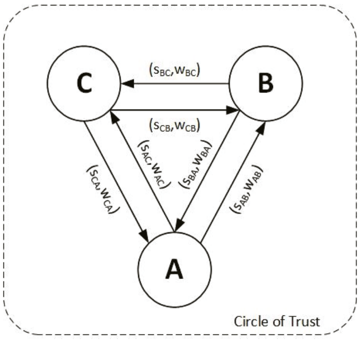


Fig. 1. Circle of Trust

As stated before, with Circle of Trust situational awareness can be improved by trading the intelligence and reconnaissance information within the participants of the Circle. Trading is usually mutual sharing where the quality and the amount of traded information are in balance.

The trading can also be used for identifying possible leakages. If there is a suspected malicious actor as a member in Circle of Trust, with labelled or water marked information to participants it is possible to detect and identify the source of leakage by following the trace of the information. If there is certainty of an intrusion to system, with Circle of Trust deceptive information can be fed to malicious actor without breaking the routines and not disconnecting the actor from the grid too soon. More over the capabilities of a hostile actor can

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

be monitored and evaluated by observing the actions it performs in controlled environment [5].

Circle of Trust is a scalable and generic concept. In international scale we can consider a military alliance such as NATO as an example of Circle of Trust. On national scale example can found from the collaboration with public authorities of safety such as between police forces and rescue service. On organizational level we can have example from ministry like Ministry of the Interior and all the agencies that it conducts or the supply chain of financial ecosystem. On the technological level all nodes in a high security network form definite Circle of Trust.

IV. Challenges in Information Sharing

In this chapter we discuss more on challenges identified within the Circle of Trust. The Circle of Trust should enable openness of information exchange, but the openness also increases the risk of revealing too much sensitive information to public.

Situation data contains always some information about the collector or origins of data by nature. This information can relate to location information, resources or capability. This information can be used against the originator. Revealing information is always risk and the delivery should be somehow controlled so that the information, knowledge or capabilities are not leaked to any hostile or untrusted recipient.

A. *Absolute Trust Does not Exist in Reality*

Within closed Circle of Trust, some parties are always more trustworthy than others. For example, in military alliance some nations are in more deep cooperation than others and some nations can have doubts from history to others. In that sense the sufficient amount of trust can be varied a lot between the actors. The consequence is that the participants in the Circle of Trust are not in the same level. In authority cooperation trust within own organization is usually unreserved. This trust is based on mutual experience, common procedures and professional community. A lot harder is to trust another authority and different organization. We can find this element of distrust in each level of Circle of Trust concept. The main concern is the leakage of sensitive information illustrated in Fig. 2. After revealing information for recipient *C*, we are not able to manage the revealed information. If *C* has a connection with party *D*, which does not belong to our original Circle of Trust, *C* might still provide some information to *D*. Assuming that *A* is the only information source, the *D* will receive information $s_{CD} \subseteq s_{AC}$.

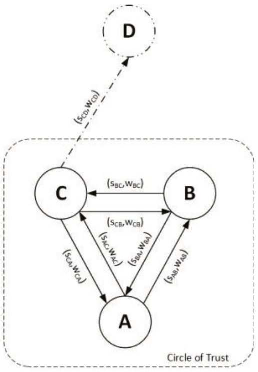


Fig. 2. Leakage of information

Another dimension of this challenge is the publicity of distrust. If one actor is not ready to release all information unconditionally to all other actors but is bound to principality of openness within the circle, how publicly this limitation of released information can be made.

B. *Managing Information Sharing in Open Network*

In the previous chapter we discussed on leakage of information. Regardless of how much we have trust on our allies, we need their information. To receive information from other parties the usual convention is to give or send information collected by the one. This actually forms a trading system where tradable information is defined by its usefulness, timeliness, trustworthiness, accuracy and comprehension. As stated in previous chapter, absolute trust does not exist in reality. Circle of Trust or any alliance is trying to form a framework where quality levels of information that are agreed on are written and we can rely that at least the exchange of information itself would actualize. Information providers try to minimize the amount of sent information but still receiving the maximum amount of information. The main goal of the recipient is to have sufficient amount of information to form awareness of a situation. The interesting question is that what is the sufficient amount of provided information to gain that goal?

Another issue arises when information is sent to the recipient. After transmission of information the provider loses all control of the sent information. That when a receiver has interpreted the information, the receiver immediately owns the information and can use it to any purpose needed. This includes also sending the information to other partners, avoided or simply not intended by original source. Having secured connection does not solve this issue since for the received information is presented in a decrypted form.

The accumulation of information can be also a problem. This situation is illustrated in Fig. 3. If *A* sends data fragment s_{AB} to recipient *B* and data fragment s_{AC} is send to recipient *C*, it is possible that both of the recipients send the data fragments to less trustworthy participant *D*. *D* can combine the both data fragments $s_{AB} \cup s_{AC}$ and create more comprehensive situation and indirectly form an increased risk to the originator *A*.

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

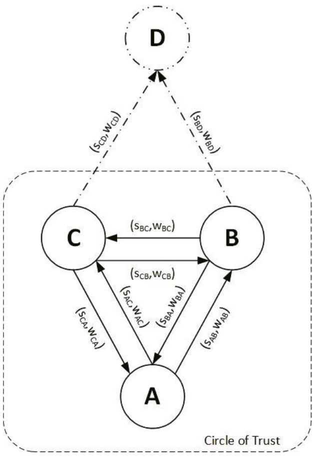


Fig. 3. Accumulation of information

C. Collateral Damage of Deception

Previously we described the possibility of deception with the identified intrusion in the secure environment. The challenge is how the intrusion is notified to other participants in the Circle without risking that the information is reached to the intruder. This problem setting is formalized in Fig. 4, in which A has some distrust with C (i.e. w_{AC} is small) and decides to send false information s_{AC}. At the same time C and B have a strong trust relation (i.e. w_{BC} and w_{CB} are large) and also A and B trust each other. If C transmits the information s_{AC} as s_{CB}, B receives false data which can be very harmful of course for B, but also for A. After exposure of deception the trustweight w_{BA} is most probable to decline, which influences the future information exchange and trade balance.

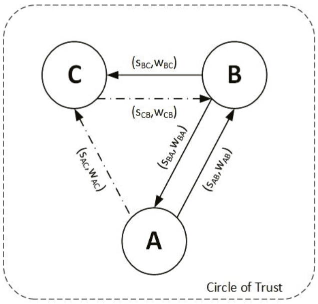


Fig. 4. Collateral damage of deception

A special case of this problem occurs when one participant in Circle of Trust identifies an intruder within the Circle. If the other participants are not trustworthy enough to identify the intruder and the deceptive data is fed to the intruder, how can we notify the other participants not to trust information that they receive from the intruder.

V. Overcoming Obstacles

Traditionally Information Sharing is technically conducted by the point to point (P2P) connections between information provider and recipient. Connections are usually secured by Public Key Infrastructure based Virtual Private Networking (VPN). The information shared within the connection is conducted by the trust between the provider and recipient. This sharing mechanism becomes complex if same information should be transmitted to several participants or a collaboration platform is needed. In addition to that, ensuring the survivability, timeliness, openness, privacy and usefulness of data across all participants of the mutual interest group is an expensive system to be developed.

We propose an approach based on blockchain technology to overcome the problems and obstacles in information sharing stated in previous section. Since implementations of the blockchain technology are evolving we will focus to the principles of our approach and relax platform specific details such as performance or security issues from the scope of this paper. The most essential additional requirements of our approach for the blockchain technology platform are support for smart contracts and privacy enabled joined transactions. In this paper we propose the Ethereum project as an example of platform containing sufficient technological features [6].

A. About Blockchain Technology and Smart Contracts

The blockchain technology is one of the most prominent new technologies. It utilizes the decentralized management of assets and ensures the consistency of information by encrypting the transactions with previous states of information. The information management and consistency are solved by miners that verify the correctness of the system and final states of information. These miners receive a small fee for their effort [7, 8].

The most famous implementation of blockchain technology is the Bitcoin system. Bitcoin is a cryptocurrency without any centralized management or issuer such bank [7]. All participating nodes the Bitcoin system have information on all accounts in the system and are responsible for ensuring the correctness of account balances. Accounts are anonymized but the contents and the transactions are public. If some amount of currency is to be transferred to the other account, a transaction entry is created with previous addresses of currency, the amount of currency and the recipient address. This entry is encrypted and delegated to the system nodes to be verified, validated and committed. System nodes that commit the transactions are called as miners and they receive a reward as Bitcoin currency [7]. This work increases the amount of currency in system which ensures the growth of the Bitcoin financial system.

Bitcoin success story has brought up several other application areas where similar technology could be utilized. Bitcoin implementation has some limitations such as scripting or lack of meta-protocols [6]. A need for passing agreements between stakeholders in more comprehensive manner was also observed. Ethereum is one of the projects that address these limitations by introducing an abstraction layer on top of the basic blockchain platform [6]. The layer contains built-in Turing-complete programming language which ensures that more complex systems can be implemented. In Ethereum, contracts can have data, conditions, operations and they can

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

return a value similarly than functions. An interesting feature is that the contract itself can also create another contract and the role of created contract in system can differ from the originating contract. This allows us to implement more sophisticated systems such as escrow-, reputation-, identity management- or gambling applications where a third party is needed for guaranteeing the agreement between contractors [6, 9].

B. *Enhanced Information Sharing Management*

Our approach is based on improved blockchain technology platform with additional components for sharing and managing the information. The blockchain implements features such as traceability and openness by design. Decentralized management improves the survivability of system and enhances the collaboration between participants [7]. The blockchain platform ensures consistency and trustworthiness of the whole chain of information with the audit trail leading back to the information origins [10, 11]. Circle of Trust requires closed environment and encryption of shared business-critical information content.

In our information sharing management scheme set of data fragments *S* from information providers are pooled and made available for every participant to use. The trust is determined towards the system by the quality of information received. This relaxes the need for trusting the other participants and transmits the trust management to the information management engine. This allows data providers to determine trust from their own perspective and asymmetry for the whole system is reached. For Information Sharing Management we extend the CoinJoin of Bitcoin [8] methodology with rules management and transaction monitoring features as an exemplary illustration in Fig. 5.

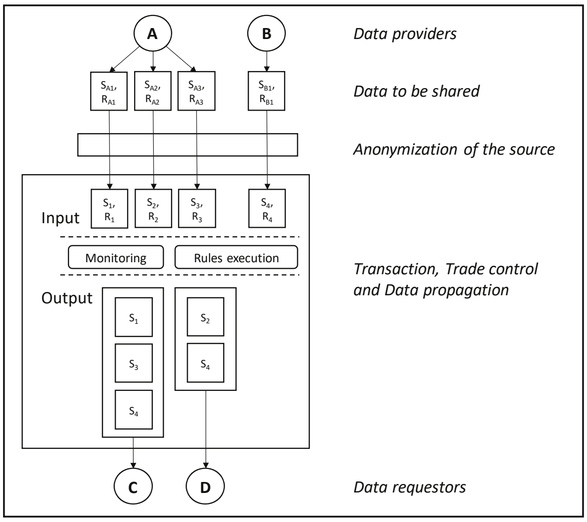


Fig. 5. Enhanced Information Sharing Management.

Before information to be shared are used as input in pool of data, the data origins are anonymized by using virtual front organization layer. The need for anonymization is to hide the exact source of the data. Despite of the anonymization, in the system the traceability still exists in consistent blockchain yet more difficult to solve.

Data pooled and entered in the transaction engine contain the data *S* and the associate rules *R* for the data. Rules can be represented as Smart Contracts in Ethereum [6]. With rules we can manage the information delivery in the system. We can for example exclude recipients from the information, prevent that two different data fragments are delivered together, adjust preconditions of delivery depending on execution of other rules, set a sequence timeline etc.

In algorithm 1 an example is provided to give an idea of contract structure for preventing accumulation of information. Coding notation resembles roughly Solidity language for smart contracts. It is essential to observe the possibility to change implicitly state of the contract, query external contracts and create highly sophisticated conditions that control behavior of the contract through whole lifecycle.

Algorithm 1. Example of contract

```
contract ShareExample
{
    address[] sharelist; // allowed recipients
    address[] deliveredlist; // where information is already delivered
    address[] exclusionlist; // accumulation preventionlist
    data information; // information to be shared, any type of data

    /* Transaction manager can use this function for getting the
    recipients of information. */
    function getSharelist() public
        returns (address[] out) {
        return sharelist();
    }

    /* Function that checks whether certain recipient has received
    information. */
    function isDelivered(address recipient) public
        returns (boolean out) {
        if (deliveredlist.exists(recipient))
            return true;
    }

    /* Function returns actual data for transaction manager. */
    function pullDeliver(address requestor) public
        returns (data out) {
        if (
            requestor in sharelist() &&
            preventAccumulation(requestor) {
                setDelivered(requestor);
                return information;
        }
    }

    /* Function that stores information on shared data. */
    function setDelivered(address recipient) private {
        deliveredlist.push(recipient);
    }

    /* Function that checks if other contract has sent its information to
    same recipient. */
    function preventAccumulation(recipient) private (boolean)
        // referring directly to another contract
        if (recipient in exclusionlist() && !(Y.isDelivered(recipient))
            return true;
    }
}
```

The transaction engine is responsible for consistency blockchain data after sharing the information to recipients. Engine decides and shares the processed information according to the ruleset of the information to the participants of the system.

The transaction engine contains monitoring service for the quality of information, trading balance between participants and liabilities of stakeholders. Trading service enables more sophisticated features such as analysis how participants have met their commitments in the Circle.

We argue, that encouraging participants to share information to the system according to their risk evaluation and enabling functional information trading system with objective commitment monitoring, the threshold for sharing critical and collaborative useful information declines and overall openness increases.

C. Evaluation

To analyze our approach, we evaluate the differences of security risk when sharing critical information. We compare our approach to the traditional VPN based P2P information transfer in Circle of Trust environment. We assume that data encryption strengths are equal in both schemes. We evaluate protection of the source, data leakage, collateral damage of deception and data accumulation.

1) Protection of the source: In VPN based system there is no protection of the source since the transmission is executed between two participants. Even if data is transferred across several nodes, the most likely origins of the data can be derived from the known relations of stakeholders. In our Information Sharing Management, anonymization of the origins ensures the improved privacy of the source. This anonymization phase ensures also privacy of distrust.

2) Data leakage: As we see from Fig. 2 data leakage can be evaluated by the distrust probability (weight) of w_{AC} and trust probability (weight) w_{CD}. The strentgth of our approach is, that we need to evaluate the stakeholder that creates the greatest risk of data leakage for our sensitive information. In VPN based P2P system, we need to consider that any distrust – trust arc combination could occur to our shared data *s*. In our Information Sharing Management we are able to prevent the data to be shared to most distrusted stakeholders. The evaluation of risk approximation can be formulated as in (1). The left side represents the VPN P2P system and right side our new approach.

$$\textstyle\sum^{n}_{x=1} [(1\text{-}w_{Ax})(w_{xy})] > (1\text{-}w_{AC})(w_{CD}). \qquad (1)$$

wherein *x* represents the direct information recipient from provider *A, n* the amount of arcs *Ax* and *y* all the malicious recipients from transmitter *x*. For simplicity we mark *C* as the most distrusted recipient of those that receive information *s* and *D* as the most trusted partner for *C* who is also malicious in relation to *A*. Simplifying the evaluation, we can approximate the greatest risk of data leakage from our most trusted partners. If data provider should care data leakage from several trusted partners (i.e. similar as *C*), the necessity of data provision should be revised, the position of the provider in Circle of Trust ecosystem should be analyzed or the sensitivity of information content should be decreased. In these cases, problem of information sharing is more political than technical. From the evaluation can also be seen, that our approach works even better the larger Circle is.

Recipient that duplicates sensitive information and publishes it against agreements or otherwise violates confidentiality is a challenge to any technical or political system. Naturally our Information Sharing Management can not prevent data duplication outside Circle of Trust if an actor intentionally executes that. However, controlled information sharing provides traceability and with watermarking the information malicious actors can be verified and exposed.

3) Data accumulation (Fig. 3): Dangerous data accumulation occurs in VPN P2P system if there is any transfer path for all data fragments in *S* that transit same stakeholder node. In our Information Sharing Management stakeholders should trust the information received from the system and not to have any other transfer schemes with partners. However, this can happen if there is more distrust between participants of Circle of Trust than to the system information. In this case having all data fragments in *S* accumulated, we need to calculate the distrust probability for all data fragments in *S* recipients. In other words, distrust represents that one stakeholder considers essential to forward received information suspecting that new recipient has not received information for original provider. Data accumulation is formulated as in (2). The left side represents the VPN P2P system and right side our new approach.

$$\textstyle\sum^{n}_{x=1} (w_{Ax1}*\ldots*w_{Axn}) > \Pi^{n}_{x=1} (1\text{-}w_{Ax}). \qquad (2)$$

wherein *n* represents the amount of data fragments *S.* In VPN P2P based system where participants trust each other information is transmitted to each other without consideration. Any information is propagated to the whole circle, which increases the risk of data accumulation. In our approach, the information provider has the possibility to prevent the accumulation. In (2) we see, that if the Circle of Trust is strong, the distrust is little and the risk of accumulation approximates 0. In other words, in our approach strong trust between the Circle participants prevents accumulation of data in contrast to P2P system where strong trust emphasizes it.

4) Collateral damage of deception (Fig. 4): Evaluation of this is special case from the data leakage. We send intentionally false information and hope that there is small trust relation w_{CB}. Protecting *B* from false information requires better information to be sent to *B*. With two different information contents of s from different providers (s_{1CB} and s_{1AB}), *B* evaluates the trustworthiness of the sources w_{BA}, w_{BC} and chooses the information to be trusted. In VPN P2P type system can happen that *B* trusts *C* more and gets false information. The possible damage and reveal of the true origin can impact negatively to the trust relation or trade balance

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

between *A* and *B*. It can also happen that *B* corrects *C*'s information with more trusted information from *A*, which exposes the *A*'s distrust to *C*. In our Information Sharing Management we can specify a rule for s_1 that s_{1AB} excludes s_{1CB}. If *C* transmits s_1 again to the system, *B* needs to evaluate the trustworthiness of the information received and to choose which one to use. Only difference is that origins of the two versions s_1 are anonymous, so the false choice affects *B*'s trust to the system not the trust towards actors *A* or *C*.

VI. Ensuring Openness in Circle of Trust

Openness in information sharing does not remove the need for privacy nor the protection of the information itself. The shared ledger that enables the collaboration and survivability with data replication, creates significant risk of exposure when propagating information across the Circle stakeholders. Minimizing the risk of exposed information, we adopt the latest research results in cryptography conducted by Huang et al. [12, 13, 14, 15]. Huang presents a novel approach to existing public key encryption schemes. For our problem we utilize his commutative encryption algorithm based on ElGamal encryption [13, 16]. With commutative encryption we are able to encrypt information more than once with different public keys. The usefulness in our problem is that the decryption order may vary as needed. This permits us to distribute the same ledger across the Circle of Trust having data sufficiently secured.

The participants have individual keys for encryption of the solution, but as we stated in previous chapters, they are not aware the accuracy or exact trustworthiness of the decrypted information with their own key. The trustworthiness is measured on trust to the whole system. Consequently, everyone has access to every decrypted solution, but only the original provider has the information of correct original data and which key or keys decrypt the best solution.

The approach is illustrated in Fig. 6. $f(A_{key})$ is the encryption on original information provided by A which results the encrypted information *A'*. For each recipient there is a key which decrypts the information with *f'* resulting the recipient specific information (in Fig. 6 [*B*, *C*, *D*]). It is noteworthy that there can also be a key or several keys for parties outside the Circle of Trust as presented in Fig. 6.

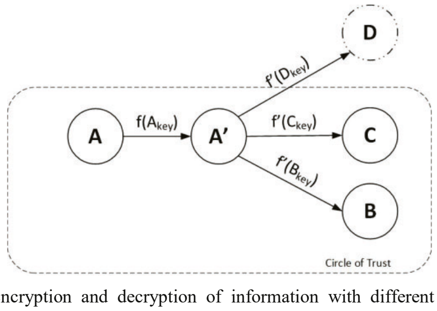


Fig. 6. Encryption and decryption of information with different levels of trust.

In practice this is achieved by encrypting the information so, that the each of the decryption key results a valid outcome. According the Huang encryption $f(A_{key})$ contains all the encryption for each recipient. That is $f(B_{key})$, $f(C_{key})$ and $f(D_{key})$. After keys are delivered to recipients the encrypted information is opened for open access. For example, with information trading between *B* and *C* the differences can be identified, but the accurate reliability cannot be solved.

For a computational issue, the malicious actor has no possibility to decrypt all possible solutions and if they do that, they are not aware which one of the results is the most accurate representation of the encrypted information. Moreover, we argue that even if the malicious actor could collect all the decrypted instances of the information from certain time, it cannot reliably determine what represent the best information.

This solution works best in timely systems where the amount of information is huge. Of course, with infrequent high security information exchange other conventional encryption methods are more useful.

VII. Related Work

In this chapter we will present a brief overview of existing concepts and technologies that are discussed similar problems such as Circle of Trust. We point out the main differentiator of our approach compared to observed one.

First, we observe the knot concept. Circle of Trust can be considered as a virtual community. In sense, it shares the similar context that Gal-Oz et al. have presented in their approach on knots [17]. A knot is defined as a subset of community members identified as having overall strong trust relations among them by directly from trust model of indirectly via transitive trust. Moreover, knots are groups of members that can rely on each other's' recommendations even if they did not rate the same experts. However, the Gal-Oz model emphasizes the symmetry of trust. The knot concept lacks also a mechanism for weighed trust relations, which is a way of quantifying the distrust in Circle of Trust. In our approach, trust might also vary when changing the recipient to a sender and vice versa. It means that the trust between the actors is not symmetrical. This feature descents from the reality, where occasionally recipient has to rely the information provided by the provider, even if there is a suspicion that the information received is not good quality and it might be that the information traded back is best that can be provided by the provider. This kind of asymmetric situation occur when the trading parts had significantly different capabilities of providing and testing the reliability of transmitted data. The technically stronger, more capable and with larger resources can use deception in information sharing and demand full accuracy and highest quality of information in return. In other words, trust varies between the actors in the context of Circle of Trust.

Second, we examine the idea of trust transitivity. Jøsang et al. have published several papers where they discussed features and possibilities of trust transitivity [18]. This research has a potential platform for enhancement where transitivity is limited by threshold when weighed arcs are chained. However, this does not avoid the fact that the first recipient owns the received data after interpretation. Trust transitivity method needs an

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

external broker to control the threshold of the chained arcs. We still find that kind of system vulnerable for exposure of data.

Third we point out that Chen et al. [19] have published a methodology where attributes of trust are delegated subjective trust evaluation. Approach considers the aspects of distrust and include a mechanism to avoid exposure of data regardless of the trust values. However, delegation of attributes and building a global trust map can quantify the accumulation problem and at least increase the knowledge on leaked and possibly accumulated information. Despite of that, it solves the collateral damage of deception problem, because the trust values can prevent sending distrusted information via trusted arcs.

VIII. Conclusions

In this paper we examined information sharing within trusted stakeholders. We defined that environment as the Circle of Trust and limited our discussion to the military context. We stated that the absolute trust never existed and information exchange is necessary in order to build a comprehensive situational awareness. We identified the three primary obstacles to adopting Circle of Trust in a military context and examined possible solutions to overcoming them. We proposed a novel Enhanced Information Sharing Management that utilizes modern blockchain and cryptographic technology. We examined how the smart contracts could improve the overall approach by ensuring the integrity and confidentiality of the shared information. We showed our system enhances the privacy, the data leakage prevention, data accumulation prevention and collateral damage of deception in contrast to traditional VPN P2P system.

We ensured the openness of system by encrypting the information simultaneously with different keys which are delivered one for each recipient. The decryption result can be controlled on encryption phase. We argued that revealing all solutions of decryption are vast, that any malicious actor has no capability to solve in reasonable time which solution has most accurate information in which parameter.

References

[1] Zaerens, K, Enabling the Benefits of Cloud Computing in a Military Context, Proceedings of 2011 IEEE Asia-Pacific Services Computing Conference (APSCC’11).

[2] Grandison, T, Sloman, M, Specifying and analysing trust for internet applications, In Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government, 2002.

[3] Abdul-Rahman, A, Hailes, S, A distributed trust model, In Proceedings of the 1997 New Security Paradigms Workshop, pp.48-60, 1998.

[4] Zhou, Z. X., Xu, H, Wang, S.P, A Novel Weighted Trust Model based on Cloud, Advances in Information Sciences and Service Sciences, 2011.

[5] Handel, M, Intelligence and deception, Journal of Strategic Studies Vol. 5 , Iss. 1,1982.

[6] Buterin, V, A Next Generation Smart Contract & Decentralized Application Platform. Ethereum White Paper. [Online]. Available: http://www.Ethereum.org

[7] Nakamoto, S, Bitcoin: a peer-to-peer electronic cash system, 2008. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[8] Bitcoin Developer Guide. [Online]. Available: http://www.bitcoin.org/

[9] Stajano F., Clayton R. (2011) Cyberdice: Peer-to-Peer Gambling in the Presence of Cheaters. In: Christianson B., Malcolm J.A., Matyas V., Roe M. (eds) Security Protocols XVI. Security Protocols 2008. Lecture Notes in Computer Science, vol 6615. Springer, Berlin, Heidelberg

[10] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 839-858.

[11] Delmolino K., Arnett M., Kosba A., Miller A., Shi E. (2016) Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg

[12] Huang, K, Tso, R, Chen, Y, Rahman, M, Almogren, A and Alamri A, PKE-AET: Public Key Encryption with Authorized Equality Test, The Computer Journal first published online April 20, 2015 doi:10.1093/comjnl/bxv025

[13] Huang, K, Tso, R, A commutative encryption scheme based on ElGamal encryption, In Information Security and Intelligence Control (ISIC), 2012 International Conference on IEEE, 2012, p. 156-159.

[14] Huang, K, Tso, R, Chen, Y. C, Li, W, Sun, H. M, A New Public Key Encryption with Equality Test, In Network and System Security, Springer International Publishing, pp. 550-557.

[15] Huang, K, Chen, Y. C, Tso, R, Semantic Secure Public Key Encryption with Filtered Equality Test - PKE-FET, SECRYPT 2015, p. 327-334.

[16] El Gamal T,. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31(4), 1985, p. 469-472.

[17] Gal-Oz, N, Gudes, E, Hendler, D, A robust and knot-aware trust-based reputation model, Proceedings of the 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM 2008), Trondheim, Norway, pp. 167–182, 2008.

[18] Jøsang, A, Pope, S, Semantic Constraints for Trust Transitivity, Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling-Volume 43. Australian Computer Society, Inc., 2005.

[19] Chen, B, Zeng, G.S, Li, L, Attribute Delegation Authorization Based on Subjective Trust Evaluation, 2008 IFIP International Conference on Network and Parallel Computing, 2008.

978-1-5386-7045-3/18/$31.00 ©2018 IEEE

National Defence University
P.O. Box 7, 00861 HELSINKI

Tel. +358 299 800

www.mpkk.fi

ISBN 978-951-25-3270-4 (pbk.)
ISBN 978-951-25-3271-1 (PDF)
ISSN 2342-9992 (print)
ISSN 2343-0001 (online)

SOTATAIDON YTIMESSÄ

Puolustusvoimat
The Finnish Defence Forces