Jussi Tuovinen & Kimmo Frilander

MILITARIZING RED TEAMING –

AGILE AND SCALABLE PROCESS FOR CYBER RED TEAMING USING ADAPTIVE PLANNING AND EXECUTION FRAMEWORK

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2019

ABSTRACT

Tuovinen, Jussi & Frilander, Kimmo
Militarizing red teaming – Agile and scalable process for cyber red teaming using adaptive planning and execution framework
Jyväskylä, University of Jyväskylä, 2019, 147 pp.
Cyber Security
Supervisor: Professor Martti Lehto

The goal of red teaming is to create better plans, policies, procedures and products in any domain by challenging the current ones. This calls for assessment and critique of status quo. Red teaming is about mitigating future risks and communicating bad news. Red teaming research has focused in adversary emulation and penetration testing practices somewhat disregarding the remediations which are the key in building better security. Cyber threats are evolving and so should cyber red teaming research. Red teaming efforts should be conducted through a comprehensive planning and execution process which considers the complete information security lifecycle starting from planning of intelligence activities and ending to implementing remediations for security to the target organization. Red teaming should be a process that can be understood and adopted by organization and it should be also transparent and traceable. The research problem was to create a comprehensive agile red teaming framework by combining adaptive planning and execution framework in information security context. Design science research methodology was used to solve this challenge. Solid knowledge base and environment description about red teaming and information security was completed in accordance with information systems research framework. Adaptive planning and execution framework, intelligence, targeting and agile methodologies were introduced to support the creation of the framework. Challenges in red teaming were identified by a survey to five cyber security companies. Challenges were remediated by success factors identified from literature and survey. The framework was created, and it underwent two Delphi iterations with subject matter experts. Main result of the study is the comprehensive agile red teaming framework which incorporates the remediations drawn from subject matter experts, military and agile methods. The scope of this study was wide and therefore results can be considered general. The significance of the created framework lies in its novelty and possibilities to adapt it to any red teams' purposes due to general outcome. Framework delivers a good basis for future work.

Keywords: Red teaming, cyber security, information security, risk management, penetration testing, intelligence, targeting, military decision making, mission command, agile.

TIIVISTELMÄ

Tuovinen, Jussi & Frilander, Kimmo
Red teamingin militarisaatio - Ketterä ja skaalautuva kyber red teaming prosessi käyttäen adaptiivista suunnittelu- ja toimeenpanomallia
Jyväskylä, Jyväskylän yliopisto, 2019, 147 pp.
Kyberturvallisuus
Ohjaaja: Professori Martti Lehto

Red teaming toiminnan tavoitteena on luoda parempia suunnitelmia, tuotteita tai käytänteitä millä tahansa toimialalla haastamalla ja kyseenalaistamalla nykyisiä malleja. Toiminnan ytimessä on etenkin tulevaisuuden riskien hallinta ja huonojen uutisten kommunikointi. Nykyinen red teaming tutkimus on painottunut pitkälti teknisiin penetraatiotestauksen käytänteisiin ja uhkatoiminnan mallintamiseen. Ongelmien korjaaminen on jäänyt osin paitsioon, vaikka se on edellytys paremman turvallisuuden rakentamiselle. Kyberuhat kehittyvät jatkuvasti, joten red teaming tutkimuksen tulee myös kehittyä. Red teaming tulisi toteuttaa kokonaisvaltaisena suunnittelu- ja toimeenpanoprosessina, joka huomioi koko turvallisuuden elinkaaren alkaen tiedustelusta ja suunnittelusta päättyen kohdeorganisaation turvallisuuden kehittämiseen. Red teamingin tulisi olla ymmärrettävä, läpinäkyvä ja jäljitettävissä oleva prosessi, jonka organisaatiot voivat omaksua. Tutkimusongelmana oli luoda kokonaisvaltainen ja ketterä red teamingin toimintamalli sotilaallisen adaptiivisen suunnittelun ja toimeenpanon mallin pohjalta kyberturvallisuuden viitekehyksessä. Ongelman ratkaisemiseen käytettiin suunnittelutieteellistä metodologiaa tietojärjestelmätutkimuksen viitekehyksessä. Ensin luotiin perusta ja tutkimusympäristön kuvaus tietoturvasta sekä red teamingistä. Sitten esiteltiin adaptiivinen suunnittelu- ja toimeenpanomalli, tiedustelu ja maalittaminen sekä ketteriä menetelmiä. Tämän jälkeen viidelle kyberturvallisuusyritykselle toteutettiin kyselytutkimus red teaming toiminnan haasteista. Tulokset analysoitiin teemoittelemalla ja haasteisiin vastattiin luomalla red teamingin kokonaisvaltainen toimintamalli tutkimuskirjallisuuden sekä kyselytutkimuksen menestystekijöiden perusteella. Mallia testattiin yritysten asiantuntijoille suunnatulla kaksikierroksisella Delphi kyselyllä. Tutkimuksen tuloksena syntyi kokonaisvaltainen red teamingin toimintalli mihin sisällytettiin asiantuntijoiden kehitysesityksiä sekä sotilaallisten ja ketterien menetelmien parhaita käytänteitä. Tutkimuksen viitekehys oli hyvin laaja ja tämän vuoksi tulokset eivät ole yksityiskohtaisia. Laaditun toimintamallin suurin merkitys on sen uutuusarvossa ja pohjassa jatkokehittämiselle.

Avainsanat: Red teaming, kyberturvallisuus, informaatioturvallisuus, riskienhallinta, penetraatiotestaus, tiedustelu, maalittaminen, suunnitteluprosessi, tilannejohtaminen, ketteryys.

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

"First, they ignore you,

then they laugh at you,

then they fight you,

then you win."

- Mahatma Gandhi-

The goal of red teaming is to create better plans, policies, procedures and products in any domain by challenging the current ones. This calls for assessment and critique of status quo.

Nobody likes a critic and red teaming is about criticism. We wanted to study a constructive method for exposing organization and its functions to critique. Red teaming offers potential for this. Red teaming should be a process that can be understood and adopted by organization and it should be also transparent and traceable. This might be the key in communicating the need for a change in an organization. A little tact and empathy might get more results than a blunt presentation of faults (RTJ, 2016).

This is a theoretical, qualitative study that aims to build understanding of the phenomenon called red teaming in the context of information security management. This is also an empirical study which attempts to enhance the red teaming process by adopting military planning, execution, intelligence and targeting activities to red teaming. Agile methodology in conjunction with military methods and a field survey is utilized in creating a framework for red teaming.

The study consists of nine chapters, first being the introduction, which describes the background, scope, aim, process and initial results of the study. Chapters through two to six are the literature basis which create understanding of the research area and provide remediations for a better red teaming process. Chapter seven describes the process of the literature and empirical study that involved five Finnish cybersecurity companies. Chapter eight presents the results from the study in detail and chapter nine concludes the study with discussion, results and propositions for future work.

We, the researchers are two military officers with more than 40 years of military experience combined from domestic and international operations. This study was conducted as a balanced pair effort. Literature study subjects were divided evenly, which are explained in chapter 7. Commenting and peer reviewing was a constant process during the literature study. Empirical phase was conducted as a pair effort also and both researchers participated to the study evenly. Framework was constructed together, and the workload cannot be separated to individual efforts in the empirical phase.

We would like to thank the participating companies (F-Secure Consulting, JYVSECTEC - Jyväskylä Security Technology, KPMG Oy Ab, Nixu Oyj, and Silverskin Information Security Oy) for their commitment, insight and tolerance towards this study. Also, we would like to express gratitude for the foundations (Finnish Foundation for the Support of Strategic Research, Werner Hacklin foundation and Defence forces support foundation[1]) that supported this cause.

1.1 Background and motivation of the study

US's Director of the national intelligence has defined cyber threats as the first in their list of global threats in its worldwide threat assessment 2018 (Director of the national intelligence, 2018). Nowadays cyber threats are widely studied and recognized as one of the main element in modern criminal landscape by EUROPOL as well (EUROPOL, 2018).

In the field of information security, information security management is the engine which drives the security. Red teaming has been a part of the information security studies since the 1990's and research has continued in implementing it to information security and assurance method for secure design ever since. (Sandia national laboratories, 2000; Wood & Duggan, 2000; Peake, 2003)

Many authors believe that red teaming, which is the practice of attacking systems to better understand how to defend them is a necessity. (Wood & Duggan, 2000; Peake, 2003; Brangetto, Çalişkan & Rõigas, 2015) Red teams allow a company to gain greater understanding of its exposure to vulnerabilities and how critical threats may be assessed. This approach to risk management allows processes to be developed (Ray, Vemuri & Kantubhukta, 2005).

Red teaming is about mitigating future risks and communicating bad news. Baskerville (1991) claims that risk analysis has a profound role as communication technique which can possibly be adapted to red teaming as well. The communication and implementation of various security policies is usually based on awareness programs. Red teaming should involve people from the first

[1] Suomalainen strategisen tutkimuksen ja seurannan tukisäätiö sr, Werner Hacklinin säätiö upseerikoulutuksen edistämiseksi ja Puolustusvoimien tukisäätiö (original names in Finnish).

moment and be based on user participation which enhances the commitment of participants to security (Spears & Barki, 2010).

In 2003 the US department of defence (DOD) declared that red teams are valuable, but underutilized tool. Report also recognized that red teaming is a cultural change which challenges the organization and its norms, and this is needed against adaptive adversaries and guard against complacency. (Defense Science Board, 2003)

There is a growing need for red teaming and penetration testing in commercial, as well as in the military sector because of the growing cyber threats. Several red teaming studies have been published, but we aim to build a red teaming framework that is aligned with the information security lifecycle and could be adopted to the organizations processes to facilitate the cultural change also.

Red teaming efforts should be conducted through a comprehensive planning and execution process which considers the complete information security lifecycle starting from planning of intelligence activities and ending to implementing remediations for security to the target organization and supporting the organization in every step of the process to be effective.

When sending a military unit into a combat it's important to acquire material, organize processes and train the people which makes them a fighting unit. This happens when you push the people to the limit in real combat exercises and they learn about their deficits. These exercises are hard, and you're not meant to win every time. Exercises are the building blocks of a functional unit. Shared experiences create shared understanding and sense of belonging. This is how we see red teaming in the world of cyber security. The defender going through hard exercises in order to build up the fighting capability as a unit. Red teams are to facilitate these exercises by attacking and teaching how to mitigate shortcomings.

1.2 Aim and scope of the study

The number of explananda (number of phenomena) in this study is large covering red teaming, information security, risk management, military decision-making, intelligence, targeting and agility. Therefore, the scope is wide and results will be general. (Siponen & Klaavuniemi, 2019)

Aim is to develop and present a process for comprehensive agile scalable red teaming in the context of information security. This will be achieved by merging several existing explananda into one comprehensive framework. In order to achieve this, we must build a rigid understanding of the phenomenon called red teaming in the context of information security management. After this we will create a red teaming framework which is embedded into information security lifecycle by utilizing military and agile methods.

The battlefield in red teaming as we've learned to see it, is the information systems architecture as described by John Zachman (1987). We are not fighting just in the technical systems or networks but also in the social world of people and physical objects. There is a need to protect the entire architecture, not just the hardware or software. Penetration testing and red teaming are often considered to be technical issues and their focus is on finding weaknesses from the systems, not from organizations or processes. This topic needs to be broadened.

The essentials of protecting or attacking an organization in the field of cyber has been called the "kill chain" with its fundamental white paper; *"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"* by Hutchins, Cloppert & Amin (2011). This kill chain is partially derived from the *"Joint publication 3-60 Joint targeting"* (US Joint Chiefs of Staff, 2013b). The kill chain paper brings forth the importance of structured intelligence and targeting.

We consider that red teaming research lacks the insight of planning and leading of red team campaigns. In military world this is referred as the military decision-making process (Norman, 2015) and the on scene management as mission command (Department of the Army, 2012). These are the processes that will be introduced in this study. We see that agile manifesto's philosophy (Beck & all, 2001) and mission command are very close to each other, but planning is also needed as stated in the manifesto. While the waterfall model by Winston Royce (1970) is popular in the military planning, we need to be more agile. Royce didn't even believe in the basic waterfall but there were several iterative interactions in the original waterfall paper as well.

We are to improve red teaming. Improvement requires a known application context, and the created *artifact* must be an improvement for example in efficiency or quality. (Gregor & Hevner, 2013) There is need to conduct red teaming efforts in an orderly fashion. Red teaming sometimes lacks comprehensiveness and visible structure. This is the main problem to be solved. Properly designed process can be repeated and measured. Measurements provide feedback for development (US Joint Chiefs of Staff, 2017). This research makes the red teaming process more comprehensive by combining long term planning, intelligence, targeting and mission command into one unified process with agile and scalable methods.

Research problem is: How to create a comprehensive, agile red teaming model by combining adaptive planning and execution framework in information security context. The main research questions with their supporting questions are:

1. What are the factors that need to be considered when implementing red teaming into information security management?
   1.1. What is comprehensive red teaming?
   1.2. What are the areas in information security management that can utilize red teaming?
   1.3. How red teaming efforts could be adopted into information security management?
2. How can adaptive planning and execution framework together with agile methodology support the creation of better red teaming process?
   2.1. Which military processes or activities could be considered in red teaming?
   2.2. How agile methodologies can support red teaming?

3. What kind of process is needed for comprehensive scalable red teaming, and how does it make red teaming better?
   3.1. What calls for improvement in current red teaming efforts?
   3.2. How does this study support the development of a better red teaming?

The objective of the study is to create a solution on how to implement many processes into one and create a framework for comprehensive red teaming. We have a strong belief, that in this research we found an interesting balance between scientific rigor and practical knowledge.

1.3 Previous studies and sources

The scope of this study is wide and therefore, the source material has a lot of breadth. Chapters through 2-6 are mostly descriptive and each have their unique genre that is later combined to form the framework.

Red teaming in the information security or cyber-genre has been a keen interest for researchers and commercial companies for over two decades (Sandia national laboratories, 2000). The research is usually technically orientated and there is a well-established research line of the topic (Caron, 2019). Penetration testing is usually used as a synonym for red teaming, but red teaming is a hypernym for penetration testing (NIST, 2013b). Social engineering is usually combined with red teaming efforts (Krombholz, Huber & Weippl, 2015). APT studies supplement the red teaming studies for they present the attacker's view of the topic (Chen, Desmet & Huygens, 2014).

There are several companies that have developed indigenous processes for executing red team – operations, but it's unusual to reveal the processes due to competitive edge of the business (Kraemer, Carayon & Duggan, 2004). A dissertation by James Michael Fleming (2010) examines different types of red teams and their processes in the commercial and defence sector. NATO Cooperative Cyber Defence Centre of Excellence has also published studies of *"Cyber Red Teaming"* (Brangetto et al, 2015) and Granåsen & Andersson (2016) have studied team effectiveness in cyber exercises.

More general red teaming studies are available from topics such as air operations (Malone & Schaupp, 2002; Hansen, 2008), organizational changes (Defense Science Board, 2003; Sandoz, 2001), intelligence (Mitchell, 2006), law enforcement (Meeham, 2007), decision-making and politics (Averch & Lavin, 1964; Goldhamer & Speier, 1959) to international relations (Guetzkow, 1959) up to disarmament negotiations (Davis, 1962) and even to mining industry (Lane, 2008). Micah Zenko's book *"Red team: how to succeed by thinking like the enemy"* has also been a valuable generic source (Zenko, 2015).

Red teaming manuals have been published by various organizations like University of Foreign Military and Cultural Studies (2015) in the US, Development Concepts and Doctrine Centre (2013) from UK, Department of defence (2017) from Australia and NATO (2017). These will be utilized to explain the versatility and adaptation of red teaming.

The context of red teaming in this study is information security. To understand the environment, various definitions of information systems and architecture were studied. (DeLone & McLean, 1992; Boell & Cecez-Kecmanovic, 2015; Zachman, 1987). Information security policy process model studies (Susanto, Almunawar & Tuan, 2011; Siponen & Willison, 2009) are the building blocks for information security management along with standards like ISO 27000 series (ISO, 2018) and NIST SP 800-53 (2013, 2013b) which were examined. A more general information security policy process model by Knapp, Morris, Marshall & Byrd (2009) was used for refinement of the red teaming framework.

Risk analysis and management were presented from the views of Baskerville (1991) (1993) and the Risk Management Standard (The Institute of Risk Management, 2002). User participation in risk management (Spears & Barki, 2010) and difficulties to implement security solutions (Siponen & Baskerville, 2018) were addressed a well.

The main sources for military processes came from US publications since they are publicly available and very detailed. Joint publications (JP) are documents signed by the joint chief of staff. JPs are guiding documents for services that create more detailed Field Manuals (FM) and according to field manuals various guiding documents are also produced. The most utilized manuals were the JP 5-0 Joint planning (US Joint Chiefs of Staff, 2017), FM 5-0 The operations process (Department of the army, 2010b), JP 3-0 Joint Operations (US Joint Chiefs of Staff, 2018), ADRP6-0 Mission command (Department of the Army, 2012), JP 3-60 Joint targeting (US Joint Chiefs of Staff, 2013b), JP 2-0 Joint intelligence (US Joint Chiefs of Staff, 2013) and FM 2-0 Intelligence (Department of the army, 2010)

Intelligence studies (Gill & Phythian, 2016) and system analytical approach (Von Bertalanffy, 1972) to targeting were presented as well as critique and development issues for intelligence and military decision-making. (Frini & Boury-Brisset, 2011; Gotztepe & Kahraman, 2015; Runyon, 2004; Marr, 2001)

The main sources for agile methods came from academic studies and practical white papers. Agile methodology and its adaptation have been studied mostly in the software business where the origins of modern agile development are derived (Abrahamsson, Warsta, Siponen & Ronkainen, 2003). Agile manifesto states the values and principles of agile (Beck & all, 2001). Scrum and Kanban were studied from the perspectives of their founders, Sutherland & Schwaber (2011) and Mr. Taiichi Ohno (Sugimori, Kusunoki, Cho & Uchikawa, 1977) as well as their interactivity by Kniberg & Skarin (2010).

Scaled agile for large organizations has immersed with multiple studies like the dissertation by Maarit Laanti (2012). Agile development is followed annually by a worldwide state of the agile study which is referred (VersionOne Inc., 2018) Most used scaled framework (SAFe®), was created on the ideas of Dean Leffingwell (2007) whose work is used as an example of agile enterprise model. Implementing agile is difficult and there is a model in between Winston Royce's waterfall (1970) and agile known as the "Water-Scrum-Fall" which is introduced as a more business reality oriented model (West, 2011; Schlauderer, Overhage & Fehrenbach, 2015).

1.4 Research methodology and initial results

This is a qualitative study where design science research methodology (DSRM) (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007) was used to create the artifact, which is the comprehensive agile red teaming framework (CART) in the context of information systems research framework (ISRF) (Hevner, March, Park, & Ram, 2004). Information systems research is a typical research setting for design science. Design science was suitable for this research, because it aims to create a solution for a problem and new knowledge is created during the process. The design science research methodology process consists of six phases (Peffers et al., 2007):

1. Identifying the problem and motivation
2. Defining objectives of a solution
3. Design and development of the construct
4. Demonstration about using the construct to solve a problem
5. Evaluation of the construct
6. Communication of results

In the first phase the research objectives for the solution and methodology were defined from literature and personal experiences from the field of information and cybersecurity. Second phase included familirization to the research domain through literature study. Phases one and two formed the fundamental knowledge base and description of the environment as described by IS research framework (Hevner et al., 2004). Adaptation of the IS framework to DSR process in the context of this study is depicted in the figure 1. below.

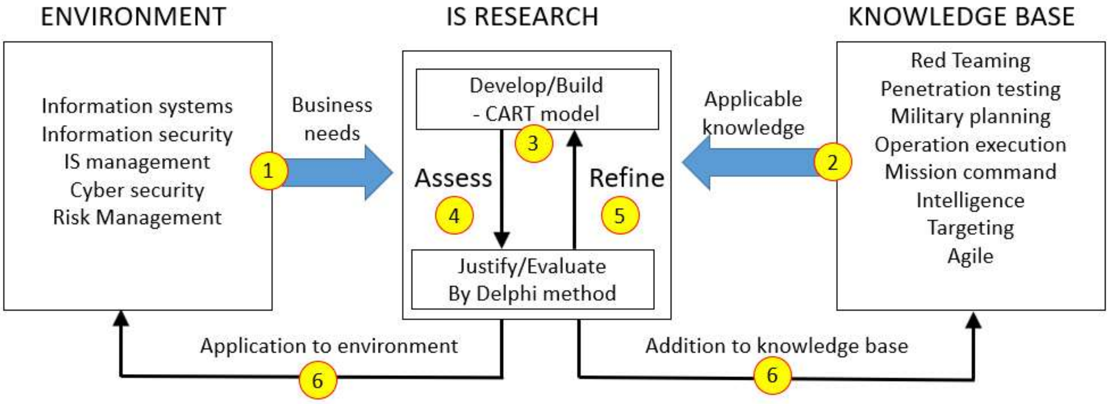


FIGURE 1 Application of ISRF Framework to DSRM.

In the third phase a survey was made to five companies about shortcomings of red teaming and different processes from the knowledge base were depicted in accordance to the environment. This led to the creation of the new construct. This is the Develop/Build block of IS Research framework (Hevner et al., 2004). Phases one to three were completed concurrently.

Fourth and fifth phase were demonstration and evaluation of model in Delphi-questionnaires with two iterations. Interaction between SME's was controlled to avoid confrontation. This leads to better reliability and judgement, because certain level of anonymity can be ensured concerning the individual responses. SME's were selected from five cyber security companies. Delphi-method was also utilized to test construct validity. (Okoli & Pawlowski, 2004). Sixth phase is the publication of this thesis and additional articles based on this study.

Term *"artifact"* is used regularly in DSR. Typical artifact in the field of information systems is a process which CART framework resembles. Position of this study in the DSR knowledge contribution framework is improvement of information security and known red teaming processes and exaptation to merge multiple military and agile disciplines to create a more structured and comprehensive process. (Gregor & Hevner, 2013)

This study has added a piece to the complicated nature of information security research puzzle and shown how red teaming fits to the research domain. The interlinkage of red teaming and information security management is also depicted. Red teaming research scope should be broadened in the information security research. Red teaming research has focused in adversary emulation and penetration testing practices disregarding the remediations which are the key in building better security. The planning and providing of security should be an integral part of red teaming. Risk management includes the future risks that cannot be derived from the past which requires an external attacker to simulate future risks. APT research supports red teaming activities in creating threat matrixes for attack simulation that can also simulate future risks.

The practical implications include introduction of the adaptive planning and execution frameworks as a problem-solving and managing technique for red team operations combined with agile practices and methods. The realization of similarities between agile methods and practices with military planning and execution was an interesting notion to be studied further.

The main result produced by this study is the comprehensive red teaming framework which underwent a thorough scrutiny from five cybersecurity companies. Constructed framework is an improvement for red teaming activities delivering structured processes to manage operations. Red teaming is a complete tool set in creating better plans, policies and procedures in any domain by questioning the current ones.

The scope of this study was wide and therefore results can be considered general. The significance of the created framework lies in its novelty and possibilities to adapt it to any red teams' purposes due to general outcome.

2 RED TEAMING

"What would I eliminate if I had a magic wand?

Overconfidence"

- *Daniel Kahneman -*

Red teaming is a topic that raises eyebrows. People tend to like the status quo and red teaming is about disturbing the status quo. Red teaming is about criticism and nobody usually likes critique especially if it's directed towards you. This is the misconception that frequently is adhered to red teaming, critique towards someone or something. If communicated properly, the critique will be a promotion of a certain goal not focusing on the shortcomings. This is the ultimate trick a red teamer can pull.

This is a descriptive chapter which builds to the knowledge base section in information systems research framework (Hevner et al., 2004) from the part of red teaming. In the design science research methodology process this chapter comprises a part of phase 2; defining objectives of a solution and enables phase 3; design and development of the construct (Peffers et al., 2007). In this chapter red teaming is introduced from several perspectives and fields of life to make the concept and philosophy of red teaming comprehensible.

Humans do not think logically especially in groups. Various biases and group pressure prevent people from stating their opinions or seeing situations rightfully (Tversky & Kahneman, 1974). Humans are unreliable decisionmakers because their judgement is affected by moods, internal and external issues and even the weather. This variability of judgement is referred as noise (Kahneman, Rosenfield, Gandhi & Blaser, 2016) Bias creates wrong decisions and noise inconsistent decisions as elaborated in figure below. Red teaming helps to overcome biases and mitigate group thinking and reduce noise with adaptation of procedures that promote consistency and impartiality.

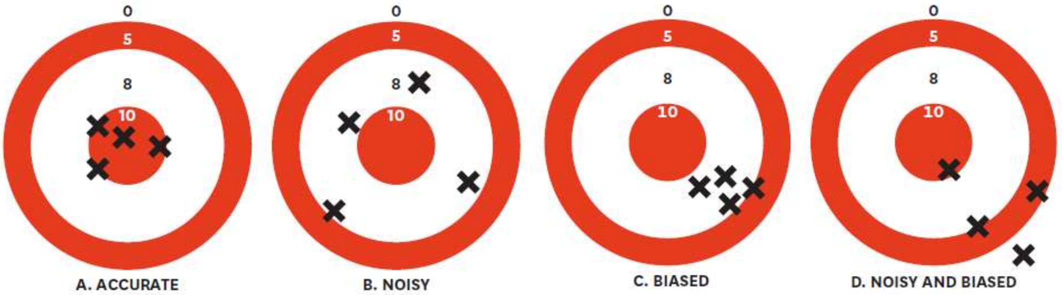


FIGURE 2 How Noise and Bias affect accuracy (Kahneman et al., 2016)

2.1 Red teaming defined

There are various definitions of red teaming. Overarching taxonomy has been attempted to define researchers like Mateski (2004) and Fleming (2010) but none exists. Military, politics, finance, academia and various other domains have a different approach to the issue. This makes the possibility of coherent taxonomy a challenge.

Some tend to think that red teaming is about adversary simulation and attacking one's organization and systems to enhance security like Chris Peake, in his paper for SANS year 2003: "Red Teaming: The Art of Ethical Hacking"

> Red Teaming is a process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to system/network/data access. This process is also called "ethical hacking" since its ultimate purpose is to enhance security. Ethical hacking is an "art" in the sense that the "artist" must possess the skills and knowledge of a potential attacker (to imitate an attack) and the resources with which to mitigate the vulnerabilities used by attackers (Peake, 2003, pp. 1-2)

Others might think red teaming as a tool to test your plans and find weaknesses through discussions or wargames. This is the case in several military documents like the US "Joint publication 2-0, Joint intelligence".

> Red Teams and Red Cells. Command red teams are organizational elements comprised of trained, educated, and practiced experts that provide the JFC an independent capability to conduct critical reviews and analysis, explore plans and operations, and analyze adversary capabilities from an alternative perspective. Red teams assist joint operation planning by validating assumptions about the adversary, as well as participating in the wargaming of friendly and adversary COAs. In contrast, J-2 red cells perform threat emulation (US Joint Chiefs of Staff, 2013, p. I28).

Financial organizations see red teaming as running stress tests against their organizations and processes. The companies also might see red teaming as a tool to manage corporate risks, like Financial times states below.

> A red team is an inside group that explicitly challenges a company's strategy, products, and preconceived notions. It frames a problem from the perspective of an adversary or sceptic, to find gaps in plans, and to avoid blunders. Red teams are one way to manage the biggest corporate risk of all: thoughtlessness (Financial Times, 2019, p. 1).

Red teaming is all of these and more. In the next three quotes from United Kingdom, United states and Australia a more comprehensive view is presented. First quote is from the UKs Development, concepts and doctrine centre (DCDC).

> Red teaming is the independent application of a range of structured, creative and critical thinking techniques to assist the end user make a better-informed decision or produce a more robust product (Development Concepts and Doctrine Centre, 2013, p. ANNEX A).

DCDC is United Kingdom's Ministry of Defence's (MOD's) think tank which produces doctrines and concepts for the British armed forces. DCDC helps to inform defence strategy, capability development, operations and provides the foundation for joint education. DCDC also provides red teaming analysis (Development, Concepts and Doctrine Centre, 2019). Second quote comes from the US army's University of foreign military and cultural studies (UFMCS).

> Red teaming is a function that provides commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment (OE) and from the perspectives of partners, adversaries and others (University of Foreign Military and Cultural Studies, 2015, p. 2)

UFMCS (i.e., Red Team University) is a US Army's institution founded in year 2004. UFMCS offers courses for the armed forces and civilians which include decision support, applied critical thinking, fostering cultural empathy, self-awareness and reflection, groupthink mitigation, red team tools, and liberating structures, all aimed at decision support. The UFMCS mission is to develop Army leaders who are agile and adaptive critical thinkers, and who operate effectively in complex and rapidly changing operational environments (University of Foreign Military and Cultural Studies, 2019). UFMCS works in close co-operation with the US training and doctrine commands intelligence branch (TRADOC-G2) (TRADOC, 2019). Third quote is also from a manual, this time from Australia's department of defence, science and technology group.

> Red teaming – (in its broadest form) - is a methodology that enables organisations to view their own vulnerabilities and challenge assumptions. It involves any activity—implicit or explicit—in which one actor attempts to understand, challenge, or test a system, plan, or perspective through the eyes of an adversary or competitor. The expected outcome of red teaming is the development of more robust plans, policies and procedures in any domain (Department of defence, Australia, 2017, pp. 10-11)

This last quote is from Australian DOD document; "A Simple Handbook for Non-Traditional Red Teaming" from year 2017. This document has taken references from the UK and US red team manuals and several research papers on human cognition and psychology as well as strategic studies and management. This paper is good combination of scientific rigor and practical relevance. The definition encapsulates well the comprehensive nature of red teaming efforts and its outcome; The goal of red teaming is to create better plans, policies, procedures and products in any domain by challenging the current ones.

2.2 Origins of red teaming

Red teaming as an art did not just appear out of nowhere. Red teaming is not an invention, it's a way of living and thinking. The earliest notions of organized red teaming can be traced all the way to ancient Greece and to the Plato's academy (established 428 BC) The nature of academy's teaching was dialectical. (Pappas, 1995) Dialectics is a discourse between people holding different points of view about a subject but wishing to establish the truth through reasoned arguments. Dialectics is the consistent sense of non-identity. It does not begin by taking a standpoint. Dialectic resembles debate, but the concept excludes subjective elements such as emotional appeal and the modern pejorative sense of rhetoric. Dialectics work with the basic, thesis, antithesis, synthesis principle. (Adorno, 1973)

Academic scepticism was favoured in Platonic academy during its existence and some say the academy went sceptic all the way (Algra, Barnes, Mansfeld, & Schofield, 1999). Scepticism is about questioning beliefs and dismissing various biases. The aim is that one ought to examine one's beliefs and abandon those that one finds to be false. Unofficially Plato's academy also worked as a think tank to Hellenic governments and was a red team for the politicians of the age (Pappas, 1995).

Plato's academy was not the only school of thinking during Hellenic times. Stoicism also had ideas resembling modern red teaming. In stoicism there is a term which is also a type of meditation practice; "praemeditatioa malorum" which roughly translates to; premeditation of adversity (Robertson, 2010). During this exercise person will imagine himself ending up in various catastrophes or perils. Then one should maintain objectivity and consider how a perfect stoic sage would respond to these events. This thinking is not considered to be an exercise of pessimism, but of reason. In more modern days this same mentality applies to the famous Murphy's law, "anything that can go wrong, will" which is also referred in red teamers way of thinking (Malone & Schaupp, 2002).

2.2.1 Devil's Advocate as the first official red teamer

The term "Advocatus Diaboli" (i.e. Devil's advocate) is frequently used in conversations – someone being the dissident thinker. Devil's advocate is nowadays one technique method of red teaming (Development Concepts and Doctrine Centre, 2013) among others, but it holds an important status in developing red teaming (Zenko, 2015). In various religions there is possibility that a person can be promoted to be a saint. In catholic church this process has developed during hundreds of years with correspondence to secular justice. The pope can first beatify and then canonize a person to become a saint. The catholic church had an office of promoter of the faith, which is commonly known with a moniker, devil's advocate. (Gray, 2015) As the name suggests, he serves a contrarian role, presenting reasons against a cause of canonization.

The canonization process in catholic church in the beginning was quite simple. To simplify the process; Candidate needs to be a good Christian or produce miracles by opinion of others (vox populi) or die of martyrdom. After a popular opinion an initiative is made to a local bishop and church will appoint a small commission to investigate the case. If no foul play is noted, the candidate is first beatified and later canonized. Everybody can see that there might be some possibilities of misconduct here. (Zenko, 2015) The need for devil's advocacy was raised in catholic church during thirteenth century by pope Innocent III for he saw that too many saints were marching in. Innocent III was a keen promoter of canonical and secular justice (Gray, 2015).

Innocent III noted flaws in the canonical papal court system and he started a process which led to a new kind of justice: the inquisitorial system. The inquisitorial system came into wide use since experience proved that it was much more effective in punishing crimes and achieving justice than the previous systems. Although in the earliest inquisitorial courts there were only three roles; the accuser (actor), the accused (reus), and the judge (iudex). The system started to develop, and the role of the accuser evolved, not being just an accuser, but a promoter of the faith, promotor fiscalis - the one who seeks the truth. The office of promoter of the faith was establish in Rome and by the height of the middle ages, the papal court had evolved into a highly developed structure to provide advice and assistance to the Roman Pontiff in matters that called for his judgment. (Gray, 2015)

Pope Gregory IX issued a decree of papal inquisition and added the canonization process to the duties of office of promotor fiscalis in year 1234. The causes of canonization were investigated through a rigorous system that included two specific inquiries (inquisitiones), within a larger twelve step process. Advocate's office was set to be a knowledgeable insider who was empowered to step outside of the Church and objectively assess each candidate for sainthood (Gray, 2015). Getting your sainthood started to be hard.

Now it starts to be clear why the promoter of faith has such a diabolical name. Even though his duty was not to prosecute the candidate for sainthood, but to promote the faith and see that no unworthy passes the process. The office of devil's advocate has a lot of red blood on its hands.

At this point one needs to see the results of office of the devil's advocate. Numbers in the saints nominated before the office of devil's advocate and after, vary immensely. The office was terminated in 1983 by Pope John Paul II and the canonization process was downgraded to a three-step process again. Result was that John Paul II canonized 482 saints which is more than his predecessors in last 600 years together (The Holy See, 2019). 1277 people were also beatified to the waiting list for step two of canonization. Now there are more than 10000 saints in the catholic church (Lipka & Townsend, 2014). The termination of red teaming from the canonization process had obvious consequences.

The office of devil's advocate was important to development of red teaming for a few reasons;

1. The function was supported and empowered by the management.
2. The process was formalized and enforced.
3. The office was outside of the organization's but still inside and aware.
4. The employees of the office were sceptics.
5. The office red teamed enough, but not too much.

These five reasons are almost the same as Micah Zenko emphasizes in his study about red teaming (Zenko, 2015). The first rule in implementing a red teaming function to an organization is the support from the management, the buy-in effect which is the most important.

2.3 Red teaming in military

War, combat and rivalry are as old as humanity. War is also the ultimate test for plans. Therefore, militaries throughout the ages have made plans for fighting. These plans have also been placed under thorough scrutiny by the commanders and their staffs. In order to develop the thinking of the commanders and officers, militaries have developed wargaming to test plans.

2.3.1 Wargames surfacing in Europe

The earliest documented wargames in western world come from Prussian military and the history of professional war gaming is dated approximately to 18th and 19th century (Wintjes, 2015; Zenko, 2015; Ciancarini & Gasparro, 2012).

This naturally is not the earliest era when wargames have been played, but the documentation of the organizing of games can be found from this era. The most renowned form of gaming is probably the Prussian Kriegsspiel which was developed by Georg Leopold von Reisswitz and then developed and introduced to King Friedrich Wilhelm III by his son Baron Georg Heinrich von Reisswitz (Taws, 2017). Earlier documents of wargames and previous development steps for Kriegsspiel are documented, but the causality of development is not proven, so Reisswitz is considered to be the inventor (Wintjes, 2015). Kriegsspiel was in fact a big table with several boxes and the game was distributed to Prussian army units and military academies in 1824. Officers also played the game during their free time in officers mess. (Wintjes, 2015)

The Prussian Kriegsspiel was not the first wargame to be developed, but it gained more momentum than its predecessors. One reason for this was its professional layout as a gaming table. This made the game credible. Earlier on in year 1664 Christoph Weickmann, an Ulm merchant produced a card game of tactics called "Newerfundenes grosses Königsspiel". A tradition of card games for war simulations was also formed elsewhere in Europe and a Frenchman Gilles de La Boissière's invented a game in year 1698 named "Jeu de la guerre" which was very popular far into 18th century. (Wintjes, 2015) Yet already over two centuries before the Kriegsspiel a Hessian nobleman Reinhard Graf zu Solms published a book in year 1559 which is nearly exclusively devoted to a game of cards, simply called the "Kartenspiel". The game was intended to be used both for preparing young noblemen for military decision-making and for supporting command and control in the field. It thus may well have been the earliest professional war game of the post-medieval period. (Wintjes, 2015) The wargaming culture has developed since and now it's a regular part of a planning process in military doctrines (US Joint Chiefs of Staff, 2017).

The learnings from Prussia war games were adopted widely in the western armies. One of the most interested developers came from the United states. In 1884 the Naval war college incorporated "American Kriegsspiel" to their curriculum (Zenko, 2015). The idea of wargaming was supported and developed. Elaborate rules for troop movements and casualties were calculated. Initially calculations were theoretical, but empirical data from real battles started to redefine the formulas in time. Games that follow this evolution were known as "Rigid Kriegspiel". This method was protested by many officers due to its difficulty to use which led to the development of more relaxed versions of the Kriegspiel which were easier to use. The wargaming culture in the United states developed towards "Free Kriegspiel" and was widely played until World War II. In Free Kriegspiel there are no calculation formulas, but referees who make judgement calls based on their experience (Davis, 1962). This of course is not a very scientifical way of resolving situations, but it's fast and depending on the referee can also be more accurate than calculated results. The Rigid Kriegspiel culture has made a comeback when computers developed. Nowadays strategic computer games and simulations fall under this term also and they are used to support various war games since the 1980's (Davis, 1984).

2.3.2 Red teams developing from red cells

The military culture is not always open to differing opinions and people who tend to question a plan which was drafted together, can be seen as a nuisance to the team. Sometimes an officer that views the world from the opponent's perspective can also been seen sympathetic towards the enemy (Davis, 1963). Also, officers are sometimes afraid to express their opinions to their seniors for various reasons. This topic of minority against majority is well recognized in psychology (Asch, 1956) and in cognitive dynamics (Osgood, 1960) as the problem of minority. Problem of minority communication is not military's by privilege. Everybody has most likely faced the same issue in their normal lives. The problem is not that a person will get upset because the correct opinion is not heard. Problem is that the leadership does not get the correct information due to fear or some other reason. Good anecdote to sum this up is from four-star general Martin Dempsey;

> When I pinned on my fourth star in December of '08, I had a four-star coming through the receiving line to congratulate me and he leaned over and he whispered, "You realize that, from this point forward, no one will ever tell you the truth again."
>
> —General Martin Dempsey, Chairman of the Joint Chiefs of Staff, 2011- (Zenko, 2015, p. 25)

These are the reasons why red teaming needs to merge into the organizations and their processes to make it an acceptable function such as intelligence. Red teaming is not intelligence, red teams also question the intelligence and support their processes (US Joint Chiefs of Staff, 2013).

Red teaming as a word emerged from the military exercises during the cold war when US troops were considered as blue force and Soviet troops were the red force. This gave birth to the red cell. (Zenko, 2015) Red cell is a threat emulation unit which acts like the enemy in exercises (US Joint Chiefs of Staff, 2013). Red cell was the earlier evolution step for a red team.

United States aircraft kill ratios between Korea (10:1) and Vietnam (2.5:1) were in deep dive. The air force needed to improve their fighting capabilities and two reports were released which stated that the training needs to be more realistic and be opted to face the enemy. This created the Red Flag (formerly known as Cope Thunder) exercise concept in 1975. (Hansen, 2008) Today the Red Flag is arguably the most advanced air operations exercise in the world with participants from 29 countries (USAF, 2012a). In this exercise a red cell acts as aggressors, including fighter, space, information operations and air defense units. The aggressors are specially trained to replicate the tactics and techniques of potential adversaries and provide a scalable threat presentation the opponent and uses adversary tactics, technics and procedures (TTP). (USAF, 2012b)

Currently the red cell activity of the United States Airforce is unmatched by any nation which is one reason why they have had air dominance in every war. The aggressor activities are housed in the 57th wing which commands the USAF Weapons School, several aggressor squadrons, air defence and space units (USAF, 2017). The link between intelligence and red cell is that intelligence briefs the 57th wing red cell about enemy TTPs in order the red cell can train those TTPs and use them in the exercise (Malone & Schaupp, 2002).

Red cells are usually supported by the intelligence branch because they have the latest information on the enemy TTPs. Sometimes the job of a red cell in tabletop games is given to an intelligence unit if a proper red cell is not in the organization (Malone & Schaupp, 2002). This makes the job of an intelligence officer hard because then he must act as the enemy and still do his job as the intel officer. This is not the best approach. That is why United states have produced a Joint Doctrine Note 1-16 Command Red Team (JDN) in 2016 which gives guidance on using red teams in military organizations. JDN 1-16 also defines the difference between a red cell and a red team. (US Joint Chiefs of Staff, 2016)

> A red cell plays the role of an adversary, the red force, through emulation in wargaming. Red cells roleplay not just mindset and decisions, but also capabilities, force structure, doctrine, and rules of engagement. Red teams assist joint operation planning by validating assumptions about the adversary, as well as participating in the wargaming of friendly and adversary courses of action, but not as the role of the red force. Red teams use a technique called adversary emulation to role play the mindset and decisions of an adversary, but they do not role play the full range of adversary actions as a red cell does. (US Joint Chiefs of Staff, 2016, p. I6)

To simplify this quote 1. Red cell roleplays the enemy and acts like the enemy 2. Red team assists the friendly operations staff and can also do adversary emulation to support the decision-making. In order these two to function, there needs to be an organization to handle their role.

Red teaming as such did not surface forcefully in the military before 2003. There were naturally various red teams and red cells in different staffs permanently or on ad hoc basis (Defense Science Board, 2003). Red teaming was still at early evolution phase and background studies were made with government funding (Sandoz, 2001).

2.3.3 US armed services turn towards red teaming

In 2003 the US department of defence established a task force (Defense Science Board, 2003) to investigate the possibilities of advancing red teaming in the department of defense. The report investigated current red team activities such as;

1. US navy's SSBN Security Program which was established in the early 1970s to identify the potential vulnerabilities that the Soviet Union might exploit to put US SSBN at risk. The program is still running and very successful and it has close connection to intelligence community.
2. Missile Defense Agency-Red Teaming Experience which has been running for twenty years. The purpose of this program is to handle risk management with the development and deployment of the missile defense system.
3. Air Force Red Team Program which provides assessments of concepts and technology.
4. The US Army Red Franchise Organization: Established in 1999 and is responsible for defining the operational environment in next two decades. The operational environment is the intellectual foundation for transforming the Army from a threat-based force to the capabilities based objective force.
5. US Joint Forces Command (JFCOM) Red Teams: This program has been using red team for joint concept development and experimentation.
6. Office of the secretary of defence’s Defense Adaptive Red Team (DART) Activity: Established in 2001 and its mission is to support the development of new joint operational concepts by providing red teaming for JFCOM, the combatant commands, Advanced Concept Technology Demonstration (ACTD) and joint Staff.

Conclusions of the report were that red teams are valuable, but underutilized tool. Report also stated that red teaming activities are increasing in the DOD and in the IC as well due to need to understand the enemy. Report also recognized that red teaming is not a bag of tricks but a cultural change which challenges the organization and its norms. This is needed if the US armed services are intended to transform into effective force against adaptive adversaries and guard the DOD against complacency. Report recommends the establishment of red teams throughout the organization in small steps and the establishment of a formal and professional military education on red teaming. (Defense Science Board, 2003)

Secretary of Defence, Donald Rumsfeld felt that US Army needed to be transformed viewing the difficulties in Operation Iraqi Freedom and Operation Enduring Freedom. In the aftermath of the second war on Iraq. Army high command recognized several problems during the wars, one of them army command being ignorant to own intelligence and warnings. Army chief intel Lieutenant General Keith Alexander formed several small red team decision-support groups and found it to be useful for battle staff. This was one of the successful red teaming activities in war and later aided in establishment of the red team university. (Zenko, 2015)

Army needed to be more agile and several changes were issued in coming years, one of them was the nomination of new army's chief of staff. Rumsfeld wanted a retired four-star general Peter Schoomaker to be the chief of staff of the army. Schoomaker career was not from the army, he was a special forces man. Schoomaker was the founding member of the 1st special forces operational detachment Delta (Delta Force) and his last post was the commander of US special operations command (SOCOM) which oversees all armed services special operations. (Zenko, 2015)

Schoomaker was an out-of-the-box-thinker and he thought that army is facing "regimentation and institutionalization of mediocrity" which can be also interpreted as complacency. He thought that army hadn't evolved much since Vietnam and same things are still taught as 30 years ago. Schoomaker took the post as the 35th chief of staff in the US Army, his strategic guidance was simple *"shake up the army"*. Schoomaker started to establish red teaming efforts first in the army and later to other armed services. Important part of the transformation was the education system and red team university was found with the name; University of Foreign Military and Cultural Studies. (Zenko, 2015).

The University of Foreign Military and Cultural Studies held its first red teaming course in 2004 for 18 students from army, marines and navy. The number of students has gone up gradually and in 2014 the university was training more than 800 students annually in its courses from all over the services and intelligence community. (Zenko, 2015) The tuition material is always developing and already the version 7.0 of their Red Team handbook, known as "the applied critical thinking handbook" (University of Foreign Military and Cultural Studies, 2015) which is a product created together with the intelligence department of the US Army training and doctrine command (TRADOC, 2019) is published. This is a military guidebook of thinking like the enemy.

The US armed services and intelligence community have now for 15 years practiced "professional" red teaming and now it is also a doctrinal issue. Red teaming is an effective function and it is now part of the joint planning process according to US doctrine, Joint Publication 5.0 – Joint Planning (US Joint Chiefs of Staff, 2017).

> The red team should be fully integrated into the planning process and assist in the initial development and revision of JPP products. When the red team is unable to support all aspects of a specific planning effort, the commander or J-5 should establish priorities for red team support. In most cases, the red team will have the greatest impact on planning during JPP Step 2 (Mission Analysis), and Step 4 (COA Analysis and Wargaming). (US Joint Chiefs of Staff, 2017, p. K3)

To guide commanders and staffs, the Joint Doctrine Note 1-16 Command Red Team (JDN) was published in 2016 which is the non-authorative guidance on using red teams in military organizations according to Joint planning doctrine (US Joint Chiefs of Staff, 2016). Nowadays other advanced nations like UK (Development Concepts and Doctrine Centre, 2013) and Australia (Department of defence, Australia, 2017) have produced red teaming manuals for their militaries and are practicing red teaming in their activities. NATO has recognized the importance of alternative analysis and produced a guidebook for the purpose as well (NATO, 2017).

2.4 Towards comprehensive red teaming in the security sector

Red teaming started to gain momentum in procurement and strategic level decision-making in the United States department of defense and military in the early 1960s with support of think tanks like RAND (Averch & Lavin, 1964). Various simulation and gaming studies can be found from the field of politics (Goldhamer & Speier, 1959) to international relations (Guetzkow, 1959) up to disarmament negotiations (Davis, 1962). Red teaming started to emerge also in law enforcement (Meeham, 2007) and intelligence communities (Mitchell, 2006) as well as aviation security (The President's Commission on Aviation Security and Terrorism, 1990) and even in mining industry (Lane, 2008).

2.4.1 Strategic negotiations with red teaming

Journal of conflict resolution in 1963 published an article by Robert Davis (1963). Davis forms a model of blue team and a red team in arms treaty provisions. The article also contemplates the psychological factors of group thinking and overcoming the biases of planning. The article is based on Davis's presentation paper at the meetings of the American Psychological Association in September 1962 (Davis, 1962) which he produced while working as government contractor. The full paper was published later by Armed Services Technical Information Agency. The report (Davis, 1962) suggests that there are at least five techniques to study social, political, and economic problems as those of war and peace. These are; Individual and group planning, scenarios, crisis games, symbolic simulations and environmental simulations.

Davis (1962) claims that the Kriegspiel techniques are a part of the group planning effort. The Free Kriegspiel has led to the development of scenarios and crisis games. Rigid Kriegspiel has led to environmental and symbolic simulations. Scenarios and crisis games should be aids, rather than methods that support the simulations.

Scenarios are aids to define the gaming world. They define the conditions and settings for a game and help to visualize the game for players. Also writing a scenario can be a useful technique itself. Scenario usually describes hypothetical situations and series of events which the players must resolve. (Davis, 1962)

Crisis games are role plays with two or more entities. Players are given roles as a person, nation, organization or whatever entity which they need to act. Therefore, specialists are needed for the roles. Then game situation is given, and players start to play their avatar. Out of these confrontations frequently come new ideas and hypotheses which may later be examined by individual or group analysis. (Davis, 1962)

Symbolic simulations are logical or mathematical in nature and they create models with interactions and causalities. Models are then examined in time perspective. The use of strictly symbolic simulations is mechanical in nature and sometimes the greatest learning experience comes from the creation of the criteria and the model, not from the results. Environmental simulations include the human factors. Humans are added to the simulation to make decisions which affect the results over time. (Davis, 1962)

Figure below depicts the relationships of these techniques and the game model that Davis created from these techniques in order to build a disarmament proposal game.

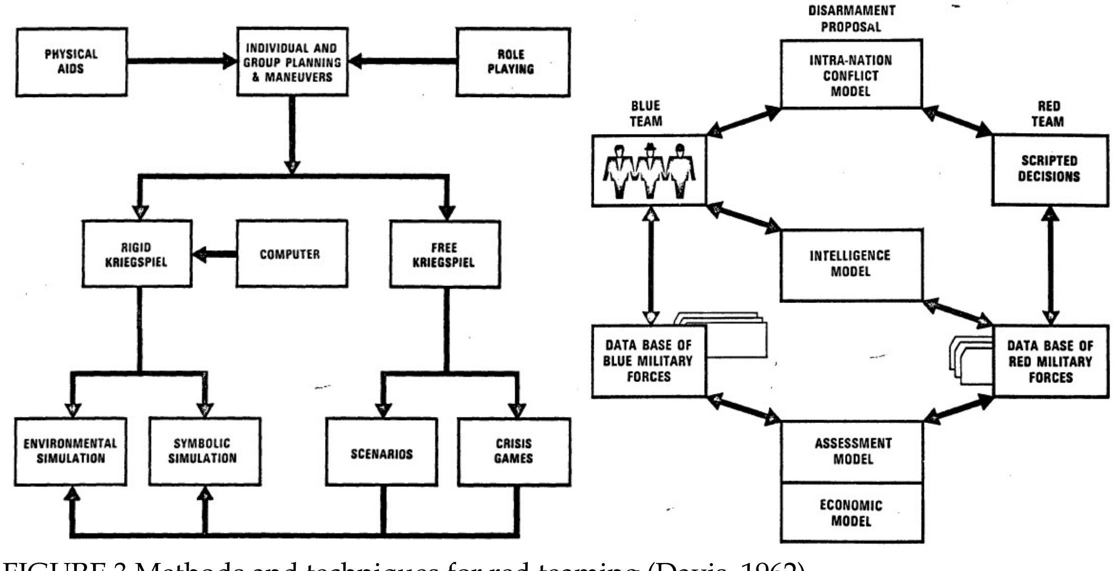


FIGURE 3 Methods and techniques for red teaming (Davis, 1962).

Game included red and blue team with military forces as a scenario. These scenarios were played by crisis games (scripted decisions) from the red team. Simulations were presented with the intelligence gained by blue team in support of their decisions. Symbolic simulations were also created in the assessments. (Davis, 1962) This is just one type of way to create a red teaming session to a complex situation.

2.4.2 Intelligence community and law enforcement turn to red teaming

Various red teaming initiatives started to emerge in the department of defense and in the intelligence community (IC) of the United States in the 1970's. During the presidency of Gerald Ford CIA had received some negative feedback from several failures (Mitchell, 2006). Presidential security advisor tried to force CIA to make alternative analysis but CIA Declined (Zenko, 2015) until Ford reshuffled his cabinet and Donald Rumsfeld[2] was appointed Defense Secretary, Richard Cheney rose to Chief of Staff, and George H. W. Bush took over as Director of Central Intelligence in 1976. Shortly thereafter, Bush approved a novel study of Soviet Cold War strategy which was known as team B. An early predecessor of current CIA red cell. (Mitchell, 2006) Bush authorized the first red teaming activities in CIA which were not embraced in the agency immediately (Bush, 1976). The idea of competitive analysis was appalling to some traditional IC members. Red teaming analysis was still done in the CIA even without an official team wasn't formed until 2001, which is marked as a key event in the history of the agency (CIA, 2016). The CIA red cell has been since endorsed as source of alternative and competitive analysis that mitigate the cognitive and institutional biases in the intelligence community (Zenko, 2015).

Interest to adversary simulation grew also in the law enforcement in the wake of terrorism in the west especially due to several hijackings of commercial aeroplanes (CIA, 1982). Commercial air travel was not similar in the past. Between 1968 and 1982 according to CIA (1982) 684 hijackings were attempted of which approximately 108 terrorist-related. That's 4 hijacks per month. Hijackings have resulted in at least 500 deaths and 400 injuries during that period. Security organizations started to acquire training from companies that ran terrorist simulations (Zenko, 2015). But the core problem was not fixed. Officials started to handle the terrorist situations and red cells were simulating hijackers. This is good, but it's better not to let the terrorists into the plane, that would have been the right answer which was learned later.

2.4.3 9/11 and importance of red teaming

In 1988 Pan Am Flight 103 was hijacked and it exploded over Lockerbie, Scotland killing 270 people. The bombing was made possible because of the several failures to screen, guard and tag authenticate bags that were loaded to the plane. Several recommendations to improve security were made by a presidential commission that investigated the incident in their report (The President's Commission on Aviation Security and Terrorism, 1990). The Federal Aviation Administration (FAA) created a special assessment team in 1991 which was referred as the FAA red team. Units tasks and orders were not quite clear at the start and concept of operations was drafted 1994 and legislative problems were

[2] Rumsfeld was the secretary of defence also in 2003 when Red Teaming was embraced in the department of defence 28 years later.

overcome in 1996 to give the team a real mandate by the Federal Aviation Reauthorization Act of 1996 (US Senate, 1996). Unit was tasked to conduct periodic assessments and unannounced investigations to determine vulnerabilities of air carriers and airports. Anonymous testing of security systems was also authorized (US Senate, 1996).

The safety of the air travel was also a concern for the United States Congress. Congress appointed a National Civil Aviation Review Commission to investigate the matter. Commission submitted their 200-page report in 1997 with several safety recommendations and summing it up by declaration *"FAA's Safety Strategy Must be Institutionalized".* (National Civil Aviation Review Commission, 1997).

The FAA red team operated and reported several issues every month under the office of inspector general in the department of transportation. In year 2000 the team reported again (report AV-2000-017) the FAA's slowness to take actions necessary to strengthen access-control requirements and adequately oversee the implementation of existing controls. Access controls were tested for six months and 117 of 173 penetrations were successful. Red team boarded 117 flights operated by 35 different air carriers with malicious materials. Employee failures were found to be the primary cause of access-control weaknesses. (U.S. Department of Transportation, 2000). Even the United States General Accounting Office gave a gloom view to the congress about the safety of aviation security in their special report in June 2000 supporting the red team (GAO, 2000). From 1990 through 1999, screeners located nearly 23,000 firearms and numerous explosive devices, resulting in over 9,400 arrests in the US airports. The main problem was the screening (GAO, 2000) and people knew that it is easy to pass the airport screenings.

The red team started to get frustrated because they had been reporting about security failures for several years and they saw very few advances happening. One reason why air carrier didn't comply with the red team was because they didn't need to. If a recommendation was not followed the carrier may be fined, but the sums were less than 50000 dollars which is not a sufficient sanction for an air carrier. In February 2001 an ex red team member Steve Elson went public and gave an interview about the shortcomings of airport security in the United States (Morris, 2001) and also demonstrated together with a reporter in May 2001 how security could be bypassed in Logan airport in Boston. In 11th of September United airlines flight 175 and American Airlines flight 11 lifted off from Logan airport and crashed to World Trade Center towers (9-11 Commission, 2004). This example of good penetration actions by the FAA red team is the best example what happens when red teaming is not supported by the management and incorporated to the business objectives.

This terrorist act was the one most devastating which started to wake the officials up and realize that they must think like the enemy if they want to match the adversary. Several red teaming initiatives have been made since in the department of defence (Defense Science Board, 2003), homeland security Exercise and Evaluation Program (DHS, 2004) and law enforcement activities (Meeham, 2007) in the US.

2.5 Modern schools of thought in red teaming

Scoping of red teaming activities is important because the tools and expertise needed from a red team is quite different in testing the security of a high security installation than challenging the vision of a multinational organizations business strategy. The scope of red teaming can be depicted in tiers such as NIST SP 800-53 portrays (NIST, 2013b) from organization level red teaming to processes and all the way to the information systems. Scoping also differs from a perspective. What the head of information security sees as a strategic question might be a technical level question to a CEO. This is elaborated in table 1 below and should be noted when red teaming activities are considered; what are you red teaming, corporation or its information security for example? Those are two very different issues.

TABLE 1 Perspectives on scoping.

	Military / Government	Corporate	Security	Information security
Strategic	Surviving as a nation	Corporate vision and strategy	Security vision and strategy	Information security strategy
Operational	Winning a war	Business management areas like security	Security policy	Information security policy
Tactical	Winning a battle	Company policies in divisions	Information security policy	IS sub policies like how to use company laptops
Technical	Killing the enemy	Teams implementing company mission	Security admin and enforcement	Technical controls

Several schools of red team have developed due to versatility of targets. Fleming (2010) classified red teams in a chart with threat emulation axis and a decision support axis to elaborate on differences in various teams. Figure 4. below describes a set of teams derived from the Flemings study with some additions.

Opposing force / red cells are used in war games and training exercises to simulate the adversary. Red cells are elaborated more in chapter 2.3.2. Physical and cyber red teams engage in activities of testing the target defences and breaking into sites. Physical FAA-team is elaborated in chapter 2.4.3. and cyber teams in chapter 4. Corporate or peer review teams commit reviews of organizational structures, processes, plans and products. These teams are not covered in this study, but in chapter 2.4.1. a similarly acting team is described Alternative analysis teams use structured analysis techniques and conduct competitive intelligence and scenarios. In chapter 2.4.1. and 2.4.2. such a team is described. Umbrella team is a unicorn. They don't exist. They are teams that combine everything and can operate in every environment. Hybrid teams do.

Hybrid teams combine aspects from various schools and adapt them to their clients' environment. Hybrid teams can also incorporate members from the defenders' side. These teams are referred in the literature as purple teams for they combine elements of red and blue (Erridge, 2018; Oakley, 2019).

The figure 4. creates understanding about differences of current schools of red teams. Figure is not conclusive, and it creates artificial boundaries to red teaming. If comprehensive red teaming is considered, all the functions from red cell up to alternative analysis need to be addressed. Emphasize on certain functions creates the difference between teams.

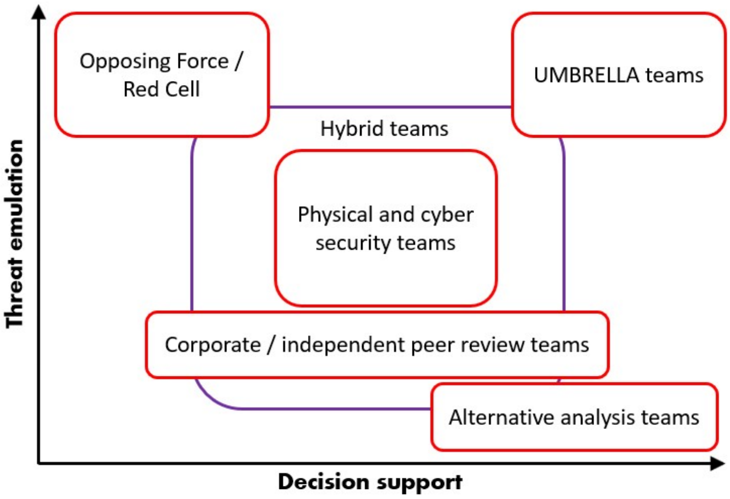

Opposing Force / Red Cell
UMBRELLA teams
Hybrid teams
Physical and cyber security teams
Corporate / independent peer review teams
Alternative analysis teams
Threat emulation
Decision support

FIGURE 4 Various types of red teams. (Modified from Fleming (2010))

Red teaming is no silver bullet and there is no silver bullet in red teaming either. There are various ways in committing red teaming activities, but one recognized fact is that a process and tools are needed to manage the effort. The following ten steps combine a basic structure of a red teaming exercise / activity (Meehan, 2007):

1. Determine the objectives of desired results (scoping)
2. Communicate with stakeholders
3. Determine the scale and type of exercise, scenario and evaluation.
4. Develop the scenario for training
5. Identify and train the appropriate participants
6. Conduct and evaluate the exercise - Document through exercise
7. Evaluate the performance
8. Develop the improvement plan
9. Make the required and desired improvements and train them
10. Go back to step 1

Red teaming is a process, not a project. The process needs to be accepted in an organization to make it a success factor in mitigating own biases and noise.

2.6 Conclusions about red teaming

Red teaming has developed in several fields of life during the last 50 years. This might reflect from psychological studies that started to question human biases (Tversky & Kahneman, 1974) and create counteractions to mitigate those pitfalls in decision-making. Military has always been keen on challenging their plans and wargaming during planning processes, but not always without resistance. Failures usually lead to self-examination and after 9/11 and several military failures, red teaming started to gain momentum. In 2003 the US department of defence declared that red teams are valuable, but underutilized tool. DOD also recognized that red teaming is a cultural change which challenges the organization and its norms, and this is needed against adaptive adversaries and guard the against complacency. (Defense Science Board, 2003)

Red teaming should not be restricted to mere adversary emulation for its purpose is to support in creating better plans, policies, procedures and products. This cannot be done by simply pointing out the flaws, but diagnostic and creative aspects need to be emphasized (Development Concepts and Doctrine Centre, 2013). Various categories have already been made for red teaming like in law enforcement Meehan (2007) separates red teaming activities into two major categories, analytical red teaming (passive) and physical red teaming (active) and intelligence mentions the term; competitive intelligence (Mitchell, 2006). These categories vary depending on domains and is the red teaming considerer more adversary emulation or decision support element (Fleming, 2010). Purple teams that combine the red team and the defender's assets are the next evolution step which creates better understanding of threat in the defender-side.

Dissident thinkers in the army or in any domain are not always welcomed or accepted (Davis, 1962). Therefore, red teaming should be a process that can be explained, and it should be also transparent and traceable. A little tact and empathy will get more results than a blunt presentation of faults (RTJ, 2016). Red teaming is about mitigating future risks and communicating bad news. Baskerville (1991) claims that risk analysis has profound role as a communication technique which can possibly be adapted to red teaming as well. This might be the key in communicating the need for a culture change in an organization. Training and awareness are the ways to increase knowledge and they are needed to implement the change (DHS, 2004).

Organizations should adapt red teaming as a part of their processes, but this also calls for attention. Insiders tend to come to agreements in roundtables due to loud and confident opinions. This can be mitigated by using outsiders or changing the processes that insiders can act as outsiders and are not affected by the opinions of loud and confident group members (Kahneman et al., 2016). Several possibilities to implement red teams are available (US Joint Chiefs of Staff, 2016). Red teaming is a process, not a project. The process needs to be accepted in an organization to make it a success factor in mitigating own biases and noise.

3 INFORMATION SECURITY MANAGEMENT

"If you think compliance is expensive, try non-compliance."

- U.S. Deputy Attorney General Paul McNulty -

This is a descriptive chapter which builds to the environment section in information systems research framework (Hevner et al., 2004) used in this study. In the design science research methodology process this chapter comprises a part of phase 2; defining objectives of a solution and enables phase 3; design and development of the construct (Peffers et al., 2007). Aim of this thesis is to study red teaming and develop it as a discipline in the context of information security management. First, information systems, information security and risk management are defined to elaborate the relationship between red teaming and information security management. Then findings from different information security management concepts and standards are presented.

Raggad (2010, p. xxix) describes information security management as *"a comprehensive framework to protect an organization's computing environment, including its people, activities, data, technology, and network"*. ISO 27000 (2018, p. 4) defines information security as *"preservation of confidentiality, integrity and availability of information"*. NIST SP 800-53 (2013, p. Appendix B) defines information security as *"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability"*

Conclusion from these definitions is that information security management does not have one overarching definition whilst same topics are contemplated. Definition is dependent on the environment, scope and purpose of the document.

3.1 Information system definitions

Information systems is an academic study area of its own. Information system like information security can be defined from different perspectives. Boell & Cecez-Kecmanovic (2015) identified 34 different definitions for information system in their research paper. The problem concerning inconsistency on definitions was identified more than three decades ago by John Zachman in his study by asking *"What, in fact, is information systems architecture?"* Zachman (1987, pp. 454-455) had a justifiable suspicion that term "information systems architecture" might even lose its meaning. He took an analogy from classical architecture and used examples such as designing a house and an airplane. Key stakeholders in architectural design are the owner, the designer and the builder. All three must understand the information system in a similar way, although the nature and level of detail in representations is different. Challenge to date remains that information systems are complex engineering products. (Zachman, 1987)

Zachman (1987) found that information system can be described from three different perspectives:

1. Functional description – generic process model (input-process-output)
2. Material description – entity-relationship-entity data model
3. Location description – node-line-node network model

And his conclusion from this was that there is not an information system architecture, but a set of them. (Zachman, 1987)

Different descriptions of information system architecture are additive and complementary, but definition is needed for interaction between information system professionals. (Zachman, 1987) So perhaps surprisingly, or not, the term information system is still taken for granted. In an editorial by the European Journal of Information Systems Paul, R.J. contemplates the issue:

> "It could be a surprise that what an IS is, is not established. On the other hand, since many people are studying IS from a variety of perspectives, maybe it should be no surprise that there are a variety of definitions. But then, how would Society know what IS is, and what it can do if there is no clear understanding?" (Paul, 2007, p. 194)

Information systems are decentralized by nature, and without a structure these distributed computing facilities can be a chaos. Order, control and discipline can be achieved by use of architecture. (Zachman, 1987) This study focuses on information systems on a generic level. Therefore, an exact architecture is not needed, but a definition must be composed.

Definition for information system can be drawn from four different views, which are technology view, social view, socio-technical view and process view respectively (Boell & Cecez-Kecmanovic, 2015).

Definition for a generic information system consists of components such as people, information (data), software, hardware and network (Boell & Cecez-Kecmanovic, 2015). Definition is supplemented with Zachman's (1987) functional description, i.e. the input-process-output model. Abstracted definition of an information system for this study is depicted in the figure 5. below.

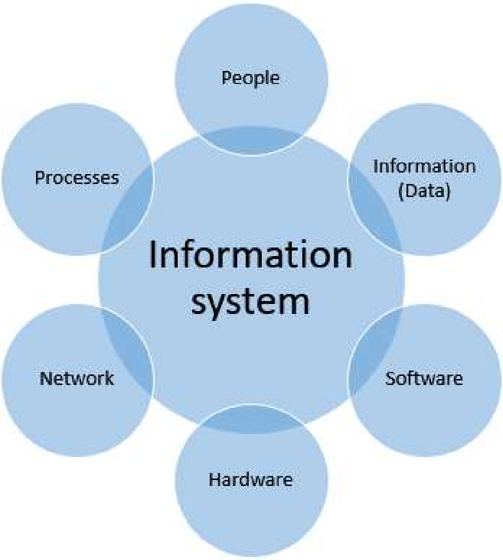


FIGURE 5 Information system combined (Zachman, 1987; Raggad, 2010 and Boell & Cecez-Kecmanovic, 2015).

These systems, or systems of systems, are in place to support organizations decision making, management and create business value. DeLone & McLean (1992) approached information systems from a success factor perspective by reviewing 180 articles written through 1980's. Result from their research was comprehensive IS success taxonomy and IS success model (DeLone & McLean, 1992). DeLone & McLean reviewed, evaluated and updated their model in 2003 (DeLone & McLean, 2003). The updated model is depicted in the figure 6. below.

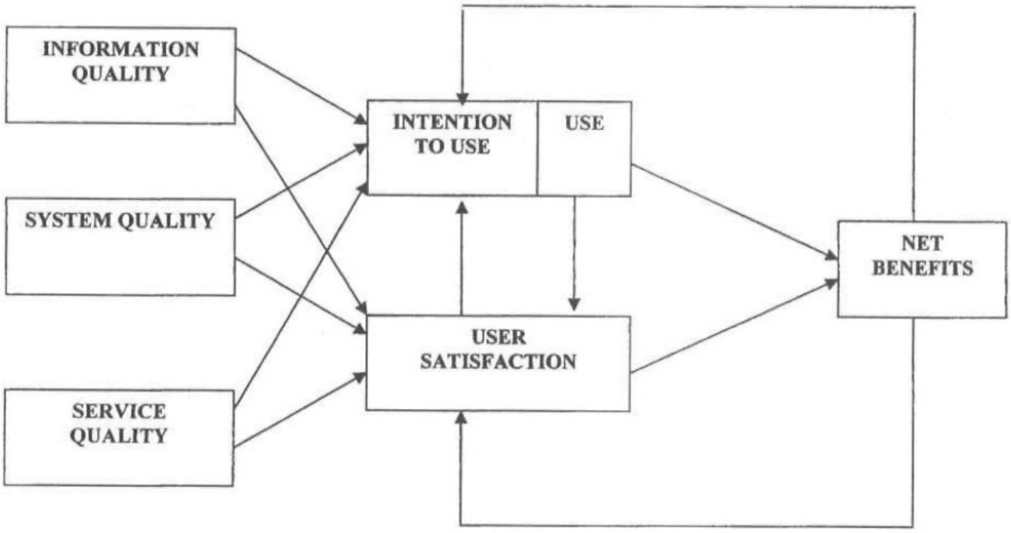


Figure 3. Updated D&M IS Success Model

FIGURE 6 Updated IS Success model (DeLone & McLean, 2003)

Information systems success is a complex, multidimensional and interdependent by nature. The either positive or negative causal associations are described by arrows in the figure 6. above. These associations need to be adapted to the context of a given study by making appropriate hypothesis. Especially the "net benefits" measuring calls for more research. (DeLone & McLean, 2003)

When referring to information system in this study it denotes to a system that consists of people, information (data), software, hardware network and processes as depicted in figure 5. Assumption on the background is that information systems are in place to produce "net benefits" for any given organization.

3.2 Information security management defined

Information quality, system quality and service quality, mentioned as success dimensions by DeLone & McLean (2003), are tightly related to information security. Information security goals, the CIA triad (confidentiality, integrity and availability), described by Raggad (2010), ISO (2018) and others are widely used as general requirements for information security. For the CIA triad definitions from ISO 27000 (2018) standard "*Information technology - Security techniques - Information security management systems - Overview and vocabulary*" are used in this study.

- Confidentiality means that data in the information system is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity means that data in the information system is accurate and complete.
- Availability means that information system is accessible and usable on demand by an authorized entity.

In the following table the success dimensions and metrics from DeLone and McLean (2003) are described with their relevance to CIA triad (ISO, 2018).

TABLE 2 Information system success dimensions relevance to CIA.

Success dimensions and metrics (DeLone & McLean, 2003)	Relevance to CIA security goal definitions
Information quality • Completeness • Ease of understanding • Personalization • Relevance • Security	Confidentiality – Information needs to be secured Integrity – Information needs to be complete
System quality	Confidentiality – System needs to be reliable

• Adaptability • Availability • Reliability • Response time • Usability	Integrity – System needs to be reliable and not tampered Availability – System needs to be usable and available
Service quality • Assurance • Empathy • Responsiveness	Availability – Service needs to be assured

Conclusions from the comparison table are that;

1. If positive net benefits such as cost, and time savings can be achieved through information, system and service quality, then
2. Adopting security as a goal along with direct business objectives supports the achievement of net benefits.

Any system is strong as its weakest link. Therefore, when managing information security, the information system must be protected comprehensively. Raggad (2010) describes this process as an information security life cycle, where integration means that all six activities must be integrated together for the lifecycle to be effective. In this study the meaning of Raggad's integration is extended. Presumption is that integration also includes protecting all the elements of a given information system, which is depicted in the figure 7. below.

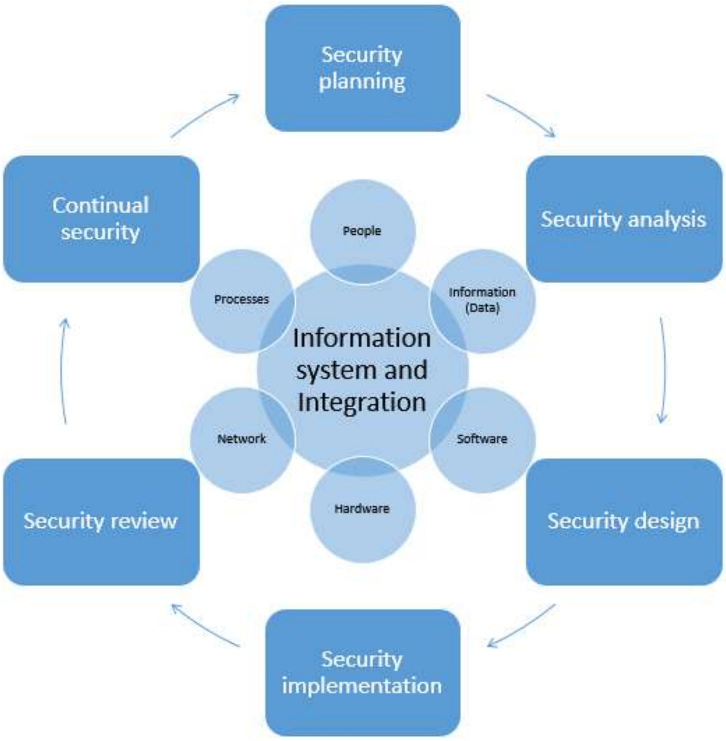


FIGURE 7 Information Security Life Cycle (Raggad, 2010) modified by Frilander & Tuovinen (2019) to "Information System Security Lifecycle".

Same principle is described by Raggad (2010) as "security of an information system", in which the interacting components are people, technology, activities, data and network as an enabler.

Deduction from the previous paragraphs is that information security is interdependent, and all components must be secured in order to achieve security. In other words, each computing system component is a possible attack vector.

Information security management framework offers a plethora of concepts and practices to pursue security. Vocabulary includes terms like information classification, governance, defence in depth, security controls, security planning, security policies, risk analysis, security analysis, auditing, threat analysis, vulnerability analysis, risk management, business continuity planning, system availability, standards and compliance just to mention a few. (Raggad, 2010)

Perhaps the most difficult task of information security management is effective implementation in practice. (Siponen & Baskerville, 2018) In a broader perspective secure cyberspace has been recognized as one of the 14 grand challenges for engineering in the 21st Century, as electronic information flow is embedded into nearly all aspects of modern life. Cyberattacks into critical infrastructure such as electricity, gas and water distribution could have serious impacts on the whole society. (National Academy of Engineering, 2019)

Information security is implemented by use of control measures, which are selected in the risk management process. Controls are managed by processes and procedures which are usually described in information security policies. Technical information security controls consist of specific software and hardware. All controls need to be integrated into organization's business processes. (ISO, 2018)

3.2.1 Risk analysis in information security management

Richard Baskerville (1993) elaborated the problems of first-generation systems analysis and security analysis used in the 1970's in the context of information systems development. Limitations of security controls led the developers to mind-set of "what can be done" instead of "what needs to be done". Controls of that time were usually presented as checklists of all security controls that can be implemented. Problem with the checklists was that the connection of a given security control and associated risk was not clearly stated.

Cost-benefit model was needed to exclude unnecessary controls depending on organization and its environment. Risk analysis was adopted as one of the early formal techniques to justify or reject different controls from checklists. It was a rational way for consistent evaluation of vulnerabilities albeit facing critique, which is subjected specially to counting probability. Addressing numerical values for probability is in the worst case nothing more than unverified guessing (Baskerville, 1993).

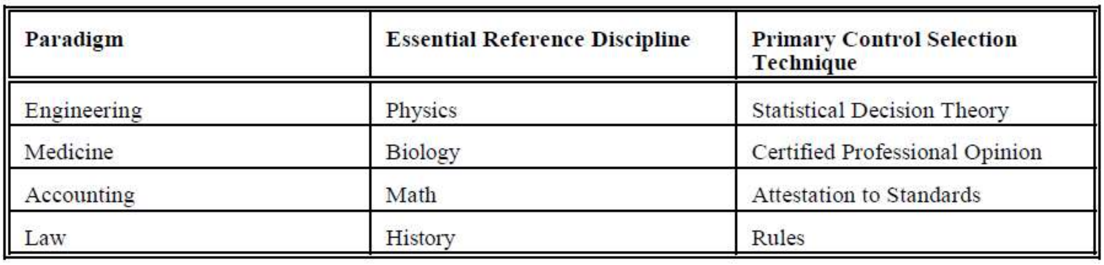
Risk analysis has kept its position as one of the information security design methods albeit facing aforementioned critique, for which academic research has offered several solutions like acknowledging cultural theories (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2006), user participation (Spears & Barki, 2010) and perception of risks (Vance, Anderson, Kirwan, & Eargle, 2014)

Risk calculation matrixes are extensive as they include factors such as threats, assets, vulnerabilities and cost in addition to probability. Amount of data that emerges from the risk calculation can be too overwhelming to enable decision-making, and still some of the factor values could be subjectively decided. Quantitative measuring of risks is doubtful due to these reasons. Different kind of specifications and checklists might also overlook innovative solutions and postdate technology advancements. (Baskerville, 1993)

Baskerville (1991) summarises critique on risk analysis in a contradictory manner:

> "The subjective nature of risk analysis, under guise of its appearance as a statistical predictor, is subject to misuse. By overrating its scientific qualities, it may cause the implementation of costly, unnecessary controls. Perhaps worse, it may also allow the deployment of inherently unsafe, fragile information systems." (Baskerville, 1991, p. 5)

Risk analysis also fails in one scientific test, results cannot be proven to be wrong (refuted). (Baskerville, 1991) After his critique Baskerville (1991) presents alternative tools for risk analysis, which are improved statistical decisions, certified professional opinion, standards and attestation, and rules respectively. Search for alternative methods has produced academic research such as utilizing game-theoretic approach to justify security investments through risk management. (Cavusoglu, Raghunathan, & Wei, 2008) In practice alternatives proposed by Baskerville (1991) overlap considerably, and another challenge for their implementation are the scientific reference disciplines presented in the figure below.



Paradigm	Essential Reference Discipline	Primary Control Selection Technique
Engineering	Physics	Statistical Decision Theory
Medicine	Biology	Certified Professional Opinion
Accounting	Math	Attestation to Standards
Law	History	Rules

FIGURE 8 Risk analysis paradigms for control selection (Baskerville, 1991)

Information system development has foundation on social science, and therefore is subjected to probabilistic social laws. Computer science however is founded on physics (Baskerville, 1991). Information security efforts aim on protecting the entire architecture as was presented in previous chapter and are therefore subjected to social sciences and physics.

Baskerville (1991) states that adoption from biology/medicine, math/accounting or history/law to risk analysis is not possible because of the nature of information systems. For example, dynamics of information system development and threats can defeat historical rules. (Baskerville, 1991)

Baskerville's main conclusions about relevance of risk analysis were that it has a profound role as communication technique between developers, management and security professionals. It enables identification of baseline controls that are economically feasible. Risk analysis strength is in its philosophical versatility. Effectiveness of controls selected through risk analysis is relative to designers and security expert's know-how, which is a risk of risk analysis that must be acknowledged. (Baskerville, 1991) Baskerville's conclusions are supported in practical implementations such as NIST SP 800-53 (2013b)

After Baskerville, several researchers have shown that risk management process can be improved by acknowledging the probabilistic social laws (Tsohou et al., 2006; Spears & Barki, 2010; Vance et al., 2014).

Even security experts are subjected to perceptions that can influence defining, choosing and implementing security controls. (Tsohou et al., 2006) Later research also supports paying attention to social elements of risk management; "Why not ask for the user opinion?". User perspective can be useful on developing the business case for security investment, as well as developing more effective controls through risk analysis and raising awareness. (Spears & Barki, 2010) Von Solms (1999) emphasizes the role of risk management as an integrated part of information security management influencing areas such as IT security recommendations, IT system security policy and IT security plan.

Tsohou et al., (2006) present a clear and easy to understand model on how risk management is consucted as a process. Presentation cites from IS27001 (2005) and Baskerville (1991).

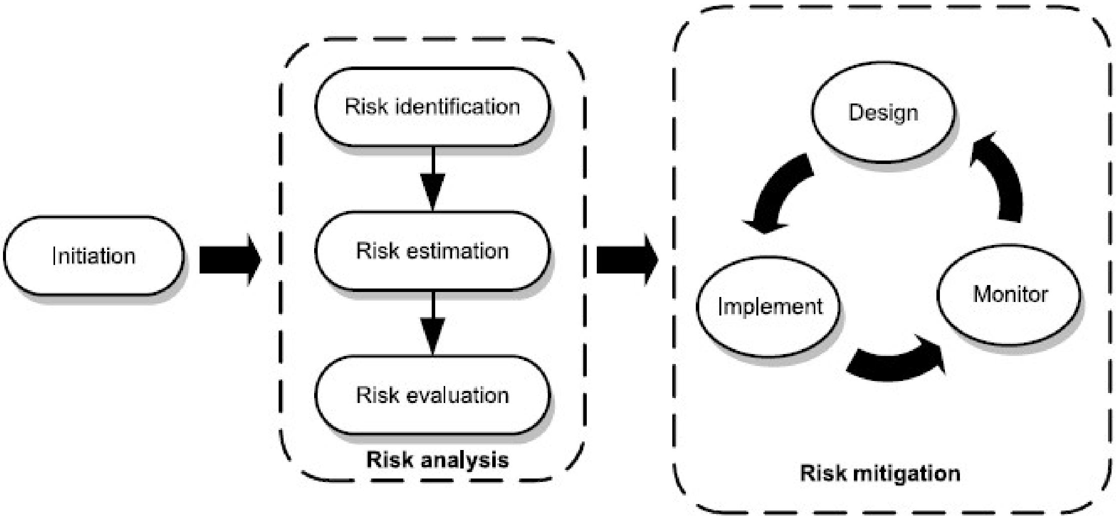


FIGURE 9 Risk management stages (Tsohou et al., 2006).

Although threat – asset – vulnerability junction is mentioned by Tsohou et al., (2006) in the text, threats are not depicted in the figure 9. It can be argued that the information security "game" between a malicious actor and an organization defending information system assets is a game of uncertainty. Defenders uncertainty of malicious actor's intentions reduces for example the effectiveness of game-theory applications. (Cavusoglu et al., 2008) Acknowledgement and identification of threats can improve defenders' position. Remembering, that the threat could come also from the inside (Raggad, 2010).

3.3 Information security management concepts

In previous sub-chapters the generic framework of information security management, risk management and their relationship to information systems and delivering net benefits through security were described. In this sub-chapter different information security management concepts, standards and academic publications are presented and compared to form a better picture of the environment. In the final sub-chapter, conclusions are made on how information security management fits into information systems research frameworks environment section, which is a part of the design science research model methodology used in this study.

Information security policy process models have been introduced in various standards like ISO27001, BS 7799, PCIDSS, ITIL and COBIT (Susanto et al., 2011) which all have their unique features, NIST SP 800-53 (2013b) for example being a risk-driven standard. All these models are still based mostly on best practices and not of research (Knapp et al., 2009). Even developed models like BS ISO/IEC17799: 2000, GASPP/GAISP, and the SSE-CMM have been found to be general in scope and should be used with certain doubt (Siponen & Willison, 2009). A general but more comprehensive model by Knapp et al. (2009) is used to examine the academia's contribution to the information security management in chapter 3.3.4. Knapp et al. (2009) model pays more attention to the content and not just to the existence of the process, which is paramount (Siponen, 2006).

3.3.1 ISO 27000 and 27001

ISO 27000 (2018) "Information technology - Security techniques - Information security management systems - Overview and vocabulary" is a capstone standard which gives an overview of information security management system. Terms and definitions for other 27-series standards are also provided in the ISO 27000 (2018) along with justification about why information security management is important.

Effective information security management requires for an understanding and identification of information assets, business needs related to information systems and compliance requirements. Systematic risk assessment is prerequisite for selection and implementation of controls. (ISO, 2018)

ISO 27000 (2018) is comprehensive. It acknowledges several information security key features such as awareness efforts, roles and responsibilities, management commitment, enhancing social values, risk assessment, implementation of controls, active prevention of threats, comprehensive approach to information security and continual reassessment of effectiveness. But still, it is generic by nature.

ISO 27001 "Information technology - Security techniques - Information security management systems – Requirements" (2013) is a standardization perspective for providing and maintaining information security management as a system.

It is vital that information security management is integrated into organizations business processes and management. Risk assessment must be tailored according to organizational needs. Foundation for all information security efforts comes from leadership commitment (INB, 2013). Or as Micah Zenko (2015) states in his book; Red Team, about implementing a new function, "the boss must buy in" and embrace the new function.

Buy-in theory is recognized by several academic researchers. User participation and effort in information security management activities affects to users' perceptions. Personal involvement has a positive influence to seeing systems and security activities important and relevant. User participation also raises awareness of risks related to business processes and business objectives. (Spears & Barki, 2010) Effective implementation of information security management calls for the buy-in to happen on all levels.

Planning of information security must cover several functional areas such as risk assessment, control measures, objectives, resources, documentation, communication, training, awareness, roles and responsibilities, actual operations, performance evaluation, audits and continual improvement. (INB, 2013)

Especially the Annex A in ISO27001 (2013) is very comprehensive. It is a normative description which sets reference control objectives and control measures for information security covering both managerial and technical aspects. Any organization would have more than adequate protection if this standard, like many others, was diligently followed and implemented. This brings us back to the main challenge in information security management that Siponen & Baskerville (2018) have raised for debate. Why effective implementation is so difficult in practice?

Information security is not an end itself. There are different perspectives such as governance, which includes overarching company objectives, risk perspective and compliance perspective. Threats in the given context should always be identified, no matter which perspective is the key motivation. (ISACA Germany Chapter e.V, 2013)

ISACA implementation guideline (2013) for ISO 27001 also puts forward a component depiction for information security management system.

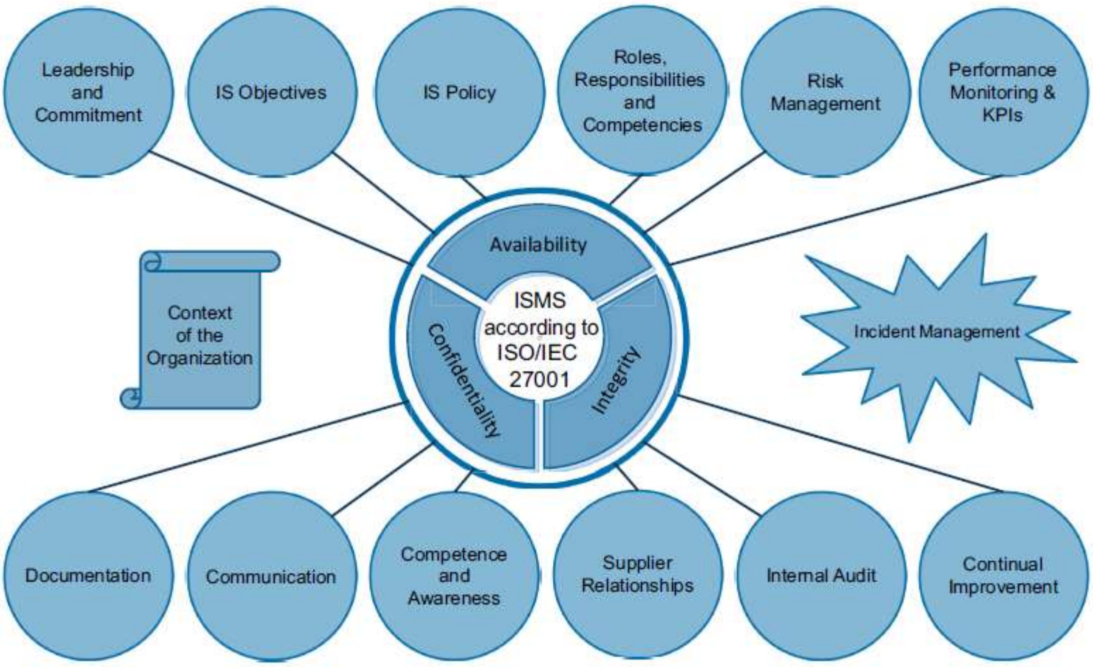


Figure 2: Components of an ISMS in accordance with ISO/IEC 27001:2013

FIGURE 10 Components of an information security management system (ISACA Germany Chapter e.V, 2013)

This component breakdown is comprehensive, but threats are not mentioned in it. It can be presumed that threats are part of risks, incident management and some other components setting the stage for control requirements. The term "threat" appears 19 times throughout ISACA (2013) implementation guideline, sometimes having adjacent meaning to risk.

According to Raggad's (2010) definition risk means that there is some level of likelihood for a threat to unfold, and there is a vulnerability which the threat can exploit. ISO 27000 (2018) defines risk merely as "effect of uncertainty on objectives". However, note 6 in the definition is more comprehensive and very close to Raggad's definition, stating that;

> "Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization." (ISO, 2018, p. 8)

Deduction is that organizations should be more aware of threats and exploitable vulnerabilities in their information system assets. Theoretically, if you take out the threat or vulnerability, there will be no more risk. From the ISO standards review it can be concluded that systematic risk management is a key information security process. One cannot select and implement controls effectively without understanding the risks.

3.3.2 Risk management standard

Risk management standard (RSM) is not a detailed document which offers checklists, and it is not a driver for a certification process. However, it identifies the existence of both positive and negative risks. Risks are most often negative in the context of information security management, as they are a threat for achieving the security goals. Therefore, information security risk management focuses on preventing the risks realization, and mitigation of impacts. (The Institute of Risk Management, 2002)

Risk management standard identifies risk management as an integral part of any organization's s strategic management. It also states that risks originate from both external and internal factors. Risk management is a tool that can add value by protecting assets and company image. (The Institute of Risk Management, 2002) This is an equivalent to producing "net benefits", as was discussed in chapter 3.2.

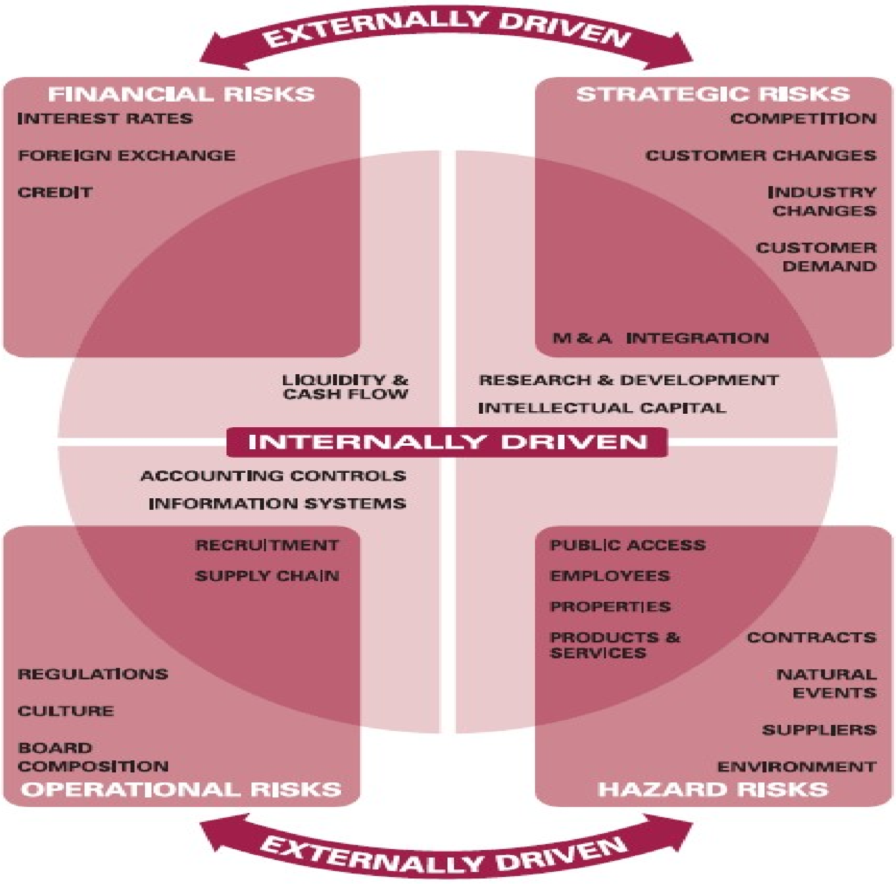


FIGURE 11 Examples of the drivers of key risks (The Institute of Risk Management, 2002)

Some of the risks can be derived from both external and internal factors, and consequently they are overlapping. One key area of such overlap are the information systems. Prerequisite for risk identification is thorough understanding of critical success factors and threats related to achieving them. (The Institute of Risk Management, 2002)

Identified and evaluated risks need to be reported on all levels in the organization. Key objectives are to show top management commitment, raise awareness, monitor the risks and understand accountability for preventing the risks realization. (The Institute of Risk Management, 2002)

Risk treatment in risk management standard (2002) is described as a *"process of selecting and implementing measures to modify the risk"*. Definition is generic, because that is the nature of the standard. In the context of this study it is assumed that "measures" are an equivalent to controls mentioned by Raggad (2010), ISO 27-series (2018) and NIST SP 800-53 (2013b).

Effective risk management requires monitoring and reviews because the environment of information security is very dynamic. Objective of this is to ensure that controls are functioning as intended. Scenario analysis, threat analysis, audits and inspections are some examples of risk identification techniques. (The Institute of Risk Management, 2002)

3.3.3 NIST SP 800-53

Building of information security in any given organization is a complex task and it's very dependent on environmental variables. In this sub-chapter an information security management implementation guideline for specific environment, federal information systems and organizations, is introduced. "NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations" (2013b) risk management framework has similar characteristics to Raggad's (2010) information security life cycle. Most importantly the cyclic nature. It also relates to ISO 27000 (ISO, 2018) from the perspective that risk assessment and risk management are prerequisite for selection and implementation of security controls.

Foundation for security comes from clear and concise security requirements and specifications. Systems and security engineering must be a parallel effort in order to build robust information technology. Security practices must be documented and integrated seamlessly into training and daily routines. Life cycle mind-set can be adapted to several functions. It covers areas such as continuous monitoring of organization and information systems, requirements that come from compliance, system development and information security. (NIST, 2013)

It is important to understand that information security is only one of the operational capabilities that are required from any information system. Information systems are in place to support business processes and in the end-state, to enable achievement of business goals. Therefore, it is crucial that risk assessment is realistic, and the prerequisite for that is understanding of threats and vulnerabilities. (NIST, 2013).

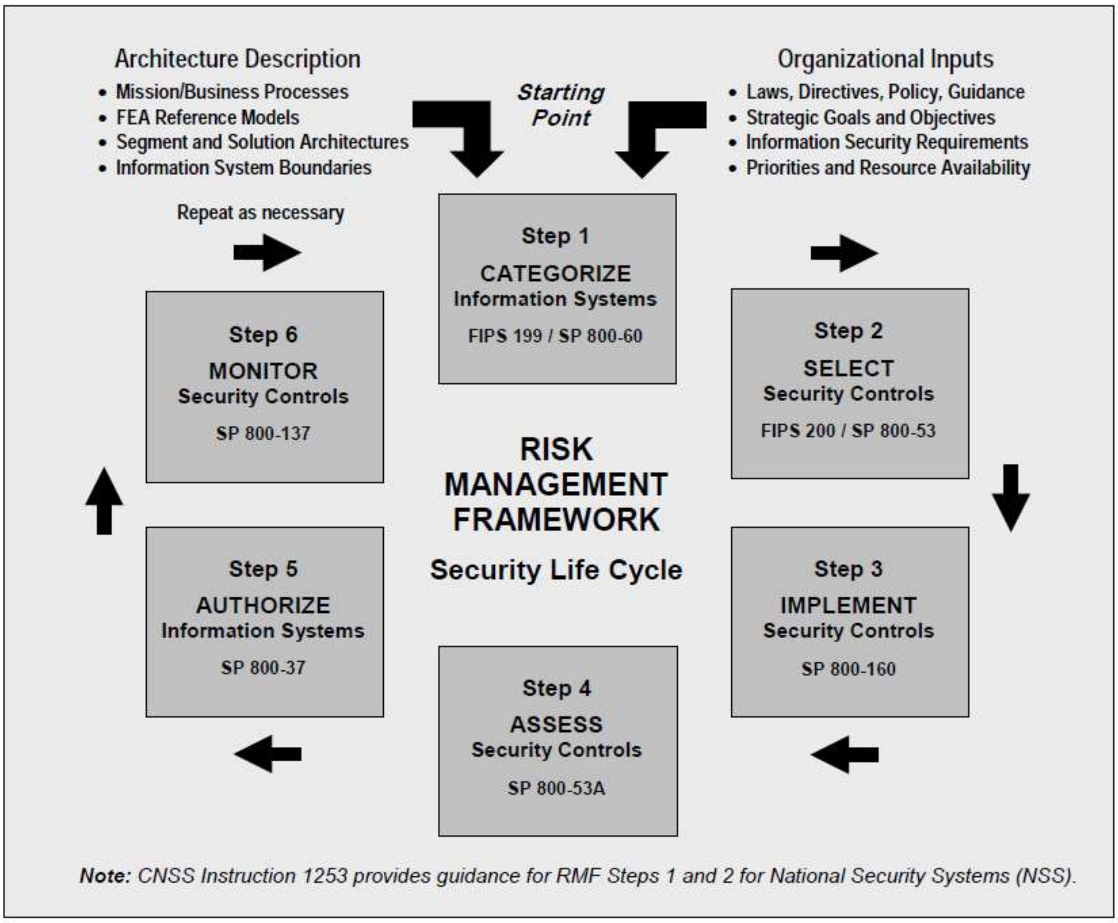

Architecture Description
• Mission/Business Processes
• FEA Reference Models
• Segment and Solution Architectures
• Information System Boundaries
Starting Point
Organizational Inputs
• Laws, Directives, Policy, Guidance
• Strategic Goals and Objectives
• Information Security Requirements
• Priorities and Resource Availability
Repeat as necessary
Step 1 CATEGORIZE Information Systems FIPS 199 / SP 800-60
Step 2 SELECT Security Controls FIPS 200 / SP 800-53
Step 3 IMPLEMENT Security Controls SP 800-160
Step 4 ASSESS Security Controls SP 800-53A
Step 5 AUTHORIZE Information Systems SP 800-37
Step 6 MONITOR Security Controls SP 800-137
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).

FIGURE 12. NIST Risk management framework (NIST, 2013).

When new information systems are built in a correct manner, security controls are implemented already during the development (NIST, 2013). This fundament is also mentioned in ISO 27000 (2018), with the mention that security failures during development will lead to additional costs at minimum, and in the worst case the security objectives cannot be met.

With so called legacy systems the situation is more difficult. Gap analysis is used together with risk assessment to identify need for additional security controls. (NIST, 2013) This is one example of many situations where red teaming can be useful, for example to identify security gaps in ever-changing threat environment, and to give additional perspective for risk assessment.

NIST Special Publication 800-53 (2013) has a strong risk assessment and risk management perspective. Risk-based selection of security controls is a judicious approach because it is a rational driver for effectiveness and efficiency. The initial security controls form a baseline, from which the final security control decisions should be tailored company specific. One key driver for tailoring is assessment of organizational risks. Risk management process should be integrated to whole organization on all levels. In the NIST SP 800-53 (2013) this is described as three-tier approach. (NIST, 2013)

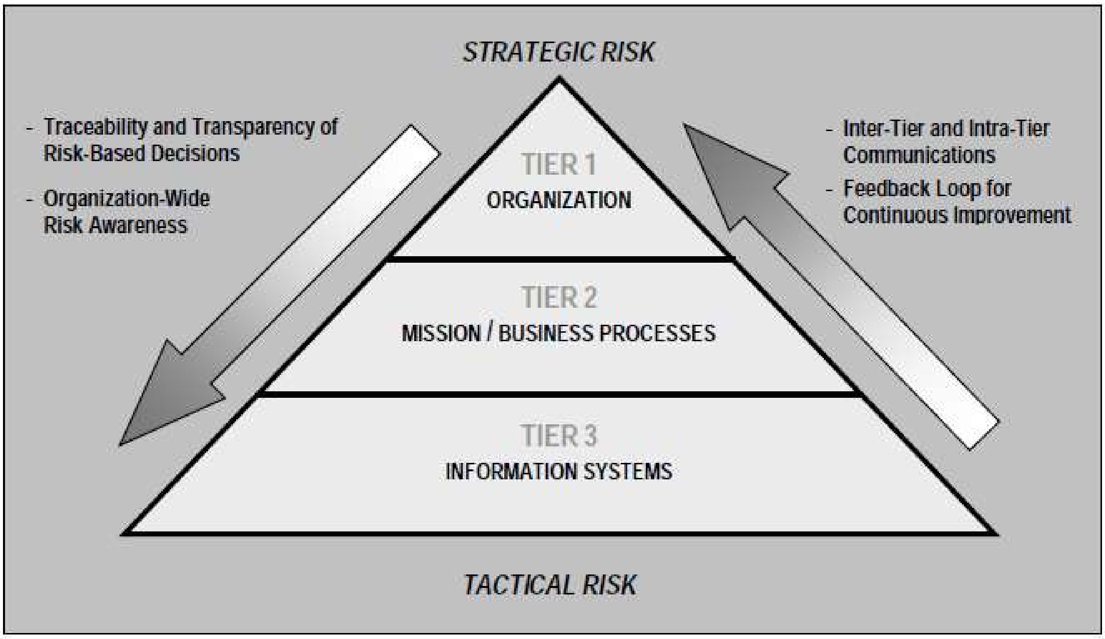

STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TACTICAL RISK

FIGURE 13 Three-tiered risk management approach (NIST, 2013).

In this study the focus of red teaming is on Tier 3, the information systems. However, companies like IBM and agencies such as CIA have used red teaming to reduce risks, and to find alternative methods for problem solving. Defence industry in the United Kingdom has recently started to apply red teaming on high level policy decisions and strategy development. These efforts are done to test that plans are coherent and robust before their deployment. (Development Concepts and Doctrine Centre, 2013) Conclusion is that in an optimal situation the red teaming effort is executed during development of documentation, policies, technology etc. if possible. Second conclusion is that red teaming could be a suitable tool for all three tiers in the SP 800-53 NIST (2013) risk management approach.

The United States Department of Defence is considering testing the cyber security of its contractors by using red teaming. Industry has provisionally agreed for testing of their vulnerabilities, because data breaches have been an issue. This might lead to convergence of commercial and military requirements concerning secure architecture and be an extension to compliance checks. (Mehta, 2018)

In the NIST Special Publication 800-53 (2013) the word “life cycle” appears 77 times. On 56 occasions it relates to the importance of integrating information security and security controls already during the information system development. Information security risk management process should be integrated into system development life cycle.

Conclusion is that information security, whether looking at the overall effort or the policy development, should be cyclic by nature, risk driven and closely related to business objectives. Relation to risk management and business objectives is also supported by NIST framework for improving critical infrastructure cybersecurity (NIST, 2017).

3.3.4 Comprehensive information security policy process model

Security programs are an essential part of implementing information security management, and security policies are the foundation for security programs. Information security policy is also described as one the most important security controls. It is important to bear in mind that information security policy is only a statement, although a powerful one from the management perspective. Still, if a process model is not favoured by practitioners, it will not be effective. (Knapp et al., 2009)

In the previous chapters information security management was defined, the key role of risk management was identified, and their relation to protecting information systems on a standardized conceptual level was presented. It was also found out that although external and internal influences are mentioned, they are not always clearly presented in the process models found from standards. However, external and internal factors are mentioned in a risk management standard from the Institute of risk management (2002). On the reviewed standards the external and internal influences were mainly related to risks and compliance.

Development and effective enforcement of the security policy requires a comprehensive organizational level process model which includes both external and internal influences (Knapp et al., 2009).

Next, a generic model, created by Knapp et.al (2009) is introduced. Researchers subjected their model for three rounds of scrutiny among certified information security professionals. The one thing that separates this model from the previous ones is that this is based on research, while at the same time taking into consideration professional practitioners' insight. Both Siponen & Willison (2009) and Knapp et.al (2009) state the standards are based mostly on best practices. The model developed by Knapp et al. (2009) is in the figure 14. below.

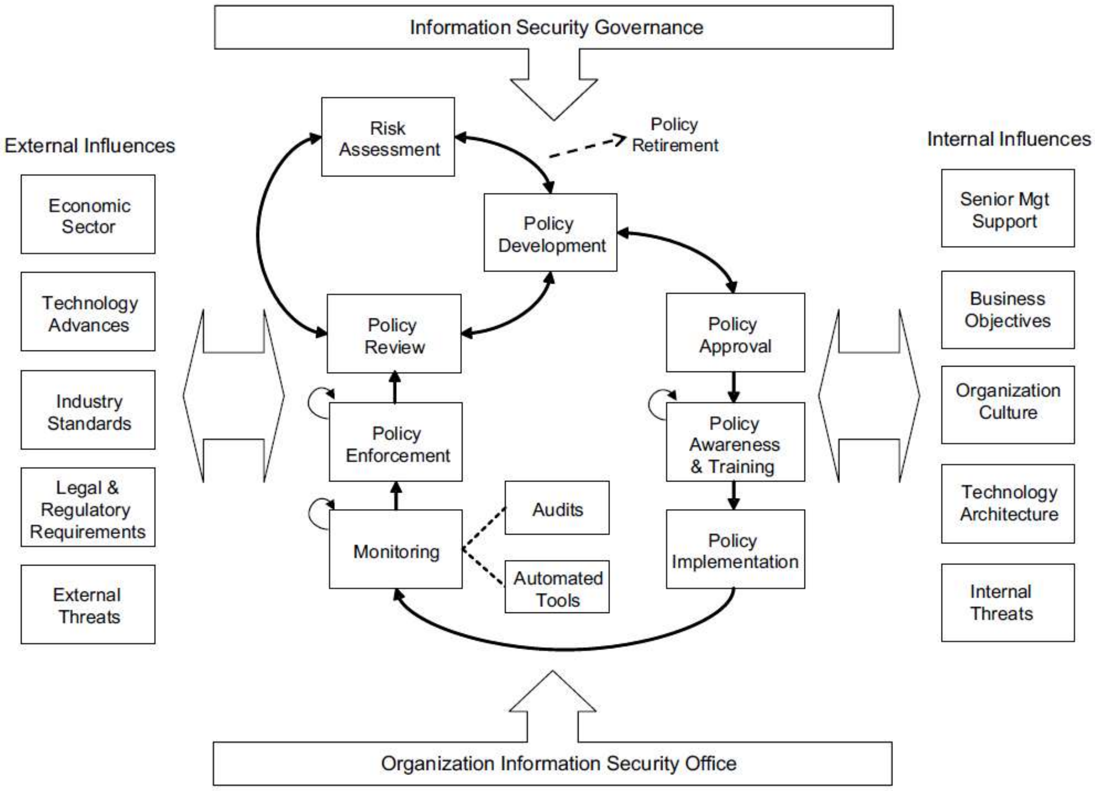


FIGURE 14 Information security policy process model (Knapp et al., 2009)

From the previous chapters it can be concluded that none of the models are perfect not even this one. Knapp et.al (2009) model incorporates and combines the interlinkage of risk assessment and information security management as well as the internal and external influences that need to be considered. This model is used to point out the relation of information security and red teaming in the next chapter due to its general, but still comprehensive nature.

3.4 Conclusions from information security management

The problem to be solved is now identified, and motivation has been given for the research topic, which is the first phase of the DSRM process described by Peffers et al. (2007). Effective implementation of information security has proven to be difficult, although the efforts are justifiable.

Information security management in practice can be defined as implementation of managerial and technical controls that are selected in risk management process and are integrated into organization’s business processes. Effective implementation calls for the buy-in to happen on all levels, from top management down to system users and developers. Positive net benefits such as cost, and time savings can be achieved from adopting information security as a goal along with direct business objectives.

Organizations should be more aware of threats and exploitable vulnerabilities in their information system assets. Theoretically, if one excludes the threat or vulnerability from risk calculation, there will be no more risk. From the reviewed standards it can be concluded that systematic risk management is a key information security process, because risk assessment and risk management are prerequisite for selection and implementation of security controls. One cannot select and implement controls effectively without understanding the risks. Risks also include the future risks that cannot be derived from the past which requires an external attacker to simulate future risks.

Elimination of all risks has proven to be impossible. Therefore, identification of emerging threats and response to them is of paramount importance in dynamic field of information security. Real world attack simulations can be used to test organizations security matureness, especially on technical level. This calls for actionable intelligence, funding, capabilities and trusted security experts to conduct testing. (Caron, 2019)

In the following chapters the relationship of threats, risk management and red teaming will be explored in the framework of information security. At this stage a justifiable assumption can be made that recognition of threats is a key driver for better information security.

In the NIST Special Publication 800-53 (2013) the word "life cycle" appears 77 times. On 56 occasions it relates to the importance of integrating information security and security controls already during the information system development. Information security risk management process should be integrated into system development life cycle.

Some key terminology and distinctive phases on building and maintaining information security are reoccurring among the literature. Therefore, a comparison matrix is presented on the table below. This table was created to elaborate the information security and risk management terminology and find similarities and differences of information security and risk management processes. Phases from different sources are in the same order as presented in the original documents. Therefore, the rows are not comparable by substance due to differing scope of the source documents.

TABLE 3 Information security and risk management terminology matrix.

Phase	Knapp et al. (2009) Comprehensive ISPP	Raggad (2010) information security lifecycle	ISO 27001 (2013)	NIST SP 800-53 (2013)	A risk management standard (2002)
1	Risk assessment	Security planning	Leadership, roles and responsibilities	Categorize Information Systems	Organisation's Strategic Objectives
2	Policy development and approval	Security analysis	Planning of security objectives	Select Security Controls	Risk Assessment

3	Policy awareness and training	Security design	Resources, awareness and communication	Implement Security Controls	Risk Reporting and decisions
4	Policy implementation and Monitoring	Security implementation	Operation	Assess Security Controls	Risk treatment and residual risk reporting
5	Policy enforcement	Security review	Performance evaluation	Authorize Information Systems	Monitoring
6	Policy review and cyclic nature of the process model	Continual security	Continual improvement	Monitor Security Controls	Continuous and developing process

Conclusion is that information security, whether looking at the overall effort or the policy development, should be cyclic by nature, risk driven and closely related to business objectives. Fusion of the comparison matrix is presented in the figure 15. below.

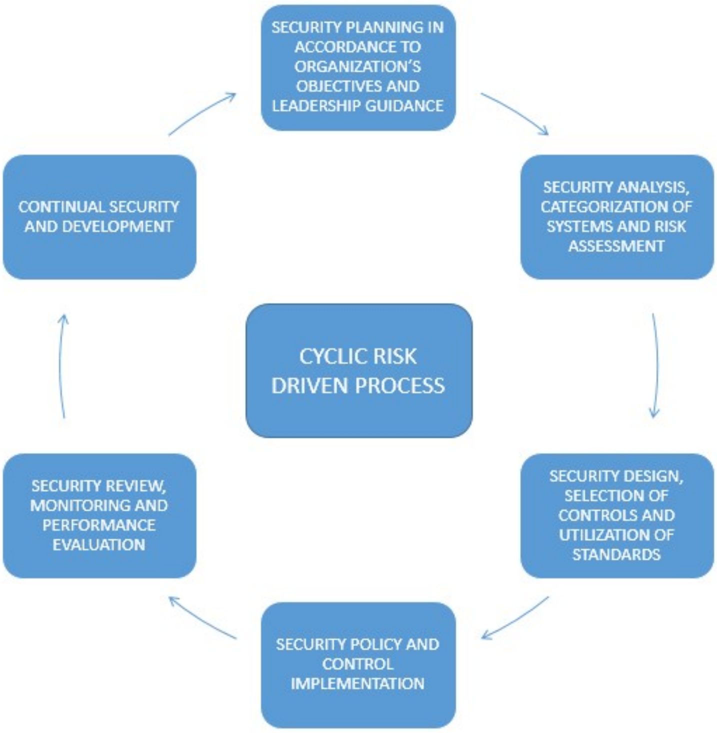

SECURITY PLANNING IN ACCORDANCE TO ORGANIZATION'S OBJECTIVES AND LEADERSHIP GUIDANCE
SECURITY ANALYSIS, CATEGORIZATION OF SYSTEMS AND RISK ASSESSMENT
SECURITY DESIGN, SELECTION OF CONTROLS AND UTILIZATION OF STANDARDS
SECURITY POLICY AND CONTROL IMPLEMENTATION
SECURITY REVIEW, MONITORING AND PERFORMANCE EVALUATION
CONTINUAL SECURITY AND DEVELOPMENT
CYCLIC RISK DRIVEN PROCESS

FIGURE 15 Cyclic risk driven information security process.

In the following chapters red teaming is introduced and defined in context of cyber security and information security. Red teaming will be reflected to the comprehensive organizational level process by Knapp et.al (2009), with an addition that information security is cyclic, and risk driven.

4 RED TEAMING IN CYBER SECURITY

"Everyone has a plan until they get punched in the mouth."

- *Mike Tyson –*

This chapters' title mentions cyber security, even though chapter 3 is about information security. These two terms are overlapping and not totally analogous. Information security as a term does not always cover all the aspects that cyber security does and vice versa. (Von Solms & Van Niekerk, From information security to cyber security, 2013). The combining factor is that both use information communication technology (ICT). Information security might handle assets that are not computerized and cybers security can handle non-information-based assets which are vulnerable to attacks but are stemming from the use of ICT. Example like cyber-bullying where CIA-triad is not compromised in any way, but the bullied person is via ICT. (Von Solms & Van Niekerk, From information security to cyber security, 2013)

This is a descriptive chapter which builds to the environment and knowledge base sections in information systems research framework (Hevner et al., 2004). In the design science research methodology process this chapter comprises a part of phase 2; defining objectives of a solution by introducing cyber security, advanced persistent threats, penetration testing and bug bounties. Part of phase 3; design and development of the construct (Peffers et al., 2007) is also covered along with exaptation in DSR knowledge contribution framework, which means extending known solutions e.g. red teaming to problems i.e. information security management (Gregor & Hevner, 2013).

US's Director of the national intelligence has defined cyber threats as the first in their list of global threats in its worldwide threat assessment 2018 (Director of the national intelligence, 2018). Nowadays cyber threats are widely studied and recognized as one of the main elements in modern cybercrime by EUROPOL (EUROPOL, 2018).

Advanced persistent threats (APT) as a term has surfaced around 2006 (Binde et al, 2011) and the attackers are constantly developing their techniques and adapting to defences (Daly, 2009; F-Secure, 2018). This makes the external attackers to be important topic to be viewed. Sophisticated insider threats started to draw attention in the same time also (Duran, Conrad, Conrad, Duggan, & Held, 2009; Willison & Siponen, 2009) forcing the defender to turn attention to inside the organization as well. These are the reasons that red teaming is needed in cyber security to emulate the modern attacker and create better technical protection, processes, response actions and training to mitigate evolving cyber threats from inside and outside.

4.1 Cyber-attacks and advanced persistent threat

The history of cyber-attacks is a controversial topic and is related to how one defines the term "cyber". Some claim that first cyberattacks were committed over 100 years before computers were even invented in a French telegraph network (Dilhac, 2001) because they define cyber with wider perspective than computer aided information systems like Von Solms & Van Niekerk (2013) do.

The Blanc brothers in France used bribes to infiltrate their messages through the national telegraph system for financial gain in year 1834 (Solymar, 1999). The messages were mixed inside the normal communication. Therefore, some say them being the first hackers (Solymar, 1999). The term "cyber" is controversial in nature and has countless of definitions. Still, definition is needed because several sources of this study use the term. In this study, the term cyber will mean something of information communication technical (ICT) and networked according to more traditional Merriam Webster's definition; *"of, relating to, or involving computers or computer networks (such as the Internet)"* (Merriam Webster, 2019) or Oxford's *"Relating to or characteristic of the culture of computers, information technology, and virtual reality"* (Oxford dictionary, 2019) or Cambridge's living dictionary; "involving, using, or relating to computers, especially the internet" (Cambridge University Press, 2019) With these definitions of the term cyber, the history of cyber-attacks is as old as the Internet which is also controversial because malware could propagate before the internet via other media as well, but for the sake of this study this definition of cyber is used.

Clifford Stoll published an article "Stalking the wily hacker" in 1988 (Stoll, 1988) where he describes a long duel against a hacker which started in 1986 Lawrence Berkeley Laboratories and ended up to Germany. The noted espionage campaign was targeted mostly against US military institutions and government contractors. During the duel attacker tried to break into more than 450 computers and successfully compromised more than 30 (Stoll, 1988). Stoll later published a book about this long cyber espionage campaign, known as the Cuckoo's egg. Traces to this campaign led to Soviet Union and its intelligence organization KGB (Stoll, 1989). This was most likely not the first cyber-attack in the history, but at least it is well documented case of an *"persistent computer intruder"* as Stoll (1988) named the adversary in his article. Term "advanced persistent threat" has also controversy of its first use in relation to computer threats but in 2006 it was used by United States Air force analysts (Binde et al., 2011) and thus the term is more than 10 years old and nowadays in large scale use throughout cyber security forums.

In this research comprehensive red teaming is addressed which includes the complete security life cycle according to Knapp et al. (2009) presented in chapter 3. This is the reason that the adversary emulation should be considered more like an advanced persistent threat actor which has the capability for following;

- Advanced - conversant with intrusion tools and techniques and possibility to develop own zero-day vulnerabilities.
- Persistent - intends to accomplish a mission with a long-term campaign with repeated attempts.
- Threat - organized, funded, motivated and they have intention and means.

These are the basic attributes for any advanced persistent threat actors (Binde et al., 2011; Chen et al., 2014; Vukalović & Delija, 2015). APT-studies have started to appear in mass ever since with the renowned kill chain article *"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"* by Hutchins, Cloppert & Amin (2011). This article is one of the industry baselines and a well referred study. Since then hundreds of APT studies have been published with various topics.

Commercial cyber security organizations like Symantec (2011), Mandiant (now part of FireEye Inc) (2013), FireEye Inc. (2014), F-Secure (2015), E-ISAC (2016), PwC UK-BAE (2017), Dragos (2017), and several others publish quality APT-studies which provide good insight about TTPs of various groups that can be used to facilitate red teaming in cyber security as adversary.

Several different variants of taxonomy of phases and mechanisms in APT attacks have been studied and the kill chain study presents the following seven phase model which is very technical in nature. This model helps the defender to understand the phases of attack and deploy countermeasures and techniques accordingly. (Hutchins et al., 2011)

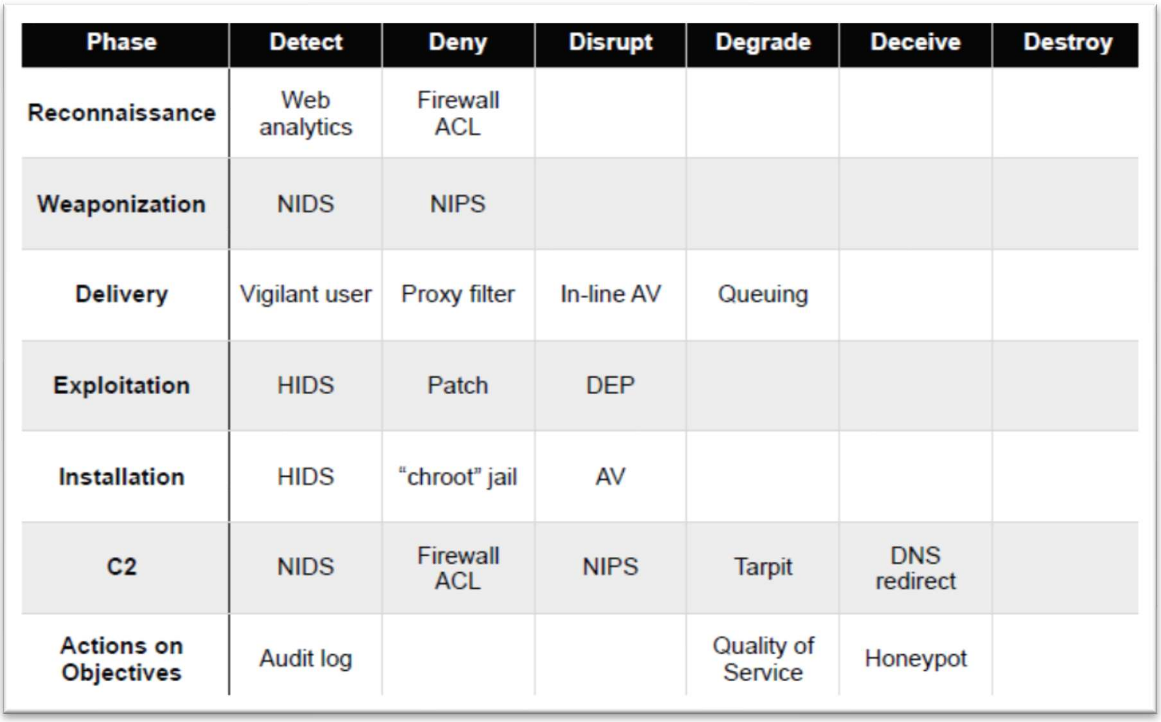
During reconnaissance phase, the attacker plans the mission and collects information and vulnerabilities from the target organization. Weaponization phase means creating malware that enables the attacker to gain access to the target system. (Hutchins et al., 2011)

The delivery phase starts the actual execution. Goal is to deliver the malware into the target system. Examples of delivery methods include phishing, customized web pages or USB - drives. After the malware is delivered to the target system, exploitation triggers the attacker's code. Most often, exploitation targets an application or operating system vulnerability. (Hutchins et al., 2011)

Malware is installed in during the installation phase. Malware can be a script or a hidden backdoor or a rootkit that allow an attacker to access and operate the target system or exfiltrate data. Installation of malware on the target system allows the adversary to maintain presence inside the environment. (Hutchins et al., 2011)

In the command and control phase, the attacker establishes a command channel to the target system. Malware usually contacts the attackers command server. Malware enables the attacker to have persistent access. Hence the term advanced persistent threat. (Hutchins et al., 2011)

Action on objective means that the attacker is now able to commit the actions planned in the target system. Objectives might include spying, data exfiltration, denial of service or other actions. (Hutchins et al., 2011)



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

FIGURE 16 Phases and Courses of Action Matrix (Hutchins et al., 2011).

Chen et al. (2014) used this model to study APT attacks from 2009 to 2014 and found support for the model. Other researchers like Vukalović & Delija (2015) have tried to create more general and commercial companies have also participated in the production of their own kill chain variants (Mandiant, 2013; E-ISAC, 2016; PwC UK and BAE, 2017) and there is a plethora of choices in use.

Important factor that has been studied is that APT threats are not completely dependent on technology and computers. The human factor in cyber security needs to be under scrutiny as well because the entry vector in several cases is the ignorant human through phishing or spear-phishing (Molok, Chang, & Ahmad, 2010). Social engineering has emerged as an art to exploit the human factor in security (Krombholz et al, 2015). Human factor also brings the insider threat approach which according to research constitutes approximately 30% of breaches. (Willison & Siponen, 2009; Duran et al., 2009; Moore, 2010) Physical security is also a part of good cyber security because physical access to a device can ease the cyber-attack tremendously (Dimkov, Van Cleeff, Pieters, & Hartel, 2010).

APT-research is mostly focused on analysing already identified campaigns which is a good approach in recognizing patterns and TTPs (Ghafir & Prenosil, 2014) (Chen et al., 2014). This is still not a fully functional way in looking at the future threats and then other approaches are needed such as war gaming to simulate the future. The threat environment is increasing so rapidly that there is no possibility to enumerate even the current threats and build defences. Therefore, generic threat matrixes are needed for defence and they can also be used in red teaming to simulate a certain threat. (Duggan, Thomas, Veitch, & Woodard, 2007)

Gaming theories have also been adopted in a study that investigated the joint threats from APT attacker and insiders. The interplay among defender, APT attacker and insiders was supported by a game theory (Hu, Li, Fu, Cansever, & Mohapatra, 2015). This kind of research combined with threat matrixes starts creating links between APT-threats and adversary emulation of red teaming and threat intelligence.

4.2 Red teaming studies and activities

To mitigate the various APT or insider attack the research of red teaming has surfaced in multiple ways. Red teaming in the information systems or cyber security has been a keen interest for militaries, researchers and commercial companies for over two decades now (Fleming, 2010). In year 1996 the Sandia national laboratories founded their Information Design Assurance Red Team (IDART) (Sandia national laboratories, 2000). Wood & Duggan (2000) published one of the first process models for red teaming under SANDIA umbrella in 1999. This method includes team building, system assessing and attacking, and reporting to the customer. Since then IDART has been evolving for over 20 years and its focus is risk-informed design assurance & vulnerability assessment for infrastructure, traditional cyber systems, and non-traditional cyber-physical systems. IDART is nowadays a NIST-recognized method in SP800-115 (NIST, 2009) technical guide to information security testing.

United States has most likely the longest experience in militarizing cyber. The first known red teaming exercise “Eligible receiver 97” in the Department of defence was held in 1997 when NSA red team acted as the aggressor towards the DOD (George Washington University, 2018). This exercise was a wakeup call for the DOD since the red teams were so dominant over the blue teams. Cyber red teaming started to gain momentum in the US since early 2000 (Kaplan, 2016) and has been developed heavily since. Nowadays NSA and USCYBERCOM are very skilled in cyber warfare and they are certifying and accrediting other red teams in DOD (US Navy, 2018).

Red teaming research does not limit to technological studies. Team dynamics have been studied by how attacking hackers operate in groups (McCloskey & Stanard, 1999) and commit attacks. SANS institute published as early as 2003 the paper: “Red teaming – The art of ethical hacking” by Chris Peake (Peake, 2003) where red reaming is still seen from a narrow view belonging only to the assessment stage of the Information security lifecycle. Whereas newer studies consider red teaming to cover broader perspective from attack trees, threat modelling, collaborative working and even automating and structuring attacks (Ray et al., 2005) to two sided games with different models proposed (Veerasamy, 2009).

The bestseller book; Art of deception (Mitnick & Simon, 2003) brought the social engineering to knowledge of wide audiences. Social engineering studies have emerged, and several trust and attack models have been studied to create better attacks and defences (Laribee, 2006). Social engineering attacks include physical, social and technical aspects which are combined to form either the attack or prepare for it (Krombholz et al, 2015). Attack methodologies and processes have evolved like environment and custodian focused methods which have been also tested in practice (Dimkov et al., 2010). Social engineering can be seen now as one of the prerequisites in conducting a good preliminary intelligence or a breach in red teaming efforts.

Red teaming studies have been broadened to involve game theories (Hu et al., 2015) to red teaming or simply simulate the efforts completely using sophisticated programs (Tan, Porter, Tele, & West, 2014) to support efforts. Modern study involves artificial intelligence solutions like Trogdor. Trogdor is an automated cyber red teaming (ACRT) defensive decision support system that generates attack graphs for known vulnerabilities in modelled networks. (Randhawa, Turnbull, Yuen, & Dean, 2018) There is also scepticism towards modelling and simulation and Skroch (2009) claims that simulations do not replace red teams but it augments practice by providing tools to both analysts and red teams and can utilize red team knowledge and apply it with less expense than live red teams.

The maturity of a domain can be thought of reaching a certain level when it turns to self-evaluation. This has happened to red teaming research as well. Red team performance and effectiveness has been studied and problem has been the confidential nature of red teaming efforts which has prevented documentation of best practices (Kraemer et al., 2004). Team effectiveness in cyber exercises have been studied to better the achievements of red or blue teams (Granåsen & Andersson, 2016). A dissertation case study (Fleming, 2010) about several red teams including the IDART was completed and the conclusion was that the cyber red teaming was the most developed compared to other disciplines. Research about the processes, organisational, legal and technical considerations of military red teams have been conducted and published like Cyber Red Teaming by Nato Cooperative Cyber Defence Centre of Excellence (Brangetto et al, 2015) which emphasizes that a framework of red teaming needs to be created to formalize the red teaming process.

Red teaming is not an audit mechanism per se, but sometimes it can be used to comply to standards and it can be an effective way to gain relevant audit evidence (Caron, 2019). Comprehensive red teaming efforts including social engineering and physical security checks create important training opportunities as well increase in security awareness. Cyber incident and recovery processes can also be practiced with red team testing (Caron, 2019). Several commercial companies offer red teaming services with various service portfolios ranging from penetration testing to complete service packages including security consulting and auditing. Some companies have extensive training environments to simulate clients' environment for training events without compromising the production environment. Five companies that operate in Finland were selected for their different background in red teaming to participate in this study and develop the comprehensive red teaming framework.

4.3 Penetration testing and relation to red teaming

The aim of penetration testing and red teaming in general can be viewed as the same, as they are both focused on uncovering vulnerabilities and patching them. Difference is in the scope and time. Whilst penetration testing can be made against application, service, machine or a building (Bishop, 2007), red teaming is deemed more comprehensive and looks at the entire security life cycle and processes as well. (NIST, 2013b). According to NIST, penetration testing is a sub category of red teaming by the following definition;

> …Red team exercises extend the objectives of penetration testing by examining the security posture of organizations and their ability to implement effective cyber defences. As such, red team exercises reflect simulated adversarial attempts to compromise organizational mission/business functions and provide a comprehensive assessment of the security state of information systems and organizations. (NIST, 2013b)

Penetration testing is defined by NIST as follows;

> The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components. Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the information systems that are the targets of the penetration testing. (NIST, 2013b)

The line between penetration testing and red teaming is thin in practice and in the field of research. Terms penetration testing and red teaming are used and interpreted by the authors differently. Veerasamy (2009) presents in his paper a *"High-level Methodology for Carrying out Combined Red and Blue Teams"* which is purely technical even though it consists of two teams. This can be considered narrow scope red teaming or wide scope penetration testing. There are also several methods in this field like *"The Penetration Testing Execution Standard Documentation (PTES)"* (PTES, 2014) which is a very comprehensive and includes social engineering, physical security, threat modelling and business asset analysis as well. Therefore, this could be interpreted more to the side of red teaming. Various other models include OSSTMM, ISSAF, NIST SP800-42 and OWASP testing guide which all have different features and taxonomies (Bertoglio & Zorzo, 2017).

There are also vast repositories of technical tooling available both commercial and open source, like the Github-page *"Awesome red teaming"* (R0lan,

2018) which constitutes completely on technical penetration testing issues. Several discrepancies in usage of terms can be found in the field of cyber security. Mitre has it's vast technology and method bundle known as Mitre ATT&CK framework which consists several cyber-attack TTPs (Mitre, 2018). Mitre does not refer to its framework neither as penetration testing or red teaming and the terms are not used.

Penetration testing is usually classified in three categories; white-box, grey-box and black-box testing depending on the amount of information that the testers receive. In black-box testers receive the product without documentation and in white testers receive all the material available. Grey-box testing usually gives testers a basic package that could be easily gathered from open sources to speed up the testing. (Bertoglio & Zorzo, 2017)

Several different techniques can be utilized in penetration testing like static application security testing (SAST) which focuses on the examination of the source code (Antunes & Vieira, 2009) and is also divided in static and dynamic code analysis (Curphey & Arawo, 2006). Dynamic application security testing (DAST) inspects the attack surface of a system while running (Diamant, 2011). Interactive application security testing (IAST) combines the running environment with the source code examination which makes it a more effective method in some cases (Stuttard & Pinto, 2008; Bau, Bursztein, Gupta, & Mitchell, 2010). Fuzzing is a black-box technique that attempts to crash systems by sending malformed input to target. This can also be used in testing of applications. (Takanen, Demott, Miller, & Kettunen, 2018). All these techniques can be applied in development and in production phase and it's difficult to classify something as a testing or penetration testing technique. Penetration tests provide value to the vulnerability identification and patching them whether in production or development.

Penetration testing is used as one testing method in secure development. A secure software development lifecycle (SDLC) which have been Microsoft's implementation of the secure development has evolved since early 2002. SDLC aims to address software security throughout the entire software development process, from before specifications are developed to long after software has been released (Lipner, 2014). The SDLC methods has been developed constantly to mitigate vulnerabilities as early as possible in the development process (Glumich, Riley, Ratazzi, & Ozanam, 2018). There still are prejudices amongst executives that want to see a convincing cost/benefit argument before adapting to more costly and slower development process (Geer, 2010). Customers demanding more for security will likely improve the security attitudes of corporations (Geer, 2010).

Based on the perceptions in this chapter it can be concluded that the research and definitions for penetration testing's relation to red teaming aren't fully defined universally. For the sake of this study; penetration testing is defined as a type of technical adversary emulation which is a subcategory of red teaming.

4.4 Bug Bounties as crowdsourced penetration testing

Bug bounties are easier to define. They are crowdsourced mostly technical penetration tests (Maillart, Zhao, Grossklags, & Chuang, 2017). The reduction of bugs from code is known as debugging during program development. If debugging fails during production, bugs remain in the production system which might cause vulnerabilities.

Donald Knuth is considered the father of bug bounties. Knuth created the TeX© typesetting system in 1978 (Knuth, 1989) wrote a book "The Art of Computer Programming". Knuth offered a 256 cent (which is a hexadecimal dollar, scientist humour) bounty for anyone who can point out flaws in his work. Then Knuth promised that he will double the bounty every year the system is in use. In 1989 Knuth had already received 865 reports of bugs and flaws which he fixed, and the bounty was 81.92 $ per bug during that time. Knuth was also joking that hopefully the bugs will disappear because he can't afford to pay 83,886.08$ in 1997 per bug. (Knuth, 1989) Knuth basically crowdsourced peer reviews for his articles and work. The bounty program has ceased as such.

Böhme (2005) presents how economic perspective started to get companies interested about bug bounties as they saw it reducing bad quality material which had to recalled from market. Hackers also started to find vulnerabilities which they did not submit to the vendor or vendor wasn't interested in buying. This accelerated the birth of vulnerability markets and vulnerability brokers who sell vulnerabilities to highest bidders. (Böhme, 2005) Bug bounties cannot still be held responsible of creation of these criminal activities like bug auctions even though there are studies that indicate them being more profitable to bug hunters than regular bug bounties. Companies like Zerodium are buying and selling vulnerabilities. For example, while Apple offers a maximum 200k USD bounty, Zerodium purportedly offers 1.5 million USD for certain iPhone jailbreaks (Breindenbach, Daian, Tramèr, & Juels, 2018). The vulnerability markets also exist due to problems in disclosing vulnerabilities that may lead to legislative sanctions towards bug hunters and therefore they turn to illegal vulnerability markets (Kesan & Hayes, 2016; Algarni & Malaiya, 2014).

Bug bounties started to gain momentum after 2000 and research also developed. Bug bounty scene wasn't very developed, and it was the interest of security researcher and hackers or even the end-user to submit bugs or vulnerabilities. Just, Premraj & Zimmermann published an article *"Towards the next generation of bug tracking systems"* (2008) where they studied bug reporting among several hundred developers and web projects and decided to create recommendations for the design of bug tracking systems. Several companies run these independent bug bounty programs nowadays such as Facebook, GitHub and PayPal (Zhao, Grossklags, & Liu, 2015).

Bug bounty companies that offer bug bounty platforms have also surfaced around 2010 such as Wooyun, HackerOne, BugCrowd and Cobalt (Zhao et al., 2015). These companies create the platform and organization for managed third part bug bounty and the customer does not have to deal with several hackers or researchers. These ecosystems have been growing rapidly (Zhao et al., 2015). The strength of bug bounty companies come from hacker community. Companies do not hire many permanent employees, but they channel the community's talent.

Masses don't always mean success. Wooyun had almost 8000 hackers at their roster in 2015, but 3725 have found only one vulnerability. The best hacker submitted 521 vulnerabilities and the top 100 have published average of 147 reports per person. (Zhao et al., 2015) There is also evidence that professional security researchers face challenging difficulties when trying to uncover bugs in large bounty programs. Maillart et al. (2017) discovered that the launch of new bug bounty programs might even have negative effect on incumbent programs regarding bug submissions. Development in bug bounties has led to the automation of bug detection and disclosure systems (Breindenbach et al., 2018; Calvi & Viganò, 2016).

There is a valid question on who should companies use? Professional security team or a bug bounty program. Bug bounty may prove to be cheaper but are they better than professional teams. Finifter, Akhawe & Wagner argues that (2013) their *"Empirical Study of Vulnerability Rewards Programs"* proves that two case studies with Chrome and Firefox appear economically efficient and consider bug bounty better than the cost of hiring full-time security researchers which slightly contradicts Zhao et al. (2015). Both ways have their advantages and it will take considerable amount of additional research to reach a credible answer.

4.5 Implementing red teaming into information security management

Information security management with risk analysis, several standards and a comprehensive policy process model were introduced in chapter 3. Implications for implementing red teaming efforts to ISM practice were derived through content analysis of chapter 2, 3 and 4 and presented in the table 4. later as suggestions how red teaming activities could support the different phases or main categories of the comprehensive information security policy process model by Knapp et al. (2009). These results are by no means conclusive but they build for the application for environment and addition to knowledge base in the IS research framework (Hevner et al., 2004).

Information security governance is the key in adopting the red teaming effort. This calls for transparency and critical review of current state and the courage to subject the organization to red teaming. This is not a technical question, but a cultural one (Defense Science Board, 2003).

Information security office's structure can benefit from red teaming when offence and defence are mixed. Adopting the purple team thinking supports the defensive processes and enables better red teaming efforts (Erridge, 2018) (Oakley, 2019).

Interlinkage with red teaming and risk management is recognized to identify security gaps in ever-changing threat environment with various techniques (Caron, 2019). Red teaming can give additional perspective for risk assessment (Cavusoglu et al., 2008) presenting possible future threats which cannot be derived from history (Baskerville, 1991) that might be missed in regular risk analysis.

Policy development if immature can benefit from outside review. Policy development should always start with review of the current policy and its shortcomings. Main support to policy development comes from the results of red teaming efforts that derive from risk assessment and concrete results. Bringing users to participate to the building of better policies creates acceptance for policy approval as well (Spears & Barki, 2010).

The training and awareness are key drivers in implementing the policies (Knapp et al., 2009). When red team acts as adversary and finds weaknesses in processes, these must be also corrected. Wargames and simulations are an effective way to create training scenarios (Davis, 1962) and build awareness (DHS, 2004). Awareness is one of the factors in mitigating risks in organizations (The Institute of Risk Management, 2002; Caron, 2019). Training and awareness support the policy implementation through learning.

Monitoring is tested with red teaming attacks. The level of monitoring cannot be tested if red team never gets caught. Therefore, during the testing if defender cannot see developed attacks, it can be beneficial to cause in the end some attacks that are noted which displays the level of monitoring and helps to plan for better controls.

Policies do not always create effects and sanctions might not always be effective though they are the usual method (Johnston, Warkentin, & Siponen, 2015). The demonstrated intervention effectiveness of the policies needs to be addresses as well (Siponen & Baskerville, 2018). The enforcement of policies can be sanctions or rewards. It should be reviewed and studied how these affect the security and adjust the enforcement accordingly (Knapp et al., 2009).

Existence of external and internal threats needs to be considered in every step of the security cycle. There are also other factors than threats to be considered like organization culture and its effects on policies. (Knapp et al., 2009)

There is no silver bullet for every organization. Different assurance and compliance factors need to be considered as well. These factors could be better noted from unbiased red team that helps to overcome biases and mitigate group thinking and reduce noise with adaptation of procedures that promote consistency and impartiality. (Tversky & Kahneman, 1974; Kahneman et al., 2016)

Last topic is the cyclical nature of policy management. This is also the nature of red teaming. Red teaming must be a continuous process because the threat environment is changing all the time and future attacks evolve constantly.

TABLE 4 Red teaming possibilities in support of information security.

ISPP AREA	Red teaming activities
Information security governance	• Red teaming as a strategic level support tool and a way to critically evaluate the focus, scope, objectives and governance of corporation security. • The need to merge red teaming into organization is imperative.
Information security office	• Critical review of company's security office and processes. • Taking security officers along RT engagement to present them the flaws in real time. • Red team liaison needs to be attached to office (Purple teaming).
Risk Assessment	• Bringing the RT findings to support risk assessment. • Making the threats and vulnerabilities visible which leads to evaluation of consequences. This forms the foundation for corrective actions.
Policy Development	• Critical review of existing policies. • Support in creation of policies that can be adopted, and which take into consideration findings from risk assessment and RT. • User participation to build comprehensiveness
Policy Approval	• Critical review of the internal and external effects the policy may have when implemented.
Awareness & Training	• Bringing the notions from RT engagement into awareness programs and creation of training events to all levels of staff. • Employees need to be trained against newly found threats in different wargaming possibilities.
Policy Implementation	• Support in developing and implementing both technical and managerial controls. • Testing of controls prior to deployment.
Monitoring	• Adversary emulation and penetration testing to expose gaps in the systems and policies. • Red team enough, not too much → get caught sometimes.
Policy Enforcement	• Review of the effectiveness of sanctions and rewards • Modifications on sanctioning and rewarding
Policy Review	• Critical review of company policies and support to update based on findings from monitoring and red teaming.
External Influences	• Reviews about competitors and future technologies. • Evaluating effects of changing standards or compliance requirements affecting the corporation. • External threat emulation and threat matrixes.
Internal Influences	• Critical review of the senior management support, business objectives and organizational culture. • Possible flaws and vulnerabilities in the systems to be penetration tested. • Internal threat emulation and threat matrixes.

All aforementioned areas can benefit from red teaming. Comprehensive process model for red teaming that can support the whole information security lifecycle, with taking into consideration various standards, is the goal of this study. These results are used in the model creation in chapter 8.

The red teaming effort does not limit to attacking but must cover the entire information security lifecycle. This is supported by the concept of dividing red team activities into diagnostics, challenge and creative phases (Development Concepts and Doctrine Centre, 2013). Following phases were created and defined to describe the red teaming effort in information security environment for the survey-phase of this research.

- Pre-engagement phase - Activities that are conducted before the actions against customer are initiated. This could be for example marketing, setting the scope, forming your team, planning the tasks and schedule, etc.
- Engagement phase - Activities that start after signing a deal with the customer. Includes planning, information collection, team leadership, infiltrations, attacks, etc. Engagement ends when activities against customer cease.
- Post-engagement phase - Activities such as analysing the results, writing the reports, briefing of results to customer and possible corrective measures conducted together with customer.

Donald Knuth, the founder of TeX© elaborates his working style by claiming *"I make mistakes. I always have, and I probably always will. But I like to think that I learn something, every time I go astray"* (Knuth, 1989). This can be considered the basic idea of submitting oneself to bug bounties, penetration tests and red teaming.

4.6 Conclusions from red teaming in cyber security

Comprehensive red teaming was introduced in chapter 2 with various examples. Chapter 3 described the environment of information security management and chapter 4 introduced red teaming in information/cyber security environment. The relation with red teaming, penetration testing and bug bounties were defined. Red teaming being a complete tool set in creating better plans, policies and procedures in any domain by questioning the current ones. Penetration testing is a part of red teaming that is used in adversary emulation whilst bug bounties are crowdsourced technical penetration tests.

This study has added to the fact of complicated nature of information security research and how red teaming fits to the research genre. The interlinkage of red teaming and support to risk management was displayed clearly through adversary emulation approach. The scope of red teaming can also vary in tiers as depicted in chapter 2.5. and NIST SP 800-53 (NIST, 2013b) from organization level red teaming to processes and all the way to the information systems as depicted below in figure 17.

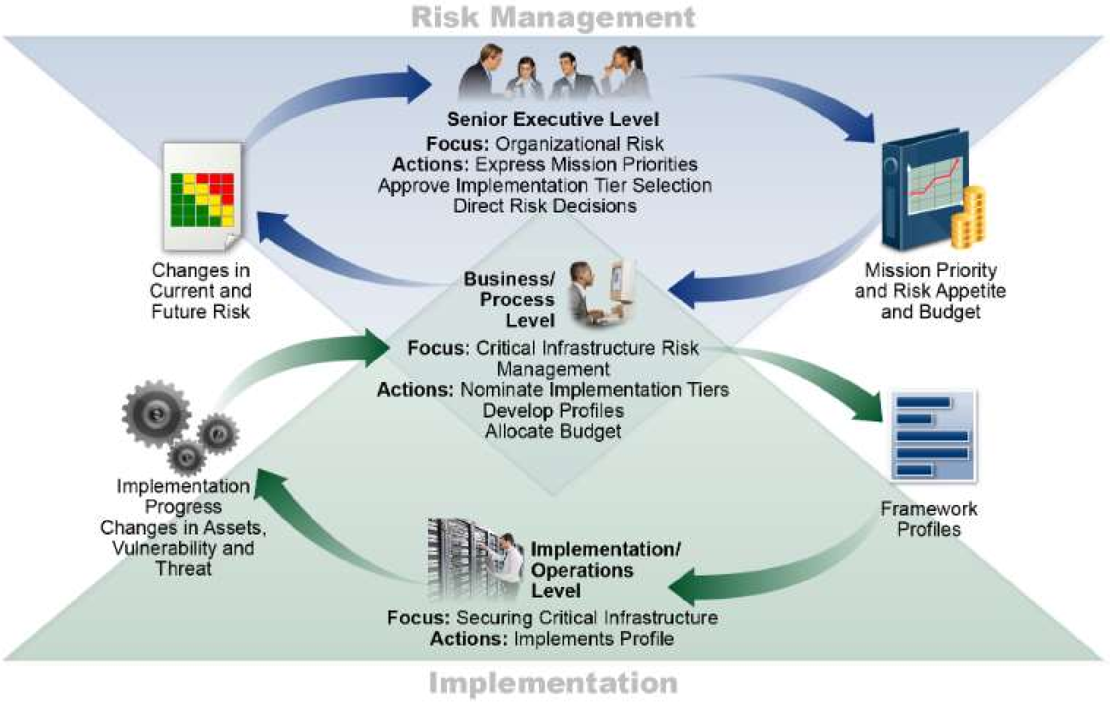

Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

FIGURE 17 Risk management and implementation relations. (NIST, 2017)

Red teaming research scope should be broadened in the information security research. Red teaming has been considered in many cases just as adversary emulation disregarding the training support and critical reviews of several issues that are not computerized but affect the security landscape such as organizational culture or psychological factors. On the other hand, APT research supports red teaming activities as well in creating threat matrixes for attack simulation (Duggan et al., 2007). The possibilities of adopting red teaming actions into information security management were described in chapter 4.5, table 4. This study has presented so far, several ideas how the usefulness of red teaming could support the information security research community.

Now there is an understanding and an idea of implementing red teaming comprehensively to information security. Next step is to start turning the red teaming into an understandable process, service or a product in the scope of this study. The next phase is supported by several military methods and agile methodology. As Govindarajan & Trimble (2010) phrased in their bestseller book; The other side of innovation: Solving the execution challenge. *“Without execution, Big Ideas go nowhere”*

5 ADAPTIVE PLANNING AND EXECUTION FRAMEWORK

"In preparing for battle I have always found that plans are useless, but planning is indispensable."

- Dwight D. Eisenhower -

This is a descriptive chapter which builds to the knowledge base section in information systems research framework (Hevner et al., 2004). In the design science research methodology process this chapter comprises a part of phase 2; defining objectives of a solution and enables phase 3; design and development of the construct (Peffers et al., 2007). This chapter also adds to exaptation in DSR knowledge contribution framework, which means extending known solutions e.g. adaptive planning and execution to new problems i.e. red teaming in the information security management (Gregor & Hevner, 2013).

This chapter describes the adaptive planning and execution (APEX) framework which includes four operational activities (OA), four planning functions and seven execution functions intended for national level military policy decision-making (US Joint Chiefs of Staff, 2017). Part of the APEX framework is depicted in figure 18. below. Intelligence and targeting are presented due to their relevance for the research.

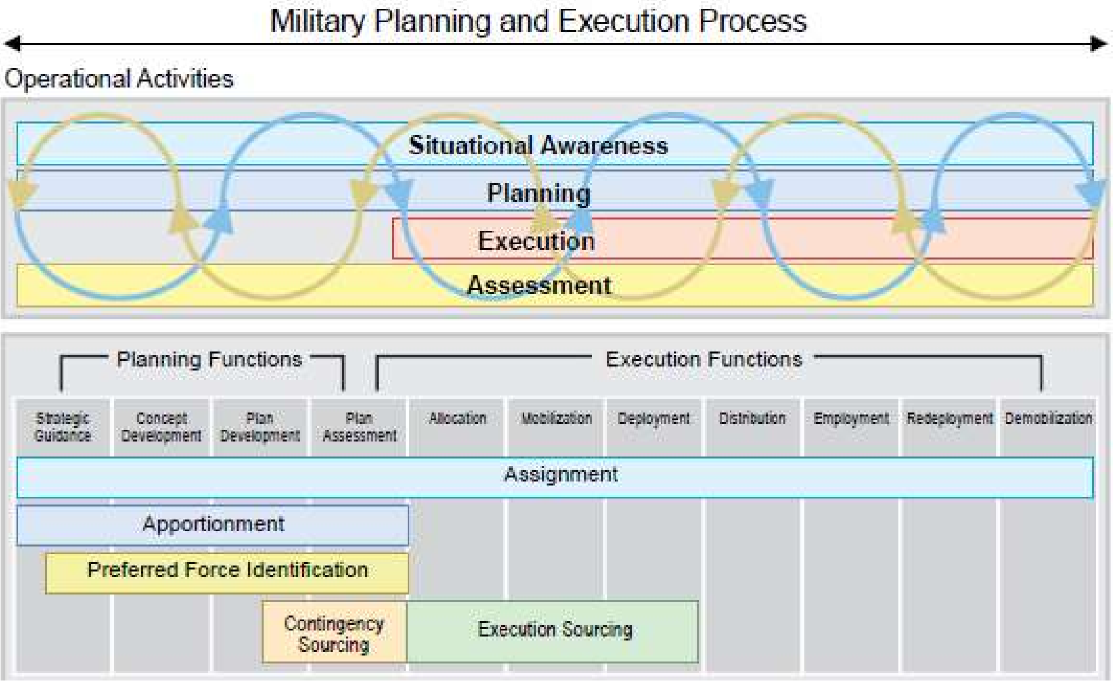


FIGURE 18. Planning activities and functions. (US Joint Chiefs of Staff, 2017)

Operational activities are continuous cyclical processes and produce products constantly such as plans, orders and reports. Some products are tied to different phases of the APEX framework which are known as functions. (US Joint Chiefs of Staff, 2017) For example, during concept development several concepts are produced which consider various force deployment possibilities. In the plan development function, they are combined and refined as a plan and contingency plans. During deployment plans are executed and troops are moving according to orders which are derived from the previous products such as plans, and more detailed products form previous steps. Intelligence reports are released constantly to build the situational awareness and support other activities. Activities commence continuously and simultaneously in order to support decision making. Intelligence provides inputs for all the framework activities. (US Joint Chiefs of Staff, 2017) Intelligence is a larger entity than situational awareness which is explained in detail in the intelligence and targeting chapter.

The interdependent and overlapping nature of continuous activities is described in the figure 19. below. Three major branches are intelligence, operations and planning (US Joint Chiefs of Staff, 2013b), which all have designated staff. Planning gives guidance and objectives for the other branches. These include requirements for intelligence and desired effects for operations. Assessment of own operations is also part of planning. Planning is supported by intelligence and operations staff. Intelligence branch gathers data from operational environment, produces intelligence products and supports in building situational awareness for the troops and targeting branch. Operations branch executes the plans with its capabilities (troops). (US Joint Chiefs of Staff, 2017; US Joint Chiefs of Staff, 2013b) Details will be elaborated later in this chapter.

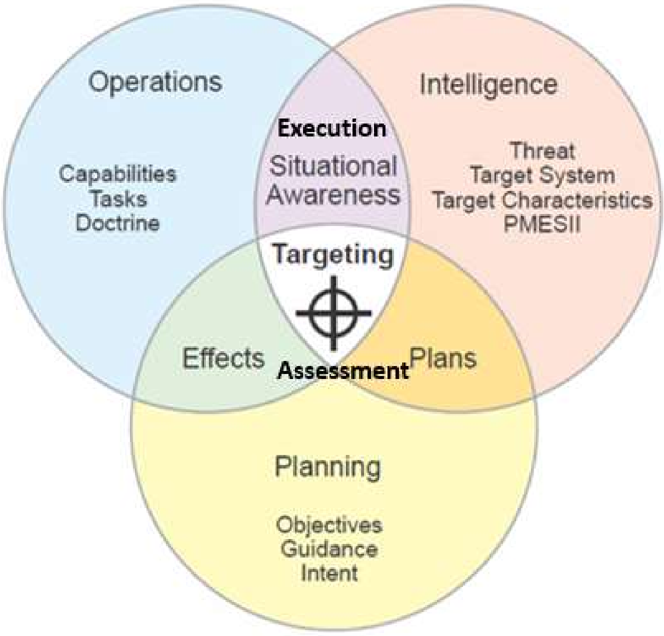


FIGURE 19 Interdependency of planning, intelligence and operations (US Joint Chiefs of Staff, 2013b); supplemented with execution and assessment.

This chapter is heavily referenced from military doctrines which are not considered as scientific research. Still their value as references is undisputed, because purpose of a doctrine is to describe the principles that enable military forces to pursue a common objective in coordinated and integrated manner. Best practices and lessons learned from operations have a strong influence on doctrine development, they are the guidebooks in waging a war. (US Joint Chiefs of Staff, 2018; US Joint Chiefs of Staff, 2017). Doctrines could be compared to standards which are derived from the best practices of the current field of information security studies.

5.1 Military planning

Planning is an activity that is conducted in continuous cyclical process which determines how to use capabilities or resources in relation to time and space to achieve objectives in future. Objectives are sometimes described as "ends", principles as "ways" and capabilities as "means". Planning should always identify an "end-state". End-state describes purpose of any given operation which is usually expressed as required conditions. Planning always takes into consideration the associated risks, and is based on realistic resources. Planning may be time compressed during emergent events to produce executable orders. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

When military planning process is examined in the context of problem-solving theory, a conclusion can be drawn that an analytical planning process is needed to support decision-making. Historical lessons from planning, and the psychological processes that human decision-makers need to consider, suggest that military planning process is an appropriate analytical model for successful decision-making. (Marr, 2001) Most common decision-making theories are rational, limited rationality, and rules-based decision making. (Runyon, 2004) Gotztepe and Kahraman (2015) acknowledge that military planning process can be extended to solve non-military problems. The need to mitigate beliefs, biases, noise and inconsistency during decision making in uncertain conditions has been a subject of research for more than four decades (Tversky & Kahneman, 1974; Kahneman et al., 2016). Enhancements to the planning process have been proposed by several researchers (Marr, 2001; Runyon, 2004; Moisescu, Boscoianu, Prelipcean, & Mariana, 2010; Gotztepe & Kahraman, 2015), this critique is discussed later.

Planning is conducted on different levels which are strategic, operational, and tactical. Strategic level planning provides military options for national security policy objectives. Operational level planning translates strategic guidance into specific military activities or operations with a specified end-state and sequencing. It is a link between strategic and tactical level. Tactical planning focuses on employment of forces in relation to each other, and the arrangement of battles and engagements. It solves complex problems on how to achieve objectives and accomplish tasks. Timeline of tactical planning is relatively shorter than of operational planning (US Joint Chiefs of Staff, 2017; US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Decisions are made based on the information and knowledge developed in the planning process. Key benefit of structured planning is to enable informed decision making, because planning identifies issues and assumptions, resource requirements, costs and cost-benefit trade-offs, and risks. Uncertain operating environment calls for adaptive and flexible planning methods. Therefore, planning must produce multiple feasible options for contingencies, which are different courses of action (COAs). (US Joint Chiefs of Staff, 2017) Planning also maintains orientation on future objectives during running current operations. (Department of the army, 2010b) Current operations are assessed continuously, which gives feedback to adapt planning. (US Joint Chiefs of Staff, 2017) This principle is part of joint planning activities and will be described more thoroughly in chapter 5.2 operations and execution.

Planning is usually done from general to specific. This means that concept of operations and the commander's intent provide the basis for detailed planning. Detailed planning focuses on intelligence, movement, fires, protection, sustainment, and command and control, which need to be considered for successful execution. However, conceptual planning must notice constraints from details as depicted in the figure 20. below. (Department of the army, 2010b)

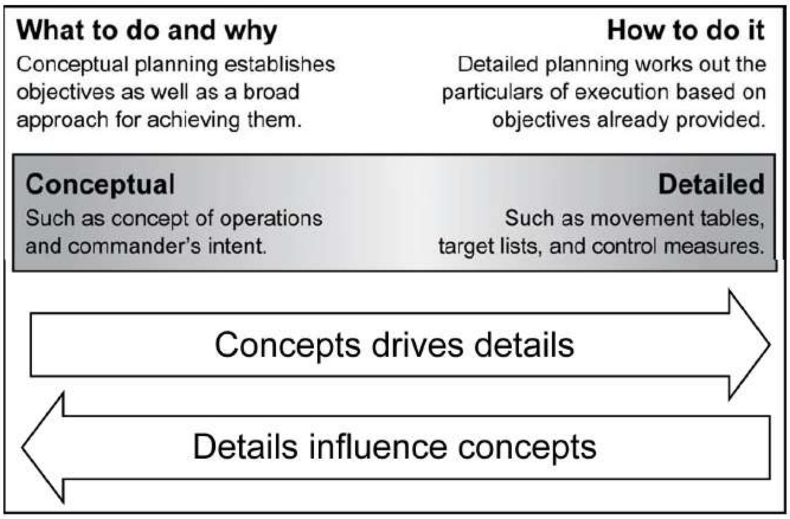

What to do and why
Conceptual planning establishes objectives as well as a broad approach for achieving them.
How to do it
Detailed planning works out the particulars of execution based on objectives already provided.
Conceptual
Such as concept of operations and commander's intent.
Detailed
Such as movement tables, target lists, and control measures.
Concepts drives details
Details influence concepts

FIGURE 20 The planning construct (Department of the army, 2010b)

In practice planning can be described as an arranged, analytical set of logical steps to define a problem, understand the situation, examine the mission and identify end-state. Alternative COAs are developed, analysed, and compared during the planning, from which a plan is produced. Planning also calls for identification of assumptions because rarely all facts are available. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Researchers acknowledge that sometimes decisions are based on beliefs which are related to likelihood of something uncertain to unfold. Fundamental problem is the subjective assessment of probability, since validity of data is limited. This leads to biased decision making. (Tversky & Kahneman, 1974) Consistency is an attribute that is expected from professionals in whatever they do. However, humans have proven to be unreliable decision makers because judgement is influenced by heuristics, and trivial factors such as mood and physical wellbeing. Variability on decisions is referred as noise by Kahneman et al. (2016). Strict work-related rules are the most common way to overcome noise. Practical method to overcome noise is to use formal methods and checklists for information collection and its application to problem solving and decision making. (Kahneman et al., 2016) Military processes are one example of methods to suppress biases and inconsistency on decision making.

5.1.1 Planning and decision-making process

There are several planning and decision-making processes in the military context. In this chapter the US Joint planning process (JPP) (US Joint Chiefs of Staff, 2017) is covered in context of APEX.

The JPP seven-step process aligns with the four APEX planning functions. The first two JPP steps (planning initiation and mission analysis) take place during the APEX strategic guidance planning function. The next four JPP steps (COA development, COA analysis and wargaming, COA comparison, and COA approval) align under the APEX concept development planning function. The final JPP step (plan or order development) occurs during the APEX plan development planning function. After planning follows the execution of plans which is known as operation. Planning continues through execution as contingency planning or planning of the next phases of operation. (US Joint Chiefs of Staff, 2017) All supporting activities like logistics, intelligence and targeting participate in every planning step with their respective inputs. JPP is described in the figure 21. below in context of a problem-solving method.

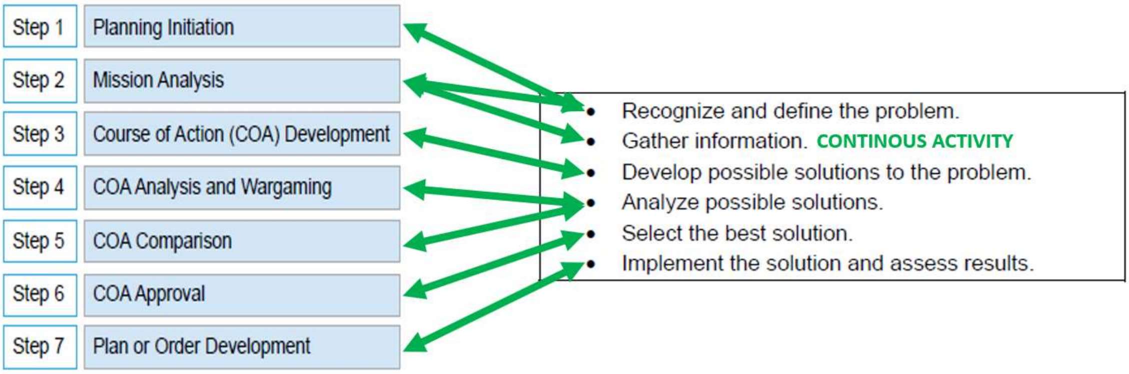

Step 1
Planning Initiation
Step 2
Mission Analysis
Step 3
Course of Action (COA) Development
Step 4
COA Analysis and Wargaming
Step 5
COA Comparison
Step 6
COA Approval
Step 7
Plan or Order Development
• Recognize and define the problem.
• Gather information. CONTINOUS ACTIVITY
• Develop possible solutions to the problem.
• Analyze possible solutions.
• Select the best solution.
• Implement the solution and assess results.

FIGURE 21 Planning process (US Joint Chiefs of Staff, 2017) and The Army problem solving method combined (Department of the army, 2010b)

First step in planning is *Initiation* or *Receipt of mission*. It is an event when appropriate authority decides to develop options with planning and gives related guidance. Key outputs are guidance for subordinates, planning group formation and initial planning timeline. Key functions are gathering of existing information and knowledge. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Second step in planning is *Mission Analysis*, in which planning staff analyses and synthesizes existing knowledge such as own resources (available troops and support), information about environment, intelligence products (enemy) and time available. This is done on the context of mission that was given. Restated mission is commander's initial intent, it describes purpose and actions to be taken to solve the given mission. Restated mission enables subordinates and supporting elements to begin their own planning. Other key outputs from mission analysis are commander's critical information requirements (CCIR), essential elements of friendly information (EEFI), estimates, assumptions and initial tasks. Key function is to understand the problem(s) to be solved. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Third step in planning is *COA development*. Course of action (COA) can be described as potential solution or method to fulfil the mission or solve the problem. It answers to questions who, what (the task), where, when and why (the purpose). Staff develops different distinguishable, feasible and acceptable COAs to provide options on how to accomplish the end state. COA outputs are written statements, tentative task organization, guidance for war game and evaluation criteria. Good COA provides flexibility to meet unforeseen events and allow room for initiatives. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Fourth step in planning is *COA analysis and wargaming*. Purpose of analysis is to examine and identify COAs that are feasible and executable, including their advantages and disadvantages. COA wargaming visualizes flow of the operation considering own forces, adversary and the operational environment using the action, reaction, and counteraction method. Each COA should be wargamed against most probable and most dangerous enemy COA. Both the positive and negative aspects of all assumptions should be reviewed, i.e. assumption will prove true or assumption will prove false. This can aid in preventing biases. Key outputs are refined COA's, potential decision points, synchronization matrixes, documentation of wargame and initial measures for operational assessment. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Fifth step in planning is *COA comparison*. It is decidedly subjective process in which COAs are evaluated independently and compared against criteria chosen by the staff and commander. Objective is to identify the COA that has the highest probability of accomplishing the mission given by higher command. This is a point in planning where decision making is facilitated by balancing ends-ways-means-risk of each COA. Key outputs are evaluated COA's (comparison matrix), COA selection rationale (advantages and disadvantages) and recommended COA. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Sixth step in planning is *COA approval*. Commander is briefed on the COA comparison, analysis and wargaming results, and staff proposes the advisable COA for commander. After this commander combines personal analysis with the staff recommendations, and process outcome is a selected COA with possible modifications. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

Seventh step is *Plan development*, in which approved COA is expanded and documented in to format of a plan or operations order (OPORD). Concept of operations (CONOPS) is the centrepiece of any plan or order as it states clearly and concisely what is to be accomplished and how it is done. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b)

During ongoing operations mission analysis commences until the operation has reached its objectives. Steps four through seven are repeated when necessary to integrate new requirements into the plan development. (US Joint Chiefs of Staff, 2017)

5.1.2 Planning considerations and critique

Simple questions can be used during the planning to frame the effort. Especially if planning is conducted during ongoing operation, and flow of information is exhaustive the right questions help to frame the problem. (US Joint Chiefs of Staff, 2017) Some questions are presented for example;

- Why are we doing this? What is purpose of the mission? What are the conditions we need to reach? (Ends)
- What are the current conditions of the operations environment? What is our situation? What is the enemy situation and where are they? Is the situation favourable to us? (Understanding)
- How do we complete the tasks? With what actions, resources, authority, restrictions and limitations? (Ways and Means)
- How will we know that we have successfully accomplished the mission – how do we assess/measure the success?
- What is the chance of failure, or unacceptable consequences when performing actions? How will we identify them? Is there an acceptable level of failure? (Risk)
- How do we present this that our commanders and forces understand what they need to do? (Visualization)

Ability to elaborate vast amount of data through questions like these into usable information is known as "operational art". (US Joint Chiefs of Staff, 2017) Operational art can be described as a cognitive approach which is based on skill, knowledge, experience, creativity, and judgment. It is used to plan and execute operations by integrating ends, ways, and means which create the operational design (i.e. CONOPS). (US Joint Chiefs of Staff, 2018) Use of formulated questions in information collection, judgement and decision making is also recognized by Kahneman et.al. (2016).

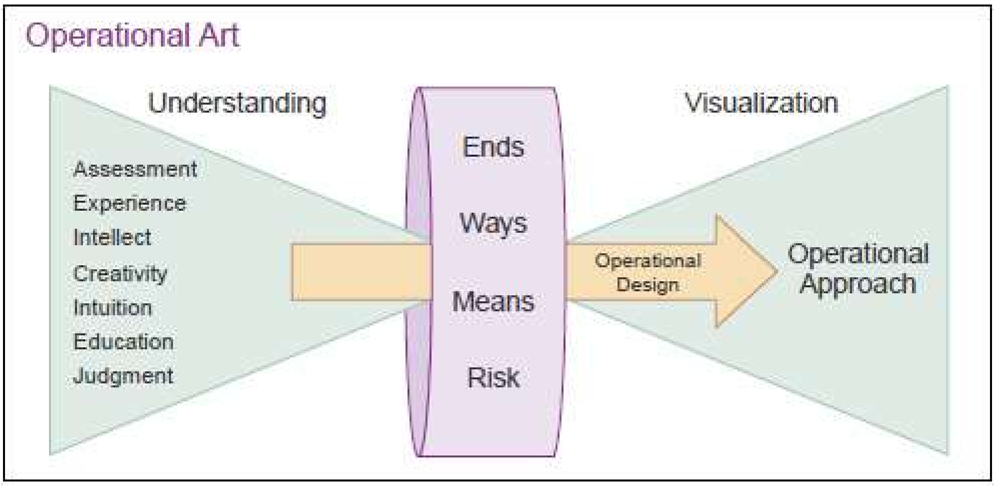


FIGURE 22 Operational art (US Joint Chiefs of Staff, 2017)

The application of operational design provides conceptual basis for understanding direction, guidance and environment, developing options and identifying points where decisions must be made. It is an iterative process which supports planning process by answering ends-ways-means-risks questions. It begins during mission analysis when goal is to understand the problem. (US Joint Chiefs of Staff, 2017) It is also a critical and creative thinking methodology to understand the environment, analyse problems, and consider potential approaches. (Department of the army, 2010b)

Executing current operations and planning for future operations can create tension. The smaller the unit, the smaller the planning team. This means that planning resources might be tied to finding solutions to reach near term objectives instead of long-term planning. (Department of the army, 2010b) Collaboration platforms and tools like automation of wargaming have been suggested to enhance and hasten the planning process. (Runyon, 2004) Use of Artificial Intelligence has been suggested to analyse flows of information in dynamic battlefield. (Moisescu et al., 2010) So far, the most radical method for suppressing inconsistency on decisions is to replace human judgement with algorithms, which on the other hand have policy and operational challenges. (Kahneman et al., 2016)

Gotztepe and Kahraman (2015) acknowledge that military planning process is a proven analytical problem-solving method to design operations. However, they propose to enhance planning with multi criterion decision making (MCDM) such as Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP).

Observations from operations suggest that theory and practical application of military planning process is not trouble free. Process might not be understood correctly, staffs that apply it are in some occasions inexperienced, and sometimes staffs fail to recognize or give relevant information to decision makers. This leads to ineffectiveness and reduced flexibility. To tackle these problems, planning staffs should receive education on decision making theories and problem-solving techniques which are meant to overcome biases and errors. (Marr, 2001)

Different decision-making theories like rational, limited rationality and rules-based decision making should be considered depending on planning task. Pre-mortem wargaming is suggested as an additional step to develop branches and sequels which provide flexibility. Planning should also pay more attention to capabilities that are needed, not just recognizing what assets are available. (Runyon, 2004)

5.2 Operations and assessment

Operations are sequenced tactical actions conducted by forces to accomplish a task or mission. Actions are unified towards common objective and purpose with command. Command is the lawfull authority that a commander uses to order and direct subordinates. Command and control (C2) includes the use of authority and direction of subordinates by commander to accomplish a given mission or task. Command is not only authority, but also responsibility to use forces and resources. Control is used to manage and direct forces and actions. It includes delegation of authority, direction of operations, and synchronization of actions. (US Joint Chiefs of Staff, 2018)

Execution is an operational activity which turns plans into action - operations. It is done by using combat power to accomplish the mission and using situational understanding to assess progress towards objective. Plans are very likely to need changes on execution phase, because force deployment will happen in conditions that are different from original planning guidance. In this situation reframing of the problem is needed to convert original plans into new decisions and timely actions. (US Joint Chiefs of Staff, 2017; Department of the army, 2010b) In other words; plan suffices only until the first contact with enemy.

5.2.1 OODA loop; Observe, Orient, Decide, Act

John Boyd wrote new conception for air-to-air combat in 1976. His concept paper is fundamentally about fighter aircrafts energy-maneuverability, focusing on subjects such as turn-rate, turn-radius and G-forces (Boyd, 1976). Boyd (1976) suggested that a fighter should be able to lose and gain energy quicker than the adversary, while out-turning it. With these characteristics it could initiate and control engagement opportunities by having a fast transient. Idea behind fast transient is that winning is possible by operating at a faster tempo than adversary. In other words, own operations happen inside adversary's time scale, which makes them ambiguous from adversary's viewpoint by creating confusion and disorder. Ambiguousness causes the adversary to over and under react. (Boyd, 1976)

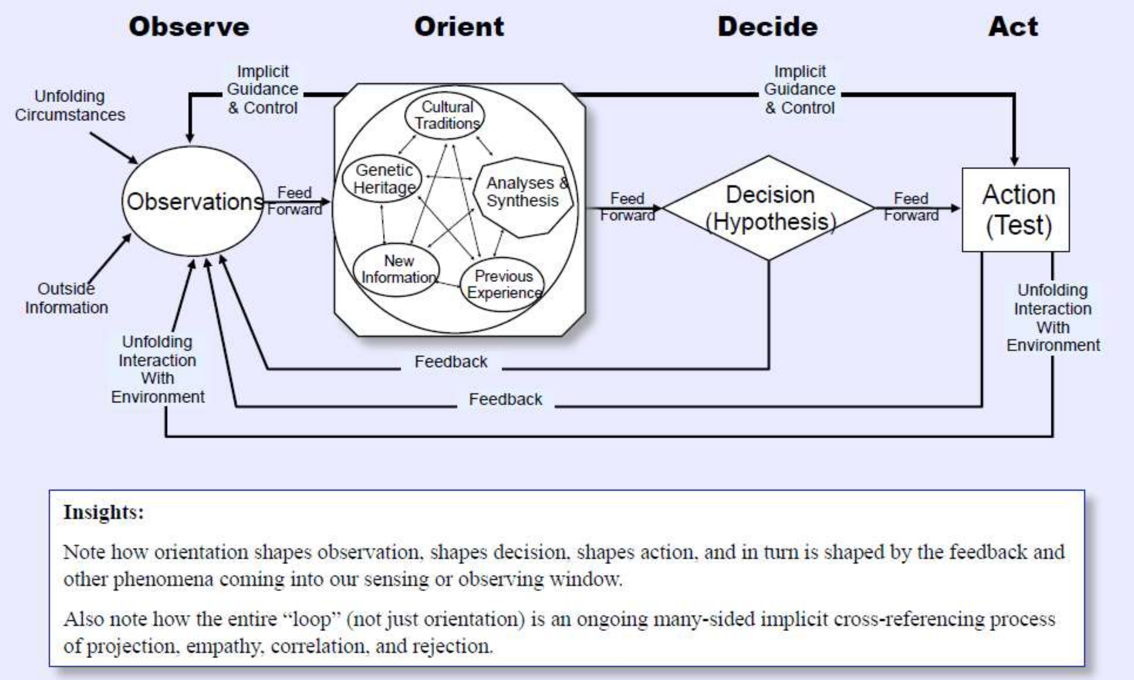
Although Boyd's 1976 paper was about air-to-air combat, he made one notion that this same principle could be applied to waging a war. Required operational features would be quick/clear *observations*, fast tempo, fast transients and quick kill. Main message of fast transients was that; *"He who can handle the quickest rate of change survives."* (Boyd, 1976) Boyd's other paper; Destruction and creation is about mental patterns and concepts of meaning. Paper sketches out how to destroy and create mental patterns for quick decision making in order to shape and be shaped by changing environment. Destruction and creation of patterns is inevitable, if one intends to survive on own terms in changing and expanding observed reality. This leads to a mental cycle, or *loop*, of structure, un-structure, restructure. (Boyd, 1976b)

Boyd's (1976) paper about fast transients introduced the term observation. Decisions can be seen to be built into fast transients and quick kills. Destruction and creation (1976b) introduced the concept of quick *decisions* and following *actions*. Decisions must be timely, based on observed reality, and actions must be compatible with the goal. (Boyd, 1976b)

Boyd's Conceptual spiral (1992) is a discourse on winning and losing. It builds from his previous studies in the context of how to succeed in many-sided, uncertain and constantly evolving reality. Boyd (1992) argues that practices of science and engineering are the key for conceptual spiral. Science provides the self-correcting process of observation, hypothesis and test, whereas engineering provides the self-correcting process of observation, design and test.

After presenting almost 60 examples of scientific and technical innovations from three centuries, Boyd's (1992) synthesis is that some portions of future are always indistinct and unpredictable. He argues that combination of science, engineering and technology functions in an analysis-synthesis feedback loop that shapes reality and adapts to it. This feedback loop produces novelty and innovations which affects us as individuals and groups by changing our *orientation*. Orientation must also be matched with novelty that is produced by forces of nature, personal thinking and competition, otherwise one will have a confusing mental mismatch. Winning is not possible without continuous orientation. (Boyd, 1992)

For three decades Boyd developed the concepts of observation, orientation, decision, action and self-correcting loop. His final product was only five unpublished slides; the essence of winning and losing. Boyd continues from previous studies and presents the OODA loop which embraces all his findings. He states that without OODA loops, depicted in the figure 23. below, it is impossible to comprehend, shape, adapt and be shaped by evolving reality. Essentially Boyd's OODA-loop represents an evolving, open-ended process of self-organization, emergence and natural selection. Key statement is that in order to win one must be able to get inside adversary's OODA loop (Boyd, 1996).



Insights:

Note how orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the entire "loop" (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

FIGURE 23 The OODA ”Loop” Sketch (Boyd, 1996)

Boyd influenced military planning process, which is a problem-solving technique, as was previously discussed. It gathers observations, creates orientation, and acknowledges that planning is based on imperfect knowledge and assumptions, because it is about envisioning events that unfold in the future. Mental models that are created during planning process facilitate decision making in changing circumstances. Even more, Boyd influenced mission command by stating that decisions must be timely, based on observed reality, and actions must be compatible with the goal.

5.2.2 Mission command

Mission command is used to conduct operations with decentralized execution which is based on mission orders. It is is the preferred method to control and combine operational activities such as intelligence, targeting, execution, planning, sustainment and assessment. Prerequisite for successful mission command are understanding of situation, full familiarity with the commander’s intent, timely decision making, directing actions and leading towards mission accomplishment. Mission command calls for initiative, independence and mutual trust and understanding between commanders and subordinates. (Department of the army, 2010b; Department of the Army, 2012)

Fundamentally mission command is exercising authority and giving direction, in which key element is the commander’s intent. Commander’s intent is a clear and concise expression about the purpose of given operation, key tasks and desired outcome or end state. Commander’s intent supports mission command by providing focus for staff, and guides subordinates to achieve desired results without further orders, even if the operation does not unfold as planned. (Department of the Army, 2012) Therefore, mission command enhances adaptability. Adaptability is based on continuous assessment of situation, critical thinking, and acceptance of both uncertainty and calculated risks. (Department of the army, 2010b)

Mission command happens in real time, and it should give freedom of action for the subordinates. Freedom of action in military context means that leader orders what to do (ends), and subordinate decide how to do it (ways and means). (Department of the Army, 2012; US Joint Chiefs of Staff, 2017) Core process in mission command is the operations process.

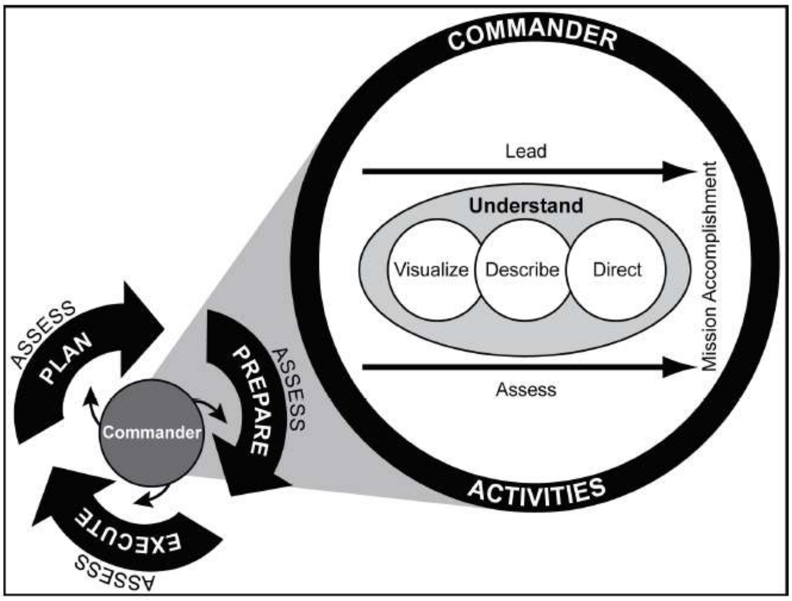


FIGURE 24 the operations process (Department of the Army, 2012)

Commander's role is to lead and assess the operations process, for which he needs understanding of situation and operational environment. Commander frames the problems in given environment and visualizes different approaches to solve them. Staff's role is to conduct the operations by planning, preparing and executing as per the commander's guidance. Assessment happens in all activities, and it supports commander's decision making. (Department of the Army, 2012)

To achieve understanding, data needs to be transformed to have meaning. Data is processed into information, from which analysis refines information into knowledge. When judgment is applied, knowledge is transformed into situational understanding.

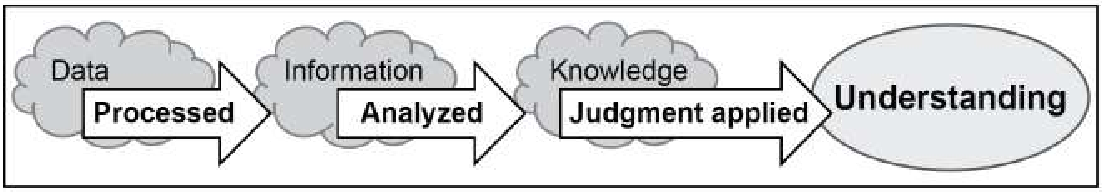


FIGURE 25 Achieving understanding (Department of the Army, 2012)

Besides leading and assessing the operations process, commander also develops teams within his staff. Team can be any group of individuals or organizations that works together toward a common goal. Commander informs and influences cooperation partners as needed to create shared understanding and synchronize actions. (Department of the Army, 2012)

Staff's responsibility is to support the commander and subordinates in understanding situations, decision making, and conducting the operations. Staff does this by conducting the operations process activities: planning, preparing, executing and assessment. Supporting activities are knowledge management and information management. Knowledge management enables shared understanding, learning, and decision making by transferring knowledge between relevant personnel and organizations. Information management is the actual procedures and information systems that are used to collect, process, store, display and disseminate information and knowledge products. (Department of the Army, 2012) Mission command tasks are depicted in the figure 26. below.

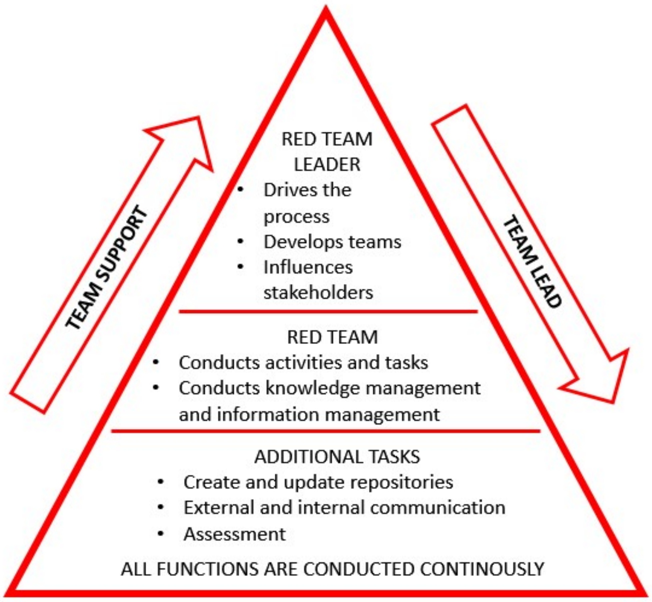

TEAM SUPPORT
TEAM LEAD
RED TEAM LEADER
• Drives the process
• Develops teams
• Influences stakeholders
RED TEAM
• Conducts activities and tasks
• Conducts knowledge management and information management
ADDITIONAL TASKS
• Create and update repositories
• External and internal communication
• Assessment
ALL FUNCTIONS ARE CONDUCTED CONTINOUSLY

FIGURE 26 Mission command warfighting function tasks (Department of the Army, 2012) adapted to red teaming by Frilander & Tuovinen

Mission command tasks for different levels are defined to integrate several activities within the staff and forces. Commander provides direction to integrate and synchronize activities, and develops teams by establishing mutual trust, understanding and cohesion. Staff conducts activities such as planning, preparations, knowledge management, information management and assessment. (Department of the Army, 2012)

Mission command cannot be conducted without a system which is used for information management, communication, collaboration and providing working environment (Department of the Army, 2012). Mission command system description is to somewhat like definition of information system which was introduced in subchapter 3.1. Component breakdown is depicted in the figure 27. below.

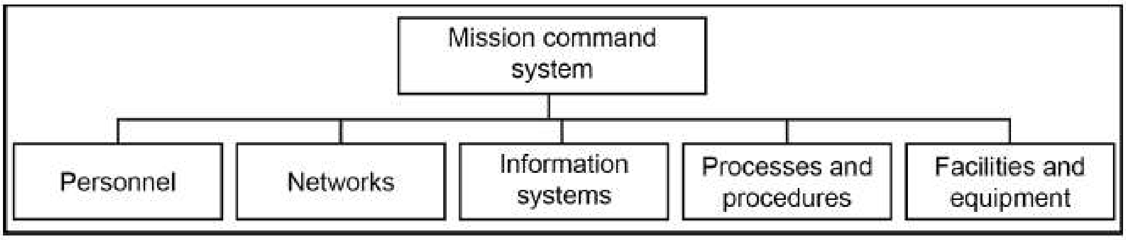


FIGURE 27 Components of mission command system (Department of the Army, 2012)

Personnel's role is emphasized as only they can accomplish the mission. Second in commands are assigned to commanders for burden sharing, and to ensure continuity if for any reason commander is not able to resume command. Staffs role is to provide relevant information for the commander and subordinates. (Department of the Army, 2012)

Networks consist of both technical and social networks which are systematically interconnected to exchange purposeful information. They are key enablers for successful operations. Information systems consist of computer hardware and software including policies and procedures for their use. (Department of the Army, 2012)

Systematic processes and procedures are in place to organize activities within staff and throughout the forces. They are needed to make mission command system effective. Examples of standard operating procedures are for example functioning of a command post and instructions on how to configure common operational picture displays. Facilities and equipment form the working environment and shelter for the other mission command system components. They include items such as buildings, vehicles, tents and power supplies, but exclude information systems. (Department of the Army, 2012)

Information (data) in information systems is an individual component. In the mission command system information resides both in information systems and personnel (Department of the Army, 2012).

5.2.3 Assessment

Assessment is an activity that is conducted as continuous process which measures the effectiveness of operations. Assessment provides feedback to adjust planning and execution of operations. It includes monitoring and evaluating the current situation, enemy and all operational activities to determine if they contribute to progress towards objectives and accomplishing a task. Indicators and measures for performance (MOP) and effectiveness (MOE) are developed during the planning process (US Joint Chiefs of Staff, 2018; US Joint Chiefs of Staff, 2017; Department of the army, 2010b) Commander's role is to prioritize assessment. It is effective only when it incorporates the logic behind the plans and orders. (Department of the army, 2010b)

Primary tools for assessment are plans, orders, common operational picture, personal observations, running estimates, and the assessment plan. Running estimates provide information from own capabilities and intelligence, which supplement to common operational picture. Assessment plan includes measures of effectiveness and measures of performance and is usually focused on the end state. However, it is also possible to develop assessment plans for intermediate objectives. Time, resources, and added complexity are the limiting factors on how many different assessment plans can be produced. (Department of the army, 2010b)

Development of an assessment plan includes six steps. First step is gathering the tools and assessment data, second step is creating understanding on current and desired conditions, third step is development of assessment measures and potential indicators, fourth step is development of the collection plan, fifth step is assigning responsibilities for analysis and recommendations generation, sixth step is identifying feedback mechanisms. (Department of the army, 2010b)

5.3 Intelligence and targeting

Joint planning process (JPP) focuses on framing the situation and end states, defining the military mission, analysis of critical factors, and designing an operational approach to accomplish mission objectives. Capabilities like intelligence are integrated into the JPP and into the Adaptive Planning and Execution framework. (US Joint Chiefs of Staff, 2013)

Intelligence and targeting are interlinked activities as described earlier in this chapter. Nature of intelligence is to facilitate the understanding of the operational environment (OE) and main responsibility is to provide information and assessments to support the accomplishment of the mission (US Joint Chiefs of Staff, 2013). To accomplish these tasks the intelligence activity needs to support planning and execution of operations with various products such as intelligence collection plans (ICP) and situational awareness (SA) products.

Primary purpose of targeting is to synchronize all capabilities to create effects to adversary's systems (US Joint Chiefs of Staff, 2013b). Prerequisite for doing so includes several other disciplines like intelligence, planning and operations.

Intelligence as an art is as old as structured thinking, because that's what intelligence is. It is also structured way of planning the collection, analysis and dissemination of information to clients (US Joint Chiefs of Staff, 2013). Intelligence studies as an academic effort can be traced to 1950s but there is still debate whether it's a discipline or a combination of other disciplines. Intelligence studies combine all the aspects of practical intelligence which include humanities (i.e. languages and history), social sciences (i.e. psychology, economics, sociology), natural sciences (i.e. physics) formal sciences (i.e. statistics and computer science) and applied sciences (i.e. engineering) (Gill & Phythian, 2016).

Targeting derives from system science which is also a multidiscipline research field like intelligence studies. General systems theory has its roots in 1920s biology and the system theory of the organism which noted that by examining just a single part or a process of an organism does not give understanding of the whole (Von Bertalanffy, 1972). Targeting has the same philosophical approach seeing the adversary as an organism that is analysed as target systems with its components and then effects are applied to certain target elements to cause wanted results. (US Joint Chiefs of Staff, 2013b) These effects can be described as dynamical system theory application which studies the changes of the systems (Von Bertalanffy, 1972).

Intelligence collects, analyses and disseminates information. Targeting incorporates the synchronization of effects and forces that provide the effects. Both intelligence ((JP2-0 Joint Intelligence (2013)) and targeting ((JP3-60 Joint Targeting (2013b)) have their respective doctrines published which describes the activities in detail.

5.3.1 Nature and roles of intelligence

According to JP2-0 Joint Intelligence (2013), intelligence has two lines of effort;

1) Plan and conduct the intelligence operations (Run the intelligence cycle)

2) Support the planning and operations execution with intelligence

This means that intelligence must plan its own actions which derive from the requirements given by the customer as commanders critical information requirements (CCIR) in order to support the forces. Intelligence is not done for the sake of intelligence, but the result needs to be actionable which is useful to the customer and they can act based on the intel. (US Joint Chiefs of Staff, 2013)

To clarify the taxonomy between data, information and intelligence the following figure 28. illustrates how data is collected from the operational environment (OE) thus building to databases. From the data which is represented by symbols, numbers or words, information is harvested by classifying the data for example by date, area, type, etc by using questions such as what, where, when, or who (Ackoff, 1999). This is enough to build situational awareness (SA) which can be described as the understanding of the current situation or knowledge which is drawn from the question, how (Ackoff, 1999). Situational awareness can be considered as a continuous activity but also as the first intelligence product which presents the current state of operational environment (US Joint Chiefs of Staff, 2013). SA as a product can be for example the daily situational report which shows all incidents from last 24 hours and makes a brief assessment what might happen in the next 24 hours. After understanding of the situation comes the final question of why which combines the previous levels of cognition into intelligence that creates efficiency (Ackoff, 1999). This is the basis of more detailed analysis for various purposes and building of wisdom.

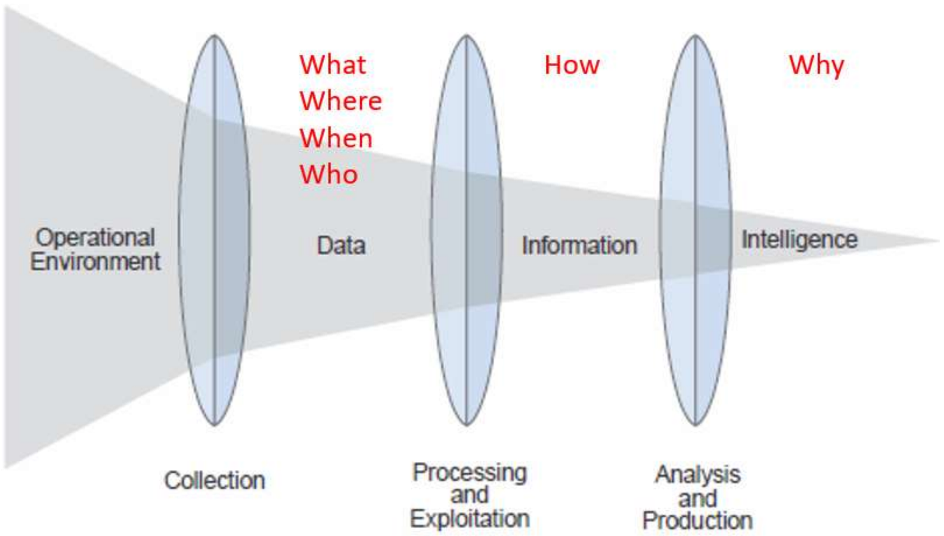


FIGURE 28 Relationship of data, information and intelligence (US Joint Chiefs of Staff, 2013). Modified by Tuovinen/Frilander 2019.

To understand intelligences' role, one must understand intelligence as a process first. The intelligence cycle in figure 29. below describes very simplistically the process of intelligence. To elaborate the figure, one should think that there is a different person in each box doing the activities. This is the functionalization of intelligence; there are collectors, analysts and managers.

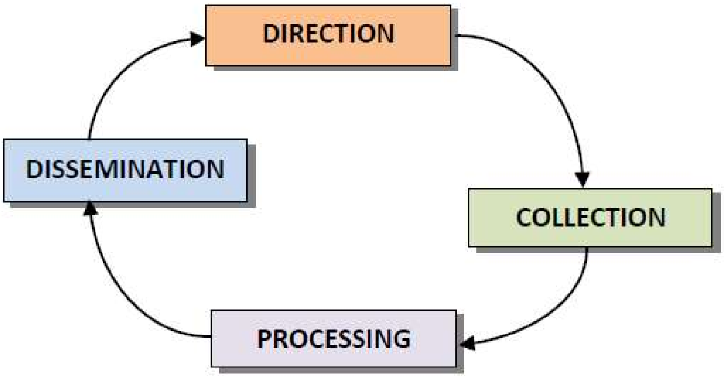


FIGURE 29 Simple intelligence cycle.

- **Direction** is issuing orders and requests to collection bodies. The direction comes from requirements set by the client which managers weight and decide how to achieve the goals.
- **Collection** is the process during which data or information is collected from different sources. Usually an intelligence collection plan (ICP) is created to illustrate the responsibilities of collection.

- **Processing** is a series of actions which consists of collation; analysis and integration of various collection bodies' information by analysts.
- **Dissemination** is the creation and delivery of various intelligence products to the customer including briefing them which can be done by anyone depending on the level of detail needed.

This is a simple description of intelligence process. The history of intelligence cycle is a debated topic and written origins can be found from 1886 when Lord Wolseley wrote the *"Pocket-Book for Army Field Service"*. The book describes guidelines for intelligence organization and gives phases for intelligence; Collection, analysis and reporting. (Tropotei, 2018) Intelligence cycle has developed since then and the four process steps as such dates back at least to 1920s when cavalry major Haines (Haines, 1926) wrote a proposed revision of TR 210-5 combat intelligence regulations where emphasis is given to consecutive phasing of the steps.

The traditional intelligence cycle has collected a lot of critique in last decades in the intelligence studies for being too simple and missing feedback loop from clients, (Lowenthal, 2016) explanation of the process, stove piping, parallel activities, lack of iterations and being only pushing and not pulling for reports (Frini & Boury-Brisset, 2011). The earliest critique dates to aftermath of WWII when "FM30-5 Combat intelligence" was published in the US and it states that steps are concurrent and while intelligence is collected, somebody else is analysing intelligence and some is using it while fourth is thinking about how to better align intelligence efforts (Department of the Army, 1951). Conclusion being; The steps are good, but the arrows should be removed from the figure 29. because there are continuous sub-processes inside every step and steps are simultaneous processes. Several intelligence studies have been made to remediate and develop the cycle since (Johnston, 2005; Frini & Boury-Brisset, 2011; Tropotei, 2018). Nowadays there is not just one intelligence cycle, but a plethora of them in use. From the US only, Tropotei (2018) listed ten different intelligence cycles used by various organizations currently. Conclusion could be that every organization has its own way of adopting knowledge, organization and processes to create intelligence that suits them.

5.3.2 Joint intelligence process

Due to APEX framework the US military intelligence cycle is presented for consistency. The cycle is renamed as the intelligence process which consists of six interrelated categories that are driven by a mission and kept under constant evaluation and feedback. The activities in categories occur simultaneously or can be bypassed if for example analyzed information is not needed in some case and the raw data suffices for dissemination. Still the raw data is simultaneously processed for other purposes by an analyst. (US Joint Chiefs of Staff, 2013). The process is depicted in the figure 30. below.

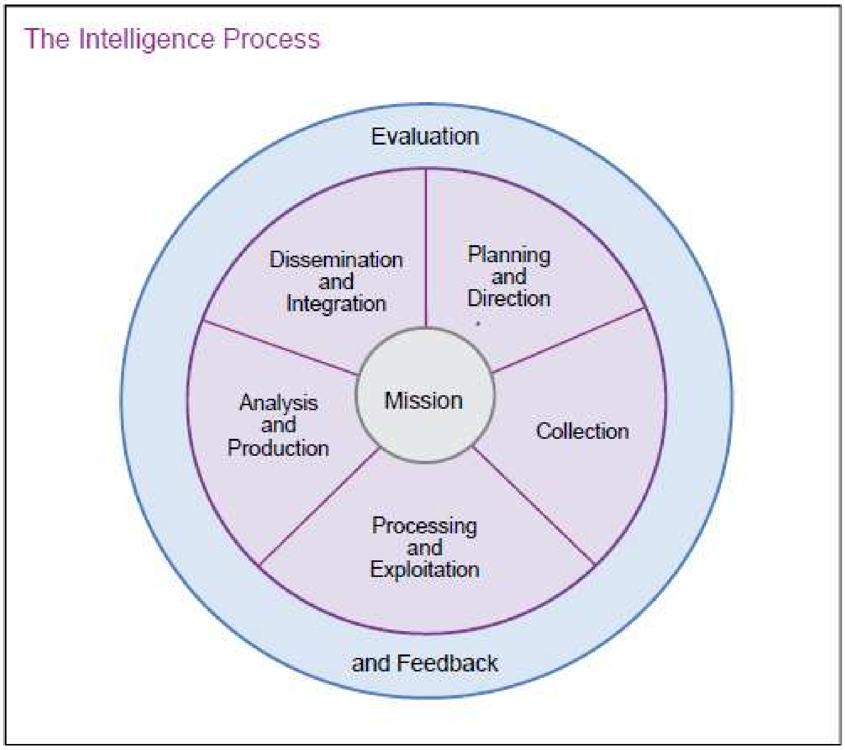


FIGURE 30 The intelligence process. (US Joint Chiefs of Staff, 2013)

The process is not much different than the simple cycle depicted in previous chapter, but its more detailed and broken down to several sub-processes which make the interpretation and managing intelligence in organization context more helpful. The planning and direction are development of intelligence plans and the continuous management of their execution. This can be a simple process dealing only with requirements for collection and intelligence collection plan (ICP). ICP defines the needs and responsibilities for collection or a very complex process with several activities varying due to complexity and size of the organization.

For example, targeting is interrelated to intelligence. During the planning, joint intelligence preparation of the environment (JIPOE) begins which means gathering the information to understand the complex operating environment (OE) and the adversary. For targeting purposes this means that target system analysis (TSA) needs to be initiated and collection assets must be allocated for support of targeting. Intelligence assets are needed throughout the targeting process to gather detailed information about targets (target development) and assess factors such as criticality and vulnerability of the target for factor analysis (FA) of the given system. Various impact and weaponeering analyses are conducted for target systems to find the suitable and most profitable places to strike. Finally estimate for the damages inflicted are done to the target as a battle damage assessment (BDA). This needs to be planned and resources allocated accordingly from intelligence units in support of targeting. Keeping in mind that the situation is constantly changing. (US Joint Chiefs of Staff, 2013) (US Joint Chiefs of Staff, 2013b)

Collection is the acquisition of data. Collection is managed by the intelligence collection (ICP) plan which is constantly updated and enforced by collection managers. Collection managers handle and combine the intelligence requirements and distribute the collection tasks to collection assets which do the collection. Effectiveness of collection through feedback is assessed constantly and management guides the collection accordingly. (US Joint Chiefs of Staff, 2013)

Processing and exploitation are converting data to comprehensible information. This can be considered as preliminary analysis or processing the data into a form that other intelligence units or customers can utilize. For example, signals intelligence (SIGINT) is increasingly automated and human intelligence analyst could not comprehend the raw data of SIGINT. Therefore, SIGINT analysts process the information for everyone to use. (US Joint Chiefs of Staff, 2013)

Analysis and production are combining all the available intelligence sources and creating products to communicate the results. The JIPOE is the key process and product for analysis. A continuous process to build a better picture of the operational environment (OE). Various kinds of intelligence products can be produced from the same information depending on the audience for which it is presented. The collaboration with intelligence producers is imperative to overcome shortages and gaps in analysis. This requires a common platform for communication and sharing, since the intelligence resources are usually geographically separated. (US Joint Chiefs of Staff, 2013)

Dissemination and integration mean the delivery of products to the customer and making them suitable for customer needs. This calls for example, understanding of the planning or targeting process and delivering integrated intelligence products to the customer. Dissemination can be push or pull orientated. Push means that products are provided and maybe even presented to the customer. Pull means that customer is given an access to certain databases or repositories where they can independently get the required information. Both options can be used simultaneously as well. (US Joint Chiefs of Staff, 2013)

Evaluation and feedback are like assessment described earlier. They are the continuous internal and external way to develop intelligence. In order to develop there must be measures of performance (MOP) and measures of effectiveness (MOE) to base the assessment on. (US Joint Chiefs of Staff, 2013)

The intelligence cycle is not of importance but the process how data, information, knowledge and intelligence is refined to support the mission. Intelligence cycle(s) offers a structured process for that.

5.3.3 Targeting methodology

According to JP3-60 Joint Targeting, targeting has one purpose; Integrate and synchronize all weapon systems and capabilities to generate specific effects on a target. This is done by systematically analyzing and prioritizing targets for mission goals. Target is an an entity which performs a function for the adversary. (US Joint Chiefs of Staff, 2013b)

Targeting is also described as a cyclical process which has sub-processes in every phase. The steps may occur concurrently, but regarding a single strike the steps are sequential. The first three steps of the cycle are planning orientated and last three steps are execution of targeting plans. (US Joint Chiefs of Staff, 2013b)

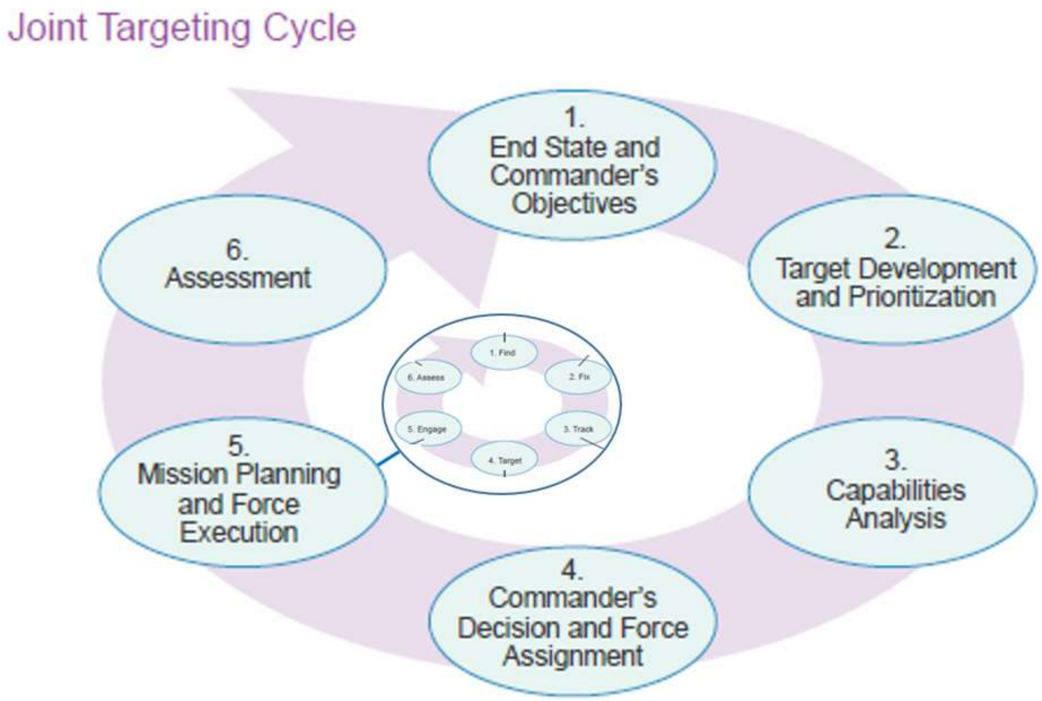

Joint Targeting Cycle
1. End State and Commander's Objectives
2. Target Development and Prioritization
3. Capabilities Analysis
4. Commander's Decision and Force Assignment
5. Mission Planning and Force Execution
6. Assessment
1. Find
2. Fix
3. Track
4. Target
5. Engage
6. Assess

FIGURE 31 Joint Targeting Cycle. (US Joint Chiefs of Staff, 2013b)

First phase of the cycle is understanding the objectives of the mission and initiating the planning of effects to support the concept of operation (CONOPS) draft. Products from JIPOE process are used to build a coherent picture of the adversary. Targeting is one part of the joint planning process (JPP) and it gives inputs to all phases. (US Joint Chiefs of Staff, 2013b)

Second step in targeting is detailed analysis, assessment and documentation of the potential targets. This is done by conducting a target system analysis (TSA) where adversary is broken down to target systems, target system components, targets and target elements. This taxonomy and definitions are dependent on the attacker and how they wish to see the enemy. There are several architectural possibilities in building the system analysis. (US Joint Chiefs of Staff, 2013b)

Third step is about assessing the possibilities to affect the targets starting with vulnerability analysis to identify weaknesses in the target elements. Available capabilities, feasibility and initial effect estimate are also considered as well as weaponeering. All of these are documented to target folders, and this gives the commander a toolbox for setting up a master attack plan (MAP). (US Joint Chiefs of Staff, 2013b; Department of the army, 2015)

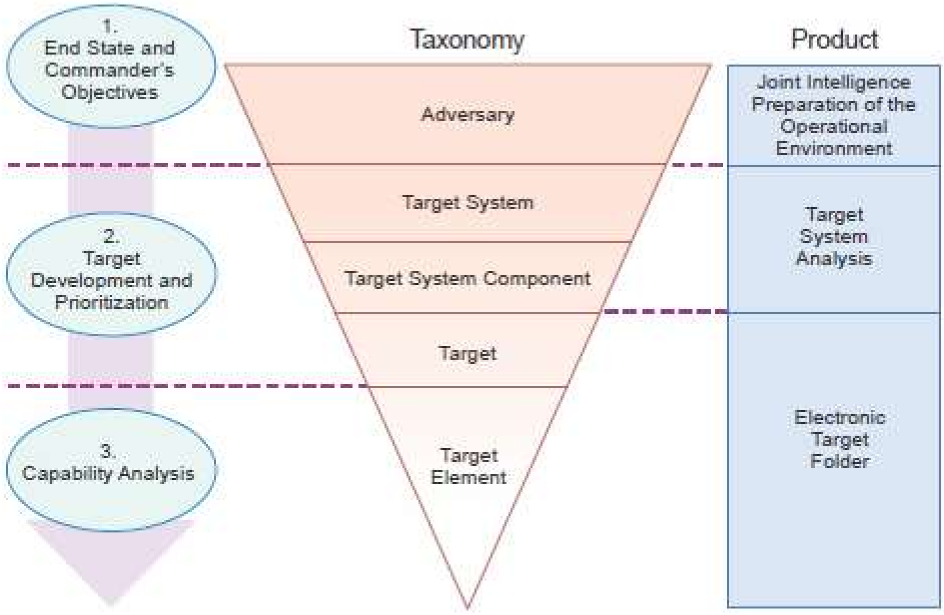


FIGURE 32 Target development relations. (US Joint Chiefs of Staff, 2013b)

Fourth step is integrating the attack plan into action by assigning targeting tasks to various units and aligning them with the other combat actions and plans. This initiates the execution and time critical actions which are described in the figure 33. (US Joint Chiefs of Staff, 2013b)

The fifth step of targeting is the find, fix, track, target, engage, exploit and assess, F2T2E2A-cycle. This is known as the kill chain and was used as a source for the renowned cyber kill chain article by Hutchins et al. (2011) The kill chain has been used as the baseline for cyber kill chains, but it disregards the big picture which is the overall planning and preparations of the mission and the supporting intelligence. The cyber kill chain has reconnaissance and weaponization, but they are not complete enough for planning a campaign. (Hutchins et al., 2011) The delivery of effects is not automatic in the fifth step but must always be aligned with the current situation. During the operations execution phase the units constantly try to find, fix, track and target their designated targets in order to be ready to engage them when tasked. (US Joint Chiefs of Staff, 2013b)

To understand the difference between joint targeting cycle and kill chain one needs to think about the time perspective. Joint targeting cycle phases 1-4 can take days, even months or years to be completed and kill chain can be completed in a matter of minutes, hours or days. Kill chain can be prolonged and in case of Osama Bin Laden it took years, but this is very unordinary. The joint targeting cycle is about integrating the effects to the mission planning with support of other functions like intelligence. Kill chain is delivering those pre-planned effects timely.

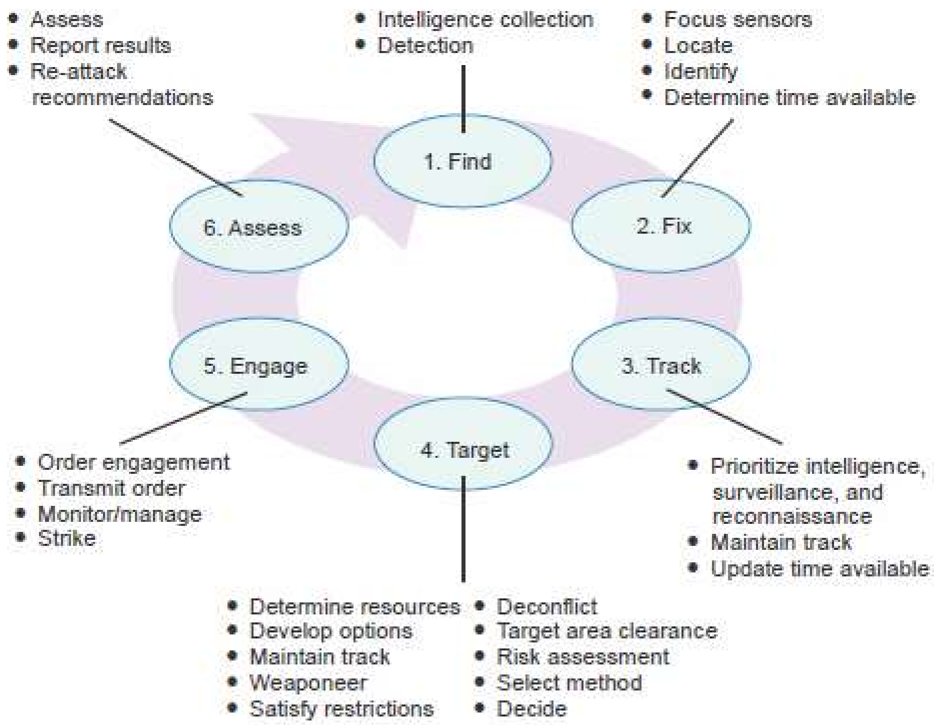


FIGURE 33 F2T2E2A – Cycle (kill chain). (US Joint Chiefs of Staff, 2013b)

Final step or a concurrent activity in the joint targeting process is the assessment. Assessment is always continuous and gives feedback from the ends, ways and means how the targeting has supported the progress of the mission. (US Joint Chiefs of Staff, 2013b)

5.4 Conclusions from APEX, intelligence and targeting

Military units conduct operations. Operation needs to have a clear endstate and ways to measure the success. Operations are planned with a planning process and executed with mission command. Intelligence creates the understanding of the operational environment to the units. Targeting aims to create effects to reduce the capabilities of the adversary.

There are interdependencies in every organization and military is no exception. Planning gives guidance and objectives. Planning is supported by intelligence and operations. Operations execute the plans with its capabilities and is supported by intelligence. Assessment is done constantly regarding own and adversary actions.

Planning process is a problem-solving technique. Completion of all steps slavishly is not an intrinsic value. (US Joint Chiefs of Staff, 2017; Runyon, 2004) To overcome this JP 5-0 (US Joint Chiefs of Staff, 2017) presents the concept of operational art. Combination of planning and operational art is easy to understand, but difficult to master. Military planning process is historically combat proven, and due to formalized structure, it can be a practical tool to reduce biases and inconsistency in decision-making.

It is prudent to acknowledge that all planning is based on imperfect knowledge and assumptions, because it is about envisioning events that unfold in the future. This is a challenge for effective planning, as uncertainty increases with the length of the planning horizon. Key value is the understanding and learning that happens during planning process, which facilitates decision making in changing circumstances. (Department of the army, 2010b)

Second key aspect of planning is synchronization of actions in time and space in order to generate maximum effort in decisive point and time. Due to future uncertainties one must remember that synchronization is a "way", not an "end". It must be balanced with agility and initiative. (Department of the army, 2010b)

Military planning process is subject for critique and can be enhanced. Some proposed enhancements are use of artificial intelligence, automation tools on wargaming, and application of collaborative methods and tools on decision making. These are all valid enhancements but if the people do not learn about the process itself and various problem-solving techniques, then process is useless.

Plans need to be executed and this requires understanding of the ever-changing environment. John Boyd's OODA-loop is the embodiment of this issue. Boyd developed the concepts of observation, orientation, decision, action and self-correcting loop. OODA-loop represents an evolving, open-ended process of self-organization, emergence and natural selection. Key statement is that in order to win one must be able to get inside adversary's OODA loop (Boyd, 1996).

Boyd has influenced military planning and execution processes as they gather observations, create orientation, and acknowledges that planning is based on imperfect knowledge and assumptions, because it is about envisioning events that unfold in the future. Mental models that are created during planning process facilitate decision making in changing circumstances. In order to win, decision-making process must be faster than of adversary. Decision making happens in a cycle or loop, which calls for constant destruction and creation of mental patterns. (Boyd, 1976b)

Mission command has evolved to be the US army's way of real-time operations execution and it takes several notions from OODA-loop. Main purpose of mission command is to create disciplined initiative within teams by empowering agility and adaptivity. It emphasizes leader's centralized intent, which is combined to decentralized execution of tasks by teams. (Department of the Army, 2012)

Besides leading operations leader's responsibility is to develop his team and to communicate. Communication efforts inform and influence cooperation partners as needed to create shared understanding and synchronize actions. Mission command cannot be conducted without a system which is used for information management, communication, collaboration and providing working environment (Department of the Army, 2012).

Intelligence is the structured process to provide knowledge out of mixed observed data. Targeting uses the intelligence to analyse the weaknesses of adversary and create effects through them. There are several different descriptions of intelligence and targeting processes, but the overall goal is usually the same; Provide actionable intelligence to stakeholders and synchronize the effects to the adversary in most effective way. There are intelligence cycles with varying number of steps. Some have three, others eight. Still they provide the same result.

Intelligence and targeting are activities that support the overall mission. Mission accomplishment is built by planning and executing tasks which are supported by intelligence. The structural process in intelligence and targeting is important due to this co-operation. Processes need to be separated due to their different functionality but communicated effectively between practitioners in order to be interlinked and aligned towards a common goal through mission command.

Continuous assessment of all previous activities is the orientation that Boyd's OODA-loop emphasizes. Fundamental question of assessment is whether the original plan or order is still relevant. This is done by establishing cause and effect relations, in which causes are the actions, and effects are results of those actions. (Department of the army, 2010b) Only by constantly assessing yourself, opponent and the environment one can achieve the advantage in ever-changing environment.

6 AGILE SUPPORT TO FRAMEWORK CREATION

"Intelligence is the ability to adapt to change"

- *Stephen Hawking* -

This is a descriptive chapter which builds to the knowledge base section in information systems research framework (Hevner et al., 2004). In the design science research methodology process this chapter comprises a part of phase 2; defining objectives of a solution and enables phase 3; design and development of the construct (Peffers et al., 2007). This chapter also adds to exaptation in DSR knowledge contribution framework, which means extending known solutions e.g. agile methodology to new problems i.e. red teaming in the information security management (Gregor & Hevner, 2013).

When agile development is mentioned people tend to think of software engineering. There are other interpretations as well. Clarence L. "Kelly" Johnson was chief research engineer at Lockheed's SkunkWorks®, an official pseudonym for Lockheed Advanced Development projects. In 1943 his team, consisting of just 28 hand-picked engineers, was given a task to develop a jetfighter to counter the growing threat from Germany. The XP-80 was designed and built in just 143 days, a somewhat agile effort in terms of time used for the project. Kelly had 14 rules of management, of which four were linked to organizing work. (Hilbert, 2017; Wikipedia, 2019a; Wikipedia, 2019b)

Decades later seventeen software development orientated people converged in Utah to find out alternatives for heavyweight software development processes. Values and principles for agile methodology emerged from this meeting in the form of agile manifesto in 2001 (Beck & all, 2001). Similarities can be seen when Kelly's working rules are compared with core values and principles of agile manifesto. (Hilbert, 2017)

TABLE 5 Kelly Johnson rules, agile values & principles - comparison.

Kelly Johnson 1943 (World of skunkworks, 2013)	Agile core values 2001 (Beck & all, 2001).	Agile principles 2001 (Beck & all, 2001).
The number of people having any connection with the project must be restricted. Use a small number of good people.	Individuals and interactions over processes and tools.	Motivated individuals can get the job done, when given the right environment and support. The best results emerge form self-organizing teams.
There must be a minimum number of reports required, but important work must be recorded thoroughly.	Working software over comprehensive documentation.	Working software is delivered frequently. Agile working method is simple, nothing excessive is done.
There must be mutual trust between the project	Customer collaboration over	Business stakeholders and developers must work together daily.

organization and the contractor, very close cooperation and liaison on a day-to-day basis.	contract negotiation.	The most efficient communication is conducted face to face.
A very simple drawing and drawing release system with great flexibility for making changes must be provided.	Responding to change over following a plan.	Changing requirements are welcomed even late in the development, and they are processed for customer advantage.

Similarities above show that the rationale of agile values and principles have been tried and tested in industry and military for decades. They are the response to bureaucracy and hierarchical management structures (Hilbert, 2017).

Agile manifesto was driven by several methods and method developers and its evolution can be traced back to 1980's. Common aim of agile methods is to manage software development in volatile business environment. Methods range from abstract principles to concrete guidance. Agile processes do not guarantee agility. Tools and working methods used in software development need to be agile also, i.e. it should be possible to adjust them depending on situation. Some agile methods cover only certain parts of software development lifecycle, and some of them do not support project management. Scrum is an example of agile method that supports project management, it can be adjusted to different situations and has empirical support. (Abrahamsson et al., 2003)

Agile development methods are based on a rationale which is grounded on human reality. Any product development invites substantial amount of learning, innovation, and therefore inevitable change. Agile methods emphasize developing products incrementally to accommodate the change. Users have possibility to use initial version quickly, which provides iterative feedback for developers. (Sutherland & Schwaber, 2011) Agile practices and agile scaling methods are implemented in the red teaming framework creation during this study.

6.1 Agile practices enabling benefits

Scrum is derived from complex adaptive systems theory. Creation was influenced by lean development principles which derive from Japanese industry, along with knowledge management strategies. (Sutherland & Schwaber, 2011; ScrumAlliance, 2018)

Scrum is an iterative and incremental framework for product development in any domain. Development cycles are structured into sprints. Individual sprint iterations length is no more than one month. Sprints take place one after the other without pause, and they are time boxed. Time boxing means that sprint ends on a specific date whether the work has been completed or not. (Sutherland & Schwaber, 2011; Cohn, 2010)

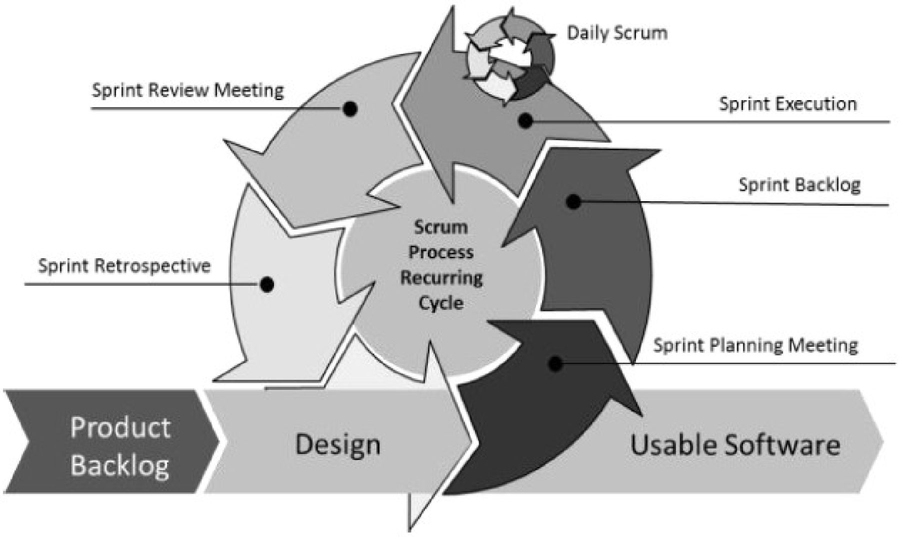


FIGURE 34 Scrum process cycle (Schlauderer et al., 2015)

At the beginning of a sprint, a cross-functional team selects items (desired functionalities) from a prioritized product backlog. Team decides on a sprint planning meeting how much work can be completed during a sprint; this forms a sprint backlog. During the sprint there are no changes to duration or goal. Team conducts daily scrum meeting to inspect progress and adjust work which is needed to complete the sprint backlog. At the end of each sprint is a review, in which the team reviews the results with stakeholders and demonstrates what has been developed. Sprint review provides feedback that can be incorporated into next sprint goals. Sprint retrospective is team's internal feedback meeting. Scrum emphasizes achieving "definition of done" (DoD) in each sprint. In the case of software development this means code that is integrated, tested and potentially shippable – it has some value and encourages feedback. (Sutherland & Schwaber, 2011; Cohn, 2010)

There are three roles in scrum: scrum master, product owner and the team. These three entities form the scrum team. Scrum master coaches the team on applying scrum, she is not a manager. This means that scrum master does not tell the team what to do or assign tasks. She facilitates the work by supporting team's self-organization and management. Her responsibility is to do whatever in range of realistic possibilities to help the team and product owner on achieving goals. This includes for example guidance on the use of scrum, protecting the team from outside interference and removing impediments. (Sutherland & Schwaber, 2011; Cohn, 2010)

Product Owner is responsible for maximizing return on investment (ROI). She identifies product features and translates these into a prioritized product backlog. Product owner interacts with the team actively offering priorities and reviewing the results of sprints, she makes sure that team is advancing to the right goal. (Sutherland & Schwaber, 2011; Cohn, 2010)

Small crossfunctional team develops the actual product, or its increment. Crossfunctionality means that the team has all required capabilities to deliver the potentially shippable increment in each sprint. If team size is more than ten individuals, it usually creates unnecessary communication and coordination overhead. Teams are also self-organizing which entails both autonomy and accountability. Autonomy means that the team has best insight to what can be accomplished. Product development includes providing ideas for product owner on how to make the product even better. Teams are most productive and effective when all members are dedicated to the given product versus avoiding multitasking in several products or projects. (Sutherland & Schwaber, 2011; Cohn, 2010)

To highlight, there is no project manager in scrum. Responsibilities of a project manager are divided and assigned for the three scrum roles. The word scrum master was invented in 1997 by Ken Schwaber, partly as a reminder that this role is not a traditional command and control project manager. Managers outside the scrum team may also be called upon to change their management style. For example, tactful questioning may help the team to discover best possible solution to a problem, rather than simply deciding on a solution and issuing it for the team. (Sutherland & Schwaber, 2011; Cohn, 2010)

Another agile development practice that is sometimes assimilated to scrum is Kanban. Its roots are in the Toyota's just in time production system. The management tool used to operate this system is Kanban, which translates to visual card. Main function is to limit anything excessive, especially work-in-progress. Like Scrum, Kanban is agile, transparent, adaptive and empirical, but it is even more configurable than Scrum. This means that fixed backlogs and time boxing are optional. In place of product and sprint backlogs is one or several Kanban boards, which present for example variable backlog, ongoing work, completed items and in production items. Board's content can be changed depending on capacity and/or demand, and it has no prescribed layout. Other key differences are that in Kanban specialist teams are allowed, and roles are not fixed. Scrum is more prescriptive and has more constraints, it focuses on iterative project work. Kanban on the other hand focuses more on the management of continuous workflow. (Kniberg & Skarin, 2010; Sugimori et al., 1977)

Benefits of agile implementation are recognized by Laanti (2012) in her dissertation. Figure below depicts a model from real world experiences in adapting agile practices (enablers) from Scrum and extreme programming. Goals represent the benefit for conducting agile transformation. Means are mechanisms for gaining value from the agile practices. (Laanti, 2012)

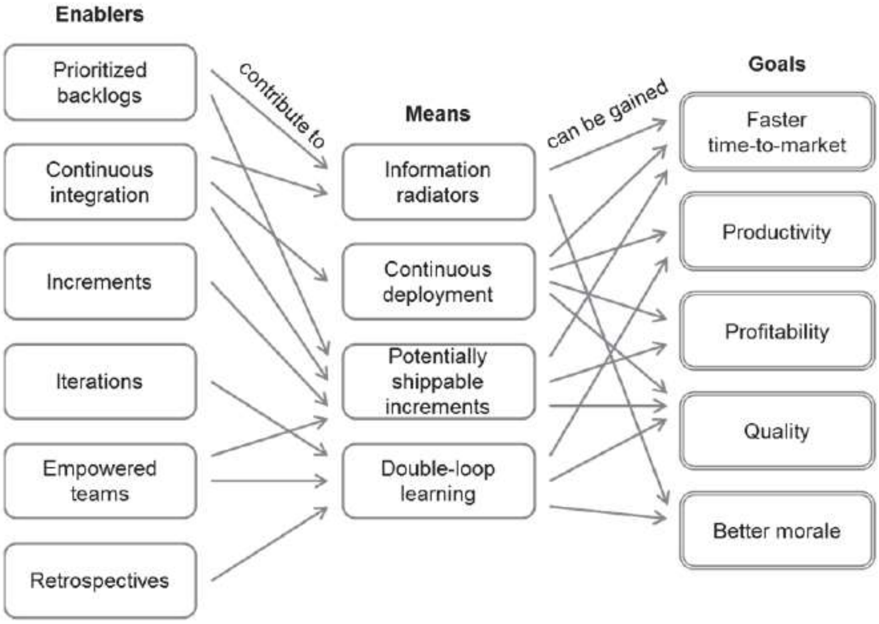


FIGURE 35 Agile goals, means and enablers (Laanti, 2012).

Agile practices often create productivity, quality and better morale within the teams as well as other benefits (VersionOne Inc., 2018). Agile practices can also be combined like any other practices. There is no value in following one practice and disregarding others due to dogmatism. (Kniberg & Skarin, 2010) The following question is how to manage the agile teams in an enterprise environment. Because teams cannot be agile if the organization is stiff, or can they? Next chapters try to cover this question.

6.2 Agile scaling

Organizations are increasingly realizing the benefits of agile practices, albeit facing challenges with competence to implement agile practices in a scale. There are several frameworks for scaling agile like Scaled Agile Framework (SAFe®) (Scaled Agile INC, 2018), Scrum of Scrums, Large scale Scrum (LESS) but none of them is ever implemented as such. Frameworks need to adjusted to the target organization. (VersionOne Inc., 2018)

Organizational culture is the critical factor in the success of agile implementation. (VersionOne Inc., 2018) Unity of leadership is mentioned by Laanti (2012) as a prerequisite for implementation. She also states that agile methods have proven to be beneficial in small organizations, and there is growing interest to scale their use into large organizations.

Enterprise agility or scaling agile tries to harness several agile teams to work in a larger context. Scaling covers areas such as portfolio level investments, and lean principles can be used to manage multiple value chains produced by multiple agile teams. (Laanti, 2014) Leans core function is to optimize delivery speed from different value chains in order to increase output from the whole system. (Laanti, 2012) Leffingwell's (2007) agile enterprise big picture depicted in figure 36. is a comprehensive model of scaling agile which also is the core of SAFe®.

Following explanation of the figure is intentionally incomplete, but sufficient for the scope of this study's goals. The figure below describes a three-level framework which depicts different planning horizons. The top level is portfolio which consists of epics that simulate the services a company could provide. These are listed in the portfolio backlog. The services are constantly evolving which is depicted as the architectural runaway. From the epics a program can be created to a customer. Various features can be collected from different epics by a system team which includes the necessary stakeholders including the client. A program is usually formed with several iterations and product releases. Teams receive tasks from the main program backlog, and they are reformed as team backlogs. Teams plan their sprints independently but taking in account the other teams. Co-operation between teams is not limited. The model is simple and missing several elements for agile scaling but gives an idea of the scaling as an example.

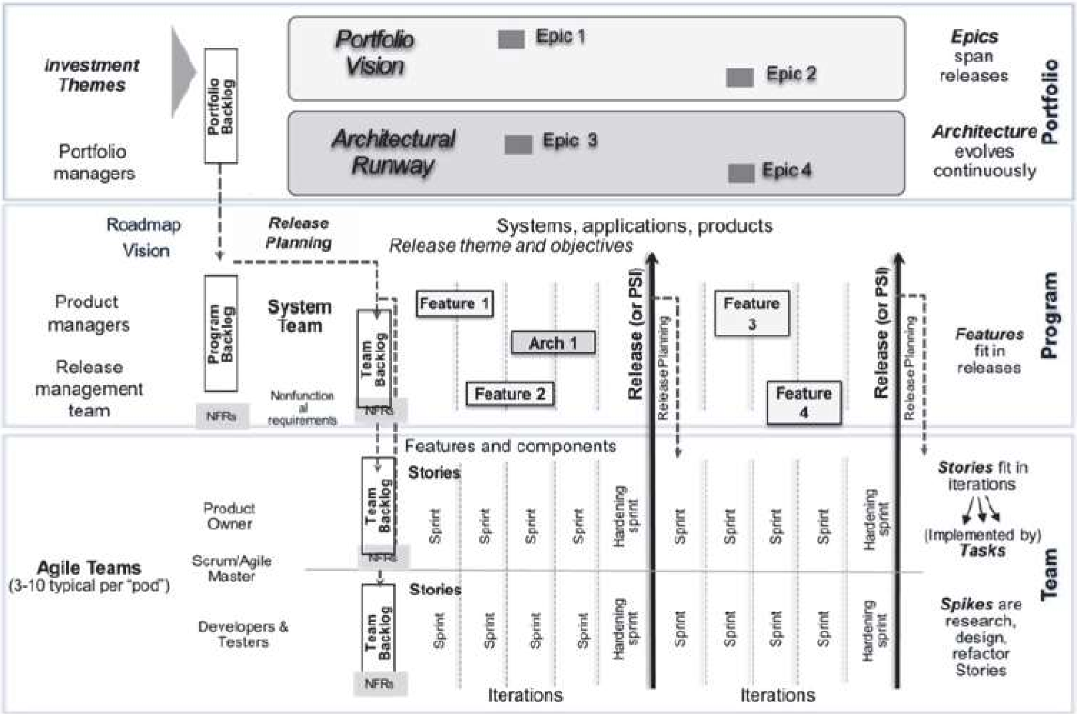


FIGURE 36 The agile enterprise big picture (Leffingwell, 2007)

The scaling of agile in enterprises can bring benefits for the entire organization by creating faster delivery, managing priorities better, enabling transparency and better productivity (VersionOne Inc., 2018). The real life does not always work like this and agility is only applied to the lowest team level. This might present conflicts in an organization. Although agility only in team level can bring benefits as well (Laanti, 2012). The reality of agile implementation is addressed next.

6.3 Water-scrum-fall

A common misconception about agile methods is that planning can be discarded. An agile team can live up to its expectations only by working in prioritized order, and therefore planning is an essential practice. (Cohn, 2010) Water-scrum-fall method is introduced in this chapter to tackle real world planning, budgeting and release issues. This does not mean that agile practices or scaling methods disregard planning.

In 1970 Winston Royce presented his findings from large scale software development for spacecraft missions. The result was the waterfall model or three waterfall models. The three models are merged into one figure depicted below. Basic waterfall has sequential phases described with green arrows. It was noted in the original document that basic waterfall is risky and invites failure. (Royce, 1970)

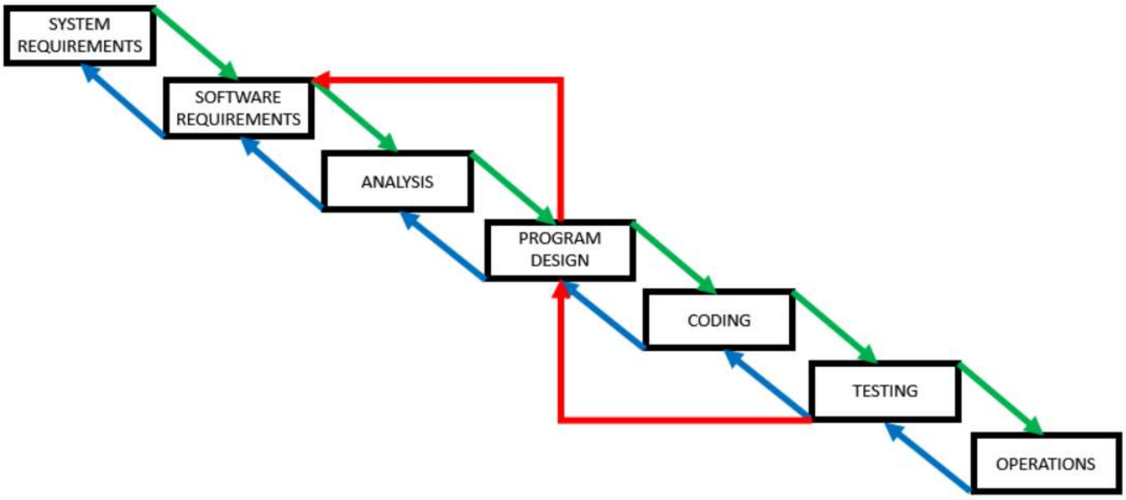


FIGURE 37 Waterfall conception outlines (Royce, 1970), merged into one figure by Tuovinen & Frilander

The blue arrows depict the iterative interactions which means basically doing every step twice which is very cumbersome. The red arrows describe phenomena that are found in testing but cannot be precisely analysed during design phase. Therefore, following redo of the software might lead development process to starting point. Remediations to waterfall, suggested by Royce himself, were thorough design and documentation before analysis and coding, doing the work twice if possible, thorough testing and involving the customer. But in the end, development lifecycle was fundamentally sequential basic waterfall. (Royce, 1970)

Waterfall model's strength is supreme logical planning before developing anything. However, it has one great weakness. The process does not allow any change should ideas or innovations emerge during development. Perhaps the greatest drawback is that waterfall relies on one big release, and many of the user ideas emerge when using the product for the first time. Also, the business environment might have changed, and the carefully developed product might be obsolete on release. (Sutherland & Schwaber, 2011)

Nowadays companies and teams embrace the rationale of agile methods described in previous sub-chapters but fall short of conducting it to full extent. Problems have emerged especially on agile implementation. Team members might multitask on several projects which hinders collaboration, and context switching creates unnecessary burden and ineffectiveness. Development, for example testing, that should be done by the team during sprint is done outside. This can lead to missed tasks and loss of feedback. Forming of new teams for each project hinders effectiveness, for example working methods must be agreed upon every time. (West, 2011)

Challenges are even bigger on corporate level. Plans drive funding from business case perspective, and these detailed plans then define the project. Agile project plan might not present enough detail for traditional business case decision making. Agile crossfunctionality might be lost, because specialized departments work on for example enterprise architecture and data governance. Agile crossfunctionality would enable faster turnaround and create synergy between different development disciplines within the team. Traditional project risk management relies on governance and documentation. In agile approach team mitigates risk by delivering working software, which can be reviewed by stakeholders. Business analysts work on requirements outside development, and therefore might not understand technological impact or possibilities. (West, 2011)

Everything said before, combined with resistance to release continuously, leads to a fact that water-scrum-fall, or hybrid/mixed agile implementation, is reality in most cases. Scrum adoption is often limited to the development teams' level due to traditional corporate management and compliance requirements that call for strong governance processes. To their benefit, traditional methods provide processual interfaces to HR management, sales, contracting, compliance and so forth (West, 2011; Theocharis, Kuhrmann, Munch, & Diebold, 2015).

In water-scrum-fall, depicted in the figure 38. below, water defines the upfront work. Definitions for the development come from governance rules and customer requirements, which dictate for a detailed plan that forms basis for a contract. When management has approved the plan, development phase is conducted with backlog-driven scrum model to release software frequently in sprints. Fall means that due to testing and restrictions on client IT architecture, deployments into production happen less frequently. Sequential waterfall is used to manage testing and deployment, which must comply with customer processes and service management. (West, 2011; Schlauderer et al., 2015)

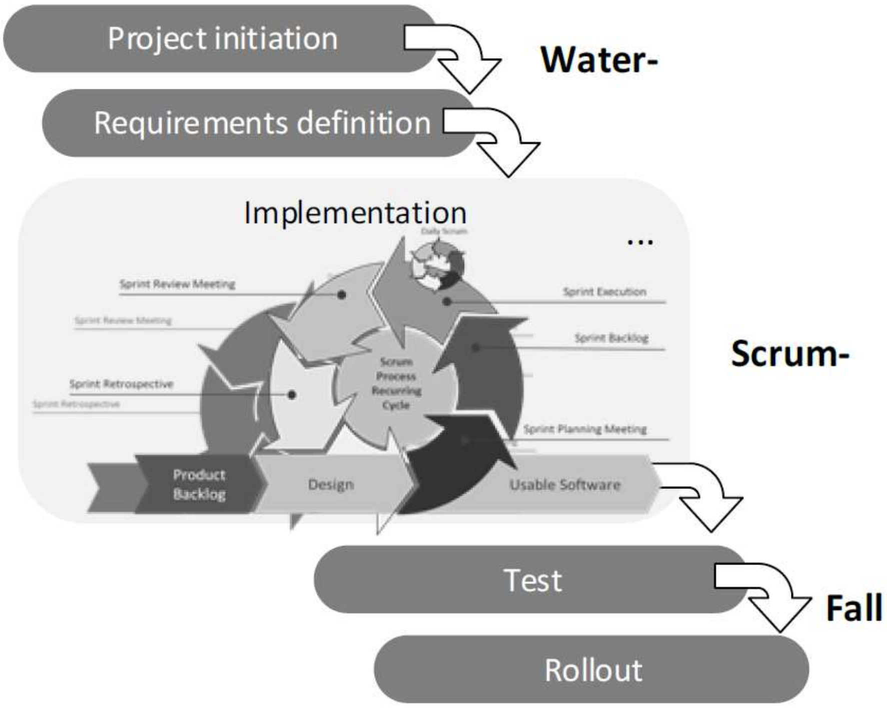


FIGURE 38 Water-Scrum-Fall (Schlauderer et al., 2015)

Waterfall is used when there is need for predictability and repeatability, typical example is referencing of test results into requirements definition. Scrum is used when there is need for flexibility and empirical process control, which is true especially during actual development of new software. (Schlauderer et al, 2015)

6.4 Conclusions

Agile practices can be found where good leaders like Kelly Johnson implement their visions to cut down to bureaucracy and hierarchical management structures but retaining the vision of their projects. Agility does not mean end of planning. It is planning with several horizons and different levels. (Leffingwell, 2007) This is similar in the military planning process.

There are several agile development methods of which few were presented like Scrum and Kanban which are the most renowned. (VersionOne Inc., 2018) Agile methods emphasize incremental product delivery where iterative feedback is quick from the iterations. (Sutherland & Schwaber, 2011) Some key enablers in agile practices include prioritized backlogs, continuous integration, increments, iterations, retrospectives and empowered teams which lead to productivity, profitability, quality and better morale. (Laanti, 2012) Agility also provides visibility and transparency of work to all stakeholders.

Agile teams are beneficial to an organization but scaling the agility to an enterprise level requires a cultural change as well. Agile portfolio and program management requires different kind of transparency than traditional waterfall planning. (Laanti, 2012) The implementation of agility to organizations can still be a beneficial process. (VersionOne Inc., 2018)

Agile enterprise transformations are harder to embrace than agile team practices. Therefore, a model addressed as Water-Scrum-Fall was also introduced. (West, 2011) WSF model tries to balance between the corporate reality which is bound by funding and plans. Without a plan there is no funding is usually the fundament. Agile methods do not disregard planning but WSF is more structural and traditional where upfront work is the basis for contract. (Theocharis et al., 2015) After this begins the more agile phase with possible iteration deployments and ending with a defined phase.

Agile methods have several similarities with adaptive planning and execution framework. Both deal with complex adaptive system environments and need the constant OODA-loop style process running. Crossfunctionality is comparable to JOINT, where different professionals combine their efforts in one team. Backlogs resemble planning, intelligence and targeting products which are produced in different steps of the process that can be interpreted as sprints or iterations. The agile scalability is based on different planning horizons which has resemblance to military strategic, operational and tactical planning which are parallel processes supporting each other with feedback mechanisms. Mission command emphasises the subordinate's responsibility of solving problems independently within limits and leader is more driving the process and fostering the team like a scrum master. Naturally there are difference between the world of military and agile, but the idea is to take the best of both worlds into the framework creation in this study.

Agile methods have reached armies around the world and USCYBERCOM is looking for ways to adapt agility in their operations as well (US DOD, 2017). Netherlands have a more ambitious goal to adapt agility in the entire armed forces (Ministry of Defence, 2018). This study is a possibility to see the interconnections between military and agile practices.

7 CONDUCT OF THE RESEARCH

"One thing a person cannot do, no matter how rigorous his analysis or heroic his imagination, is to draw up a list of things that would never occur to him".

-Thomas Schelling-

This chapter describes the process and methodology of the study in detail supplementing the first chapter. Reliability and validity of the study are also evaluated.

This theoretical and empirical, qualitative study was completed in accordance with the DSRM process (Peffers et al., 2007) and in the context of information systems research framework (Hevner et al., 2004). Research was done in following sequences according to figure 39. below.

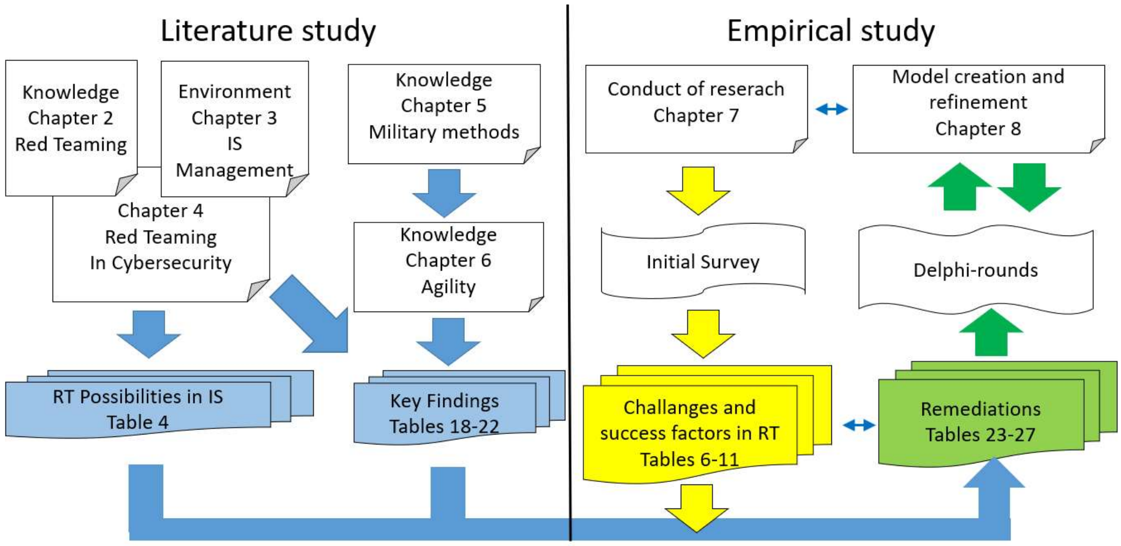

Literature study
Empirical study
Knowledge Chapter 2 Red Teaming
Environment Chapter 3 IS Management
Knowledge Chapter 5 Military methods
Chapter 4 Red Teaming In Cybersecurity
Knowledge Chapter 6 Agility
RT Possibilities in IS Table 4
Key Findings Tables 18-22
Conduct of reserach Chapter 7
Model creation and refinement Chapter 8
Initial Survey
Delphi-rounds
Challanges and success factors in RT Tables 6-11
Remediations Tables 23-27

FIGURE 39 Conduct of the research.

Chapters two, three and four were completed to build understanding of red teaming, information security management and consider the possibilities of red teaming in information/cyber security. These intermediate results were documented in chapter 4 (Table 4) as possibilities. Chapters 5 and 6 were written concurrently to present ideas from military and agile methods. Key findings from chapters 2-6 were documented in chapter 8 (Tables 18-22) to function as the building blocks of the framework. During this time the companies were contacted and co-operation was initiated.

Initial survey was sent to the companies to address challenges and success factors in red teaming. After receiving and analysing results from the initial survey, they were documented in chapter 7 (Tables 6-11) Challenges were remediated by using key findings and red teaming possibilities. Construction of the framework was initiated. Remediations were documented in chapter 8 (Tables 23-27)

Initial model was sent to companies with background information in order to validate the comprehensiveness of the created framework. This was the first Delphi round. Results from the first Delpi-questionnaire were analysed and documented in chapter 7.4. Refinements to framework were documented in chapter 8.4.

Framework was modified according to results from first Delphi round and second Delphi round was turned into a live presentation which was followed by the questionnaire. Results were again analysed and framework was modified accordingly. This is depicted in chapters 7.5. and 8.5.

Final modifications to the framework were discussed between the authors and the report was finalized. Finalized comprehensive red teaming framework is depicted in chapter 8.6. Chapter 9 discusses the process, results and future work.

7.1 Research design

This is a qualitative study where design science research methodology (DSRM) (Peffers et al., 2007) was used to create the construct, which is the comprehensive agile red teaming framework (CART) in the context of information systems research framework (ISRF) (Hevner et al., 2004). Information systems research is a typical research setting for design science. Design science was suitable for this research, because it aims to create a solution for a problem and new knowledge is created during the process.

The Design Science Research Methodology process consists of six phases (Peffers et al., 2007):

1. Identifying the problem and motivation
2. Defining objectives of a solution
3. Design and development of the construct
4. Demonstration about using the construct to solve a problem
5. Evaluation of the construct
6. Communication of results

In the first phase the research objectives for the solution and methodology were defined from literature and personal experiences from the field of information and cybersecurity. Second phase included familirization to the research domain through literature study. Phases one and two formed the fundamental knowledge base and description of the environment as described by IS research framework (Hevner et al., 2004). Environment consists of information systems, information security, IS management, risk management and cyber security. Knowledge base includes red teaming, penetration testing, military planning and operations, intelligence, targeting and agile methods. Phases one and two are overlapping, as the research aim and scope are defined during creation of the knowledge base. Adaptation of the IS framework to DSRM process in the context of this study is depicted in the figure 40. below.

Primary data in the environment and knowledge base is publicly available material which went through document analysis. The material has been, to some extent, created for other purposes. Multiple triangulation types were used in content analysis to support validity. Various data sources about the same topic includes data triangulation. Researcher triangulation was committed continuously by the two researchers involved and commenting each other's work and methodological triangulation was added by using several different methods (ISRF and DSRM). (Flick, 2006; Denzin, 1978)

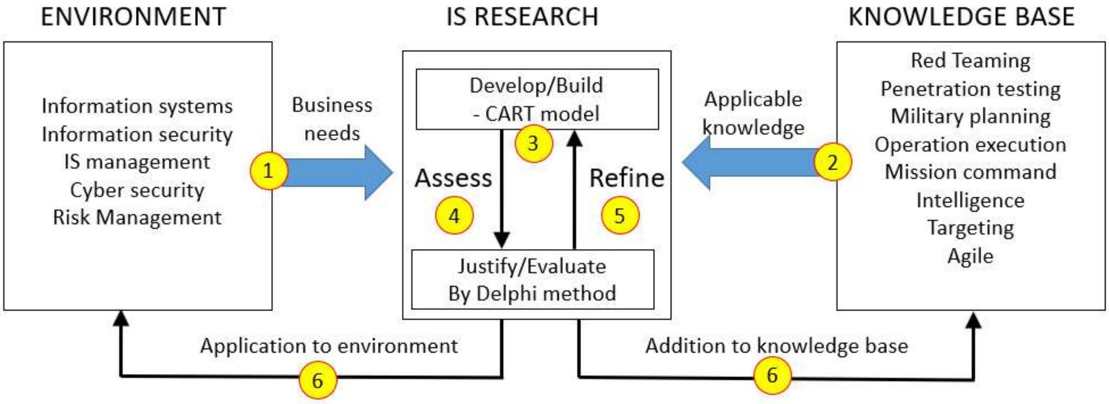


FIGURE 40 Application of ISRF to DSRM.

In the third phase a survey was made to five companies about shortcomings of red teaming and different processes from the knowledge base were depicted in accordance to the environment. This led to the creation of the new construct. This is the Develop/Build block of IS Research framework (Hevner et al., 2004). Phases one to three were completed concurrently. The initial survey answers were categorized in themes and main challenges were identified. Challenges were remediated by using the findings from the previous chapters and success factors.

7.1.1 Delphi-questionnaire

Fourth and fifth phase of the study were demonstration and evaluation of model in Delphi-questionnaires with two iterations. Delphi-method is used for group advice in order to avoid something that is only opinions. Delphi-method originates from future forecasting, in which refining opinions is especially important. (Dalkey, 1967) Although this study is not about future forecasting, the comprehensive research framework for Red Teaming with the use of DSRM methodology is a new model. Therefore, the need for subject matter experts (SME) was useful with different points of view in developing the new model.

Delphi-method is a consensus driven technique which promotes group communication between subject matter experts. Interaction between SME's was controlled by researchers in order to avoid confrontation. This leads to better reliability and judgement, because certain level of anonymity can be ensured concerning the individual responses. Delphi-method is not a statistical study, but more like a confined group decision mechanism. Due to this fact the SME's were selected from five cyber security companies. Delphi-method can be also utilized to test construct validity in new research areas. (Okoli & Pawlowski, 2004).

Divergence of answers is not a problem. It demonstrates that there has not been a negative "committee effect" among recipients. Delphi procedures three main aspects are 1. Anonymity 2. Controlled feedback and 3. Statistical group response, minimize the negative effects. (Dalkey, 1967)

Anonymity was ensured with written questionnaires and personal meetings. Companies were not informed of each other. Summarized and anonymized feedback and statistics about initial survey was included in the questionnaire and consecutive rounds. Use of Delphi-method can increase accuracy and reliability of the research by uncovering implied models behind the opinions. (Dalkey, 1967) This is something which can be called as informed intuitive judgement (Helmer, 1967). Applied phases for the Delphi –method are (Renzi & Freitas, 2015):

1. Formulation of questionnaire
2. First iteration for SME's with feedback from initial survey
3. Anonymization of the answers and preparation of controlled feedback for the second round
4. Second iteration for SME's as a presentation with feedback from the previous phases
5. Analysis of the second iteration answers and remediations

In the figure 41. below DSRM (Peffers et al., 2007) and IS research framework (Hevner et al., 2004). processes are depicted to clarify working methodology.

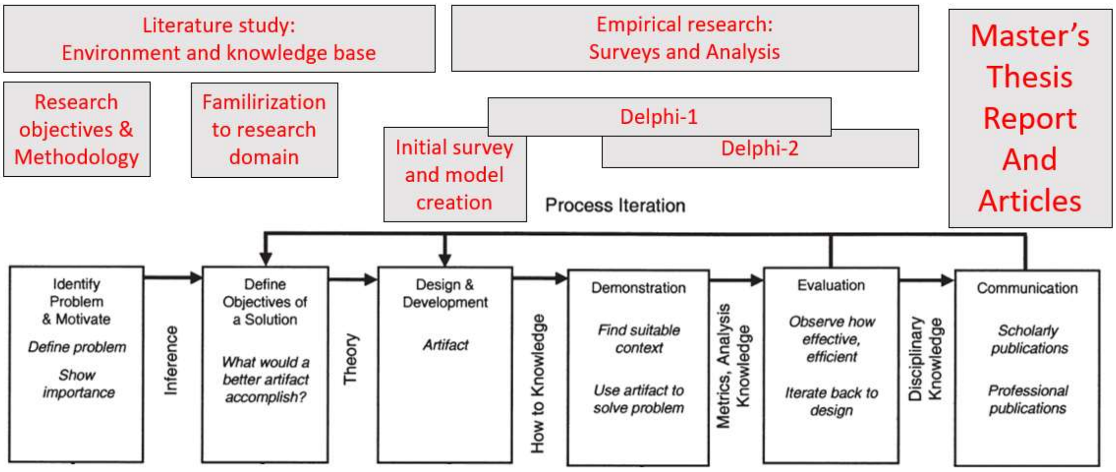

Literature study:
Environment and knowledge base
Empirical research:
Surveys and Analysis
Master's Thesis Report And Articles
Research objectives & Methodology
Familirization to research domain
Delphi-1
Delphi-2
Initial survey and model creation
Process Iteration
Identify Problem & Motivate
Define problem
Show importance
Inference
Define Objectives of a Solution
What would a better artifact accomplish?
Theory
Design & Development
Artifact
How to Knowledge
Demonstration
Find suitable context
Use artifact to solve problem
Metrics, Analysis Knowledge
Evaluation
Observe how effective, efficient
Iterate back to design
Disciplinary Knowledge
Communication
Scholarly publications
Professional publications

FIGURE 41 Process description in context of DSRM and ISRF.

With the use of Delphi-method, design, demonstration and evaluation was iterative and incremental with the feedback from SME's. First Delphi round led the study back to DSRM phase three. Second Delphi iteration produced last refinements for the framework by returning to the phase three once more. The first Delphi round emphasized more the demonstration of the frameworks comprehensives and second one evaluated the benefits and deficits of the framework.

7.1.2 Artifact creation

Term *"artifact"* is used in design science. Typical artifact in the field of information systems is a process (Gregor & Hevner, 2013) which CART construct resembles. Position of this study in the DSR knowledge contribution framework is improvement of information security and known red teaming processes and exaptation to merge multiple military and agile disciplines to create a more structured and comprehensive process. Marc & Smith (1995) have stated that: *"real problems must be properly conceptualized and represented, and appropriate techniques for their solution must be constructed"*. Problems were identified by the expert panel and then represented, and finally appropriate techniques were applied to create solutions. This was achieved by combining practical knowledge to scientific rigor. Flexibility was needed, because learning happened during the research process, and research produced facts to deepen understanding along the process which is typical in this type of research setting. (Robson, 2002). Fundamental considerations throughout the research were trueness and novelty of the created knowledge which are important in DSR (Gregor & Hevner, 2013).

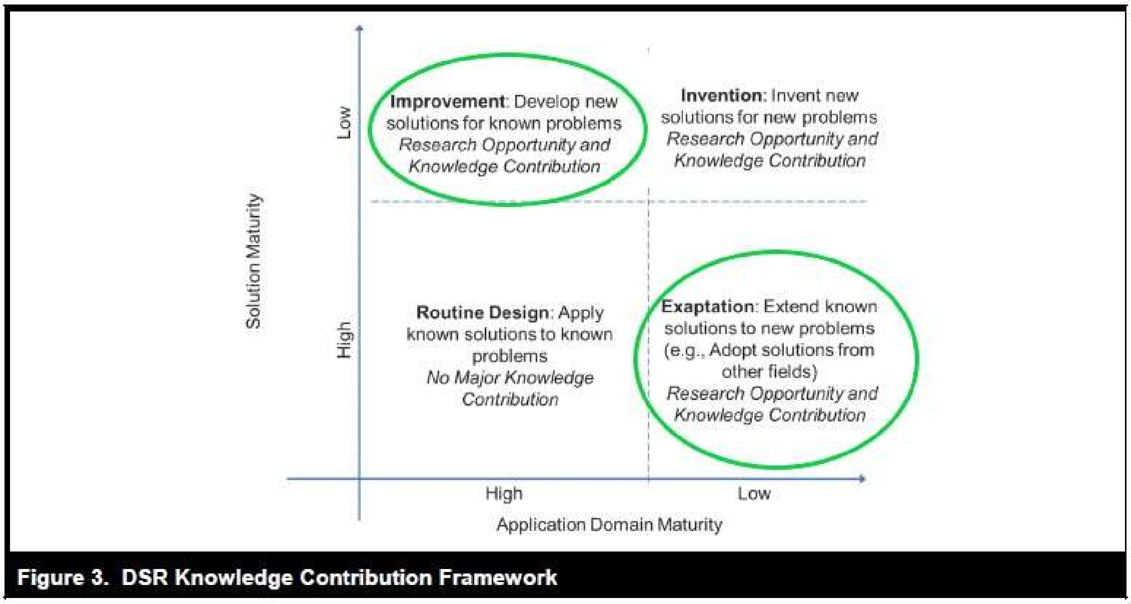

Low
Improvement: Develop new solutions for known problems
Research Opportunity and Knowledge Contribution
Invention: Invent new solutions for new problems
Research Opportunity and Knowledge Contribution
Solution Maturity
High
Routine Design: Apply known solutions to known problems
No Major Knowledge Contribution
Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields)
Research Opportunity and Knowledge Contribution
High
Low
Application Domain Maturity

Figure 3. DSR Knowledge Contribution Framework

FIGURE 42 Focus areas within DSR Knowledge Contribution Framework (Gregor & Hevner, 2013).

Improvement requires a known application context which was red teaming in the selected companies. According to initial survey red teaming lacks comprehensiveness and visible structure. The created *artifact* must be an improvement for example in efficiency or quality which it is. (Gregor & Hevner, 2013) CART is something that did not exist but creates the structured framework to conduct red teaming activities.

Exaptation calls for experience and insight from multiple disciplines to see interconnections. (Gregor & Hevner, 2013) Military, intelligence, targeting and agility were studied to extend knowledge to red teaming. This process was nontrivial but suitable for the challenge which defines exaptation (Gregor & Hevner, 2013). Exaptation was also the instrument for improvement.

7.2 Literature study

Literature study was conducted from September 2018 to April 2019. First phase for the researchers was to get acquainted with red teaming and information security management in depth. Both researchers studied the topics and then workload was divided as follows. Jussi produced the chapters two and four about red teaming and Kimmo produced chapter three, information security management. All chapters were then peer reviewed and modified after other researchers' comments. The implementation table 4. which consists of the results from chapters 2-4 about adaptation of red teaming into information security management was produced together.

Second phase of literature study was the introduction of adaptive planning and execution framework, intelligence, targeting and agile methodology in chapters 5 and 6. This workload was divided as follows; Kimmo produced the military planning and decision making as well as the operations and execution part. Jussi wrote the intelligence and targeting chapters. Then chapters were again peer reviewed and commented by the other researcher. Chapter six was written mostly by Kimmo and peer reviewed and commented by Jussi.

Commenting and peer reviewing was a constant process and several findings were done both ways during the process. The literature study is almost 90 pages and rough estimation of work done is about 50/50 by the researchers.

7.3 Initial survey

For the initial survey a preliminary study for the selected companies was completed. Five different companies in scope and size were selected as target recipients.

Initial survey was conducted by presenting some of the results from the literature study to recipients in five separate onsite meetings during February and March 2019. During the meetings research goals were introduced along with the methodology. All five companies agreed to participate to the research and answer the three rounds of questions.

During the five meetings the company representatives started already to share information about their challenges which were mostly lack of adamant processes for the red teaming effort. Red teaming was also seen and conducted in various ways depending on the company. These issues were noted and recorded onsite.

Open questionnaire was created for the companies to answer after the preliminary meetings. The questionnaire and cover letter are in ANNEX 1 and in ANNEX 2. Main questions are listed below, and the phases are depicted in ANNEX 2. Questionnaires were posted in first week of March 2019.

1. Please list the top five challenges you face in red teaming from every phase of the engagement. Please provide a short title and rationale for each of your issues.
2. Please list the top five success factors / Good things / Easy to do / etc. issues from every phase. Please provide a short title and rationale for each of your issues.
3. Please list Maximum of five additional general issues about red teaming, positive or negative or things that should be developed in general.

The aim of the questionnaire was to reveal challenges that needed to be solved and adapted to the new model. Success factors were identified to be implement to the model as well. Solutions for challenges were not asked for, because this might have guided the research too much. Results were received from five companies by the end of March 2019.

A content analysis was performed for the answer sheets and issues were sorted and merged due to variety of terms used by respondents in the titles. Rationales also differed from each other's. Responses were interpreted and categorized by their explanations. New issues were created to combine some topics into wider categories. The sorted answers are depicted in the next two sub-chapters in tables 6-11. Remediation suggestions for these tables are introduced in chapter 8.2. from the literature study and success factors.

7.3.1 Challenges raised by initial survey

Purpose of the initial survey was to frame the challenges and success factors in red teaming through the experiences of professional red teamers. Main perception from the answers was that there is no predetermined process framework for comprehensive red teaming efforts and assignment tasking is customized for each effort even though some red teaming/penetration testing process models are used.

This lack of rationalization and functionalization leads to problems in communicating the effort and managing the process itself. The pre-engagement phase challenges are sorted in table below with the number of how many recipients saw them as an issue.

Scoping of the future assignment was stressed in all responses from various perspectives and it needs the most effort to be remediated. Scoping problems are somewhat linked to preliminary knowledge and business domain understanding as well as client maturity. Adversary emulation method is also seen lacking maturity and red teams seem to proceed with their own know-how to missions, rather than emulating a custom attacker. Clients usually are not mature enough to ask for attacker profile. Many of the problems are related to internal or external communication.

Next level challenges lie with the red teaming companies and their own TTPs, documentation and reporting processes, as well as team generation issues to find the right competence for a job. Sales challenges fall in between these two because they usually manage the expectations between the client and the red team. Documentation is also found to be lacking from the beginning of the assignments.

TABLE 6 PRE-Engagement challenges.

ISSUE	n=	Challenges
Scoping	5+	• Artificial scope limitations • Scope creep during engagement • End-state and objectives are not clearly defined • Client's wishes might not be what is actually needed • There might be internally different opinions about scope on client side • Setting schedule and executing accordingly • Setting rules of engagement • Discrepancy between red teaming and penetration testing • Lack of comprehensive approach on red teaming
Client maturity	4	• Client does not have enough baseline security to be tested, policy review or penetration testing would be enough • Client has technical debt • Lack of management support on client side, related to sales challenges • Red teaming is seen as security issue only • Client does not know who can authorize red teaming • Client does not know or cannot describe relations and dependencies to partners and service providers
Team generation	4	• Pre-planning of resources and finding right competence for the task • Scoping does not provide enough information for team generation • Schedules change and previously planned personnel might be on other assignments • It is not possible to use the most competent individuals on all assignments due to their workload • Finding time to support marketing

Adversary simulation method	4	• Attack methods and tools are not realistic • Scope limitations are contradictory to scenario with powerful attacker (e.g. APT) • Predicting future threat scenarios • Red team uses the methods it knows, which might not emulate the actual attacker
Technique, tactics and procedure generation	3	• Overall development of tools, tactics and procedures is not systematic enough • Finding resources for tool development
Documentation and reporting	3	• Lack of documentation during sales and planning initiation with client
Sales challenges	3	• Sales is too technically focused • Sales focuses only on security, when clients operative management should participate also • Discrepancy between red teaming and penetration testing • Internal communication between red team and sales • Client is not willing to pay for comprehensive testing, related to scoping problems
Business domain understanding and preliminary knowledge	3	• Red team has limited understanding of clients business domain and processes • Red team has limited understanding of clients infrastructure, e.g. SCADA systems • Client is not able to provide appropriate experts for red team planning, therefore information from target system might be inaccurate • It is possible that even the client does not have enough information about target environment

Main challenges in the engagement phase were lack of red team TTPs and process management. Internal communication is a part of leading the red team during engagement and communicating within the company. These derive from the previous phase and lack of red teaming framework with its supporting tools and repositories for sharing information. Communication with the client was a challenge along with the sudden realization of lack of defences on client side.

TABLE 7 Engagement challenges

ISSUE	n=	Challenges
Team, technique, tactics and procedure generation	5	• Red team is unfamiliar with client's technology, e.g. testing of SCADA systems • Social engineering, finding suitable methods for different cultures • Lack of common tool repositories • Need for specific tooling is identified during engagement, e.g. when planned attack vector does not work • Realistic scenario development and attacker emulation • Simulation of advanced attacker with possible future scenarios
Process management	4	• It is challenging to describe complex technical effort as an easy to understand process • Lack of clear process distracts clients situational awareness

		• Lack of process hinders red team synchronization and workflow management • Schedules are stretched, related to scoping challenges • There is general lack of standard operating procedures and framework
External communication	4	• Defining how much information (results) can be provided for the client during engagement • Client influences and directs red team during engagement • Client’s technical personnel is not willing to acknowledge shortcomings • Rules of engagement, e.g. approval to proceed if some specific case is not covered • Client creates countermeasures during engagement • Overall management of external coordination, communication and collaboration is challenging
Documentation and reporting	3	• General lack of reporting and reporting procedures during engagement • Creating connection between results and client’s business • Reporting during stretched engagements, related to scope “creep” • Handling of sensitive data
Client maturity	2	• Target systems are in artificial test configuration • Too easy to get access • Lateral movement between systems is too easy • “Zero-days” can be expoloited • Client has technical dept • Same attack work almost every time • Lack of follow-on from client side
Internal team communication	2	• Overall management of internal coordination, communication and collaboration is challenging • Lack of structure in communication and collaboration

In the post-engagement phase the main issue was ending the effort after demonstrating the flaws of the target organization. This is linked to the understanding gap how red teaming is perceived. People tend to think that red teaming is about breaking and entering whilst the main idea is to remediate the flaws discovered. Clients are not supported enough after the engagement or clients do not understand the importance of remediations and work that is required for it.

After closing the engagement with final report and presentation, there often are no follow-on activities ordered from client side. The client is left with the report and very little is done in supporting the client to implement the needed changes. This is also a client-side problem for not understanding that the remediations need supporting work also. This all comes back to the scoping and product portfolio that should be introduced before starting the effort and explaining red teaming in a more comprehensive way.

Documentation and reporting had various issues presented which can be addressed along with the demonstration of business impact. Main issue was creating good enough documentation throughout the entire assignment that would ease the reporting in the end. This also applies in creating reports that are intriguing to read by different levels in the client organization, which means understanding the business impact along with technical issues.

Final part was the team development. During engagements team members learn a lot, create new tools, find new vulnerabilities and find better ways in doing their work. These new ideas and inventions might not be documented or shared which hinders the development of the team and other teams in the company.

TABLE 8 POST-Engagement challenges

ISSUE	n=	Challenges
No follow ups	5+	• No follow-ups from client side • Inability to admit problems on client side • Lack of post mortems • Client does not buy remediations • Red team company does not sell remediations • Client fixes only the most critical findings • Client does not understand criticality of several small glitches, which can accumulate to fatal errors • No "counceling" for targets of social engineering • Red teaming is seen as stand-alone efforts
Documentation and reporting	4	• Reports are overwhelmingly extensive • Client does not understand the report • Creating of connection between technical findings and business impact • How to communicate results effectively • Creating an executive summary from huge amount of information is difficult • Lack of standardization, e.g. templates
Understanding of business impact	3	• Creating a connection between technical findings and business impact • Understanding business impact from client side • Inability to speak domain specific business language
Team development	3	• Re-usability and documentation of customized system spesific tools • No time to learn and document challenges • Finding time for in-house training

General challenge which was recognized by four of the recipients was the legislative part of red teaming and rules of engagement during an engagement. This varies depending on different national regulations and target organizations business domain.

These challenges are remediated with the input from success factors and key finding from chapter 8.1. Remediations are documented in chapter 8.2. Initial framework was created with activities and phases and presented in chapter 8.3. The product backlog was drafted but it is not complete. A single product was placed in every activity during every step to show the incremental nature of products.

7.3.2 Success factors recognized from the initial survey

Success factors and pleasant things in red teaming through the experiences of professional red teamers were reported by the recipients in slightly differing manner. Several respondents emphasized the capability and versatility of their individuals. Clear message was that quality beats quantity in red teams. The red teaming was also seen as a growing field in security and companies with good references seem to be getting a lot of attention thus red teaming creates more red teaming. One company stressed that they have a mature planning process and management tool which helps them immensely in their assignments.

TABLE 9 PRE-Engagement success factors

ISSUE	n=	Rationale
Team capability	4	• Skilled, talented and experinced teams • Cyber and physical competence, crossfunctional talent pool • Competence aids on scoping • Open source tools available • IoC's and technical activities defined on practical level
Demand for red teaming is growing	2	• Red teaming "boom" • Service or product is easy to sell • Limited competition
Communication	2	• Succesfull initial planning meetings • Documentation received from client • Setting goals with clients that have previous red teaming experience
Reputation	1	• Trusted vendor with good reputation • "word of mouth"
Planning process and tooling	1	• Clear in-house planning process and tools for red team activities • The more detailed objectives, the more detailed actions

During engagement phase the intellectual challenge in solving real security problems was a success factor which motivates the teams to do a better job. Red teamers are capable in assisting on fixing the security problems, which stresses the importance of follow on activities. Diversity of clients was a positive challenge in building up the capabilities of the team. This is linked to the continuous development of the individuals which was appreciated. Red teamers tend to be skilful individuals that are capable in independent working and therefore the flexible management and working hours were also seen as positive issues. One company replied that their management tool and automated attack repository is also a success factor.

TABLE 10 Engagement success factors

ISSUE	n=	Rationale
Tackling real problems	3	• Finding real problems which client is willing to fix • Intellectually challenging job • Exploits with social engineering are succesfull • Various sources available for target information
Honest communictaion	2	• Open communication externally and internally • Mutual respect and open working culture • Clients's are willing to hear bad news
Diversity in engagaments	2	• Variety of problem solving in different kind of target systems • Getting help for problem solving outside of the team
Flexibility of work	2	• Flexible working hours • Flexibility of working methods
Continous learning	2	• Learning from new engaments • Learning from colleagues • Development of new tools and procedures
Process and tool management	1	• In-house execution management tool • Customized automation tools • Clearly defined terminology

In post-engagement phase the presentations or final meetings were seen productive in both ways, and results are appreciated. Dialogue is needed on both technical and managerial level to spread awareness. Remediation workshops are productive, especially if they are supplemented with videos and demos. Post-engagement phase is good opportunity for internal development. One company reported to have automated reporting tool.

TABLE 11 POST-Engagement success factors

ISSUE	n=	Rationale
Presentations	4	• Red team has good capability to give feedback • Dialogue with customer on several levels, from technical experts to security management • Video captures and demo's to make impacts more concrete • Making connection between defender's and attacker's actions • Remediation workshops
Team development	2	• Continous development • Brainstorming for reporting
Awareness being spread	2	• Results are apprecitiated • Client realizes the reality of risks
Reporting and documentation	1	• Automated reporting based red teams attacks
Good follow ups	1	• Client orders further work based on results

Success factors were implemented as remediations in chapter 8.2. if possible.

7.4 Execution of Delphi-survey round 1

The initial framework described in chapter 8.3. and ANNEX 4 (detailed slides about the framework) together with ANNEX 3 - the cover letter along with ANNEX 5 (the questionnaire) were sent to the companies in April 7th year 2019. **The purpose was to demonstrate the capability of the framework to solve the comprehensiveness problem in red teaming**. This is the fourth phase of the DSRM (Peffers et al., 2007). Additional material was also sent along with results from the initial survey to present the feedback that is required in Delphi process (Dalkey, 1967). Shortened version from chapters 1-5 to elaborate details of the framework (25 pages) was also sent. The overall package was quite heavy consisting of approximately 50 pages of text. Answering deadline was set to 26th of April, but last answers were received by 7th of May. Questions which were asked in the first Delphi-round were;

1. How are you acquinted with the background material? 1-5. Open comments if any?
2. Is the CART framework conceivable? Can you understand and differentiate the purpose of continuous activities, phases, steps and products? 1-5. Please submit issues for development.
3. Give grade for the continuous activities from (1) to (5), with the help of reference grading below. Should something be deleted, combined etc?
4. Give grade for the phases from (1) to (5), with the help of reference grading below. Should something be deleted, combined etc?
5. Give grade for steps from (1) to (5), with the help of reference grading below. Should something be deleted, combined etc?

Responses were submitted with a 1-5 Likert scale with predefined meanings for 1,3 and 5 leaving 2 and 4 blanks. Open comments were also asked for each response. Questionnaire sheet is in the ANNEX 5.

7.4.1 Evaluation of Delphi 1 – answers

Delphi-survey round 1 produced some variation on responses due to different background of companies. Divergence of answers is not a problem. It demonstrates that there has not been a negative "committee effect" among the sample group. (Dalkey, 1967)

The initial answer was still, yes - The model solves the comprehensiveness problem. Maybe too well, being a bit overwhelming and covering almost all aspects of red teaming as one response phrased the issue. The numerical assessment of the framework is presented in the table below.

Question one measured the background work which the recipients committed to and that shows an average of 3,6 which means that the heavy background package was read by all.

Question two showed that the framework is understandable, and one company (4) could have implemented it as such whilst two companies (1,5) thought of it a bit obscure and crowded. The result is that the framework as such is conceivable with minor changes.

Question three affirmed that continuous activities are viable even though their substance is not fully understood. Activities were considered useful to connect the phases by company 4.

Question four proved that phases are valid, but one response was criticizing their proportionality (5) whilst other complemented the variability (4). One (1) added that phases are set up like in security consulting.

Question five assured that steps are detailed and actionable although respondents did not always understand the substance inside every step. This was not even the meaning. One response (4) noted that the line between steps is very narrow and several steps could be completed simultaneously inside a phase which is entirely correct and adaptive use of the planning process. One response (1) suggested removing the "internal development"-step from the active framework although it should be kept as a continuous activity.

TABLE 12 Numerical results from Delphi 1 – questions.

Subject/ Question	Company 1	Company 2	Comapny 3	Company 4	Company 5	Total
Background	3	3	4	4	4	**3,60**
Framework	2	3	3	5	2	**3,00**
Activities	3	4	4	4	3	**3,60**
Phases	3	4	3	5	3	**3,60**
Steps	4	4	3	4	2	**3,40**
Average	3,00	3,60	3,40	4,40	2,80	**3,44**

Even though the companies claim to have familiarized the material the comprehension has not always followed as one response (5) noted. This is most likely due to vast amount of background material and people's unfamiliarity with military or agile methodology. To raise a few misconceptions; One response (3) claimed that the attacks in engage phase have no campaign planned and are based just on gathered intelligence. In this case the responder did not understand that the campaign is planned in the previous phase and presented as the concept of operation (CONOPS). Same responder also confused the activities and phases in the replies and analysis was proposed as additional phase, when it is one element of intelligence activity.

One response (5) claimed that there are no feedback loops, or the model is not operating iteratively and would have like to have an IPO (input-process-output) loop presented. The feedback loop is in every step's retrospective and every step is its own IPO-loop which has an input from the previous step and runs through five activities as a process and gives output to the next step. Both misconceptions are not the fault of the responder, but of bad communication from the researchers. This led to the first discovery that the model should be communicated in a clear and precise way to the audience taking their background into consideration more thoroughly.

The most positive respondent (4) claimed that the framework is a great background plan but requires a mature organization to handle all the steps. It takes effort from a team to go through every step, but when done correctly the result is more consistent. The responder also noticed that the phases are the baseline of the framework and steps are the details inside the phase which complete the process. This led to the second discovery that two models should be created; 1. for the client to present what is done and 2. to the red team to show how it's done. Naturally the model 2 is the more detailed one and needs more training. This presents an old Finnish folk wisdom; *"The trick and how it's done are two different things"* meaning that what may seem simple, actually needs a lot of work in the background but it's needless to show it for the audience because then the trick is ruined.

One response (2) noted that it would be beneficial in some cases before the engage phase to provide pre-training for the client if the maturity is not sound enough. This was noted in the previous phase of the study in initial survey, but the authors simply forgot to add this element to the model. Second respondent (1) noted that the word "agile" is in the headline, but it's not mentioned in the model and could be presented more clearly. The main notion was that most of the issues brought forth by the respondents are already included in the framework, but they are hard to see, hence better communication is needed for comprehension of the framework.

7.4.2 Processing of Delphi 1 – answers

The answers were classified into themes and three main issues were discovered that were constant. These issues are depicted in the table below.

First notion is about the overwhelming nature of the framework. The model is intentionally comprehensive, or heavy. However, when conducting the joint planning process, fulfilment of all possible steps with related products is not mandatory. User can pick the things she needs from the framework if she follows the basic idea of phases and continuous activities. The product backlogs are created in the planning phase and can be adapted in the engagement phase if needed. Conclusion is that in the refined model this needs to be communicated more clearly and visualized better as several respondents (1,2,5) claimed. Also, a simplified cyclical model is needed for marketing purposes and customer relations.

The second and third issue were about understanding the substance of military way of thinking, planning and executing operations. The terminology and products like intelligence collection plan (ICP), Joint intelligence preparation of environment (JIPOE), concept of operation (CONOPS) were not very familiar to all respondents but since they form the basis of the framework they cannot be banned. Terminology can be changed, but the understanding comes through learning which requires training. For the researchers these issues are very clear due to military background, but most of the people in ICT-business do not have a military background. Therefore, better communication of the model and its terminology are pursued.

TABLE 13 Issues for remediation from Delphi 1 - questions

ISSUE	Rationale
Framework is heavy (5 respondants)	• Picture is crowded • Requires good maturity from the red teaming company • Difficult to sell for clients • Challeging to implement • Contains too many elements
Activities are obscure (4 respondants)	• Idea of continous activity is not obvious • Targeting not understood, could align with intel. • Activities and products of different phases and are not understood • Presenting of stakeholders might help to understand the model better i.e. Chief intel, red team leader, etc.
Military terminology and agile events not understood (4 respondants	• Intelligence cycle or products are not familiar to recipients • Retrospective role as feedback/iterative mechanism not understood • Planning products (COA, CONOPS) not understood to be the campaign plan.

All the presented issues are real, and they lead to two questions:

- Is the initial CART-model too complicated?
- Was the initial CART-model communicated properly for the companies?

The framework was complimented by comprehensiveness noting that it requires maturity from the red team as well. This led to the following conclusions that are implemented in the next Delphi round:

1. Create a simplified cyclical model for presentation.
2. Implement minor changes suggested by the respondents.
3. Highlight that completion of every single detail is not needed to complete the framework and it's just a framework for flexible use.
4. Create a training program for the model for the red teams if someone tries to implement the framework in practice.

7.5 Execution of Delphi-survey round 2

The second survey round was conducted as a briefing to the companies in five separate onsite presentations during May and June 2019, each lasting approximately 35-45 minutes. The presentation consisted of short feedback from the previous phases of the research and results which is a pre-requisite for a delphi-survey (Dalkey, 1967).

First goal of the presentation was to enhance understanding of the framework which was noted inadequate on the first round. Second goal was to find out if the framework is too complicated even when explained. Third purpose was to evaluate the benefits and deficits of the framework according to the 5th phase of DSRM (Hevner et al., 2004).

Brief basics of agility, agile scaling and water-scrum-fall were presented before advancing to the simplified model. This was to make sure that the audience could connect the agile functions in the model to the framework that was presented.

Simplified model highlighted and explained the phases and cyclical nature of the framework. Activities, steps and related products derived from military and agile methods were explained in the revised complete framework. This created understanding in how military and agile methods support the framework.

Presentation ended with takeaways from the framework. All presentations were interactive, and audience was encouraged to ask questions and present comments throughout the presentation, which they did. The presentation is depicted in ANNEX 6. After the presentation approximately 45 minutes was spent in answering the five presented questions. This phase was conducted as a semi structured interview. The questions are presented below:

1. Did the presentation clarify the model?
    - Grade 1 – 5
    - What is still obscure?
2. Does the comprehensive CART framework offer improvements to red teaming activities?
3. Do you see any benefits in using military methods (planning, intelligence and targeting) to develop red teaming?
4. Do you see benefits in using agile methods to develop red teaming?
5. Final words on comprehensive agile red teaming framework.

7.5.1 Evaluation of Delphi 2 – answers

Question one measured the effectiveness of the communication and presentation of the model to avoid misconceptions. The presentation received a very positive feedback and several respondents claim that it's more time efficient and understandable to present a complex and new issue in 30 minutes than spend several hours in reading the background material. Presentation of the agile principles and the new cyclical model were considered to be clarifying steps. Grade of the model from the all the five companies was a constant 4,0. All the respondents claimed that they understood the phases, activities, steps and agile factors of the model. Some obscurities were noted which do not have a major impact in creation of the framework. Most of the obscurities were detail level questions and implementation of the model into practice which are out of scope and subject to future research.

Question two, three and four evaluated the positive impacts and improvements of the framework in red teaming. Several issues were noted, and the framework is seen as a development in red teaming activities. Most beneficial issue mentioned by all was that the structured model is possible to repeat and use flexibly.

Question five presented the respondents a possibility to express feedback of the research process and any other issue they saw fit to express. Respondents raised several topics which call for future studies.

The onsite presentation proved to be an effective way to communicate the model instead of background reading material package that may cause misunderstandings.

7.5.2 Processing of Delphi 2 – answers

Answers were collected after the presentations from the five audiences and they were documented by the researchers. All answers were collected into document which listed the obscurities, benefits and miscallaneous comments. Results are depicted in the text below and on the associated tables.

Obscurities after the presentations were mostly about details of the products and activities. There were also questions on how to implement and lead a team with such a framework. That is out of the scope of this research and calls for future studies. The main conclusion about obscurities is the same which was noted in the first Delphi-round; If this model is to be implemented, it needs to be trained for the teams. Probably the best results would be achieved in a workshop style training session where all details are communicated, and the model is aligned to the target organization's needs.

TABLE 14 Obscurities in the CART framework.

Obscurity	Rationale
Focus	• Several activities and lot of products to digest, need for training • What is the most relevant thing to do, and what can be skipped if process needs to be streamlined? • Rules of thumb needed for different steps
Implementation	• How to adopt the model into practice? • How should the steps be timeboxed? • How do you lead such a team / organization? • The client interface and communication was left a bit open
Products	• Intelligence, planning and targeting products are seen useful and structured but their contents require training. • What are the most valuable deliverables to the client?
Terminology	• Some terms were used differently than respondents are used to • Terminology needs to be defined and trained

	• Agile terminology or methods are not always known by red teamers

Benefits of the framework are listed in the table below. Several comments were about structural nature of the framework, which can be seen in the planning, intelligence and targeting. All military activities were seen useful if properly adopted. Planning, intelligence and targeting products that were presented received a good feedback and were considered usable. Product platforms and agile methods were seen useful in creating transparency in the workflow, both for the red team and for the client.

Cyclical nature of the model and phases were seen important, because currently majority of red teaming effort revolves around the engage-phase. This creates inefficiency to planning and implementation of the results. Amount and training of personnel that is needed to conduct different phases can also vary. In provide-phase the red team might need more security developers than penetration testers. A thorough planning phase might also reduce unnecessary work in the engage phase. Water-Scrum-Fall was seen useful basis due to it emphasizes planning and provide phases, while keeping the engagement agile and team driven.

Respondents agreed that there is a need for common taxonomy for the process which would make the management of red teams easier. Taxonomy would be useful in creating backlogs and would help in planning the resources during missions. Due to several novel issues in the framework all the respondents agreed that the model needs to be trained for the teams if proper implementation is sought for.

TABLE 15 Benefits of the CART Framework.

Benefits	Rationale
General	• The framework formalizes several issues that are already done but not documented • Framework makes it easier to train red teaming with common taxonomy and terminology • Scoping in two steps helps to really map the customer need and provide the most useful service • Additional sales are possible by emphasizing the provide phase • The cyclical nature and importance of plan and provide phases is essential in creating better red teaming engagements • Structured process makes it easier to involve right people to different phases and steps which creates efficiency • Utilization of platforms in communication, workflow and knowledge management creates efficiency • Framework creates transparency towards client • Framework creates means for assessment and development of internal processes • Creates formula of success; "if you commit all the steps and develop all the products, you win" (which is a heavy process)

Military	- Structural planning creates a good process which is easy to manage and communicate for the team - Need to lead the red team in a more efficient way - Intelligence process is needed with structured intelligence questions and incremental products to manage the collection more effectivly. - Targeting process creates structured focus and visualizes the environment and effects more consistently and helps with impact reporting - Common taxonomy and terminology clarifies the process and it's easier to communicate if everyone knows the processes and talks about same products (potentially shippable increments) - Military methods were acknowledged to be combat proven and therefore useful in practice as well
Agile	- Visualization and transparency of the workflows brings benefits for teamwork - Roles in agile teams can be utilized such as scrum master - The backlogs help in scoping and workflow management - Scaling is good for continuous development of company portfolios and personnel usage - Water-Scrum-Fall makes the Plan and Provide phases more relevant and more realistic - Scaling is useful in personnel management during multiple simultaneous engagements

All the respondents gave open feedback which some are out of scope like the business issues which this framework does not solve. The research process was commented by complementing the initial survey and Delphi-2 phase. Delphi-1 was seen too heavy and difficult, which was noted by the researchers also. All the respondents admitted that their comprehension of red teaming evolved during this research process and new ideas surfaced.

The need for training and means to deliver it for red teaming companies was discussed. Several ideas rose from the discussions. The main message for communicating and training a new framework like this was; Don't assume anything. If you are to train this framework it is prudent to acknowledge that the target audience is going to be very heterogeneous and there is a need to start with the basics of agile and military methods during the training sessions. A case study to conduct a red teaming assignment with the framework was also proposed.

TABLE 16 Open issues about the Framework and the project.

Open issues	Rationale
Research process	- The initial survey and delphi-2 were good rounds. Delphi-1 was too heavy for the respondents - One hour of clear F2F-interaction was seen better than 50 pages of reading - The process was communicated in a clear and concise way to the respondents and it was easy to follow

	• Tunnel vision has been broken with technical experts, bigger scope gives depth to red teaming work
Training	• Need for training was identified in companies • Should training be lectures, workshops or tabletop games? • Map the knowledge level before training session. Training needs to be customized. • Provide taxonomy and templates for products • Case study would be good to test the model in training
Don't assume	• RT Personnel most likely do not know anything about military planning, intelligence or targeting • RT Personnel might know very little about agile processes or project management • If people read material, they might understand it different than the author intended
Business	• How do we involve business impacts to red teaming? • How can we make this simple enough to sell it? • If the scope of task is small, the framework is too heavy • Creates positive image of red teaming • Change of scope in real life might prove to be hard

The processed answers were meant to respond for these two questions that were raised during the first round and evaluate the usefulness of the framework.

- Is the initial CART-model too complicated?
- Was the initial CART-model communicated properly for the companies?

Result is that with a better communication the modified framework is conceivable, but it needs training if red teams are to utilize it. The usefulness of the framework was undisputed but adaptation of the framework to practice needs further research.

7.6 Reliability and validity of the research

Reliability means that results from the measurements can be replicated. (Hirsjärvi, Remes, & Sajavaara, 2004). Internal validity means that research method gives purposeful knowledge. External validity means that view of the subject and conclusions are credible. (Flick, 2006) Delphi method was the most important tool for testing reliability and validity of the construct for which it is suited for (Hirsjärvi et al., 2004).

This is a qualitative research where reliability is hard to assess. Therefore, it is important to note the references of literature and where does the researchers' interpretation begin when doing the reporting (Flick, 2006). This was done by separating the literature study and its results in several tables as possibilities and key findings. The literature study can be read from chapters 2-6 and the conclusions to framework creation can be seen from chapter 8 tables.

The replication of this study is possible but not completely due to surveys taken. It would be hard to discover matching research setting. The literature study is simple to replicate and similar conclusions might be discovered.

In qualitative research it is important to describe how the research process was carried out, and how the conclusions were drawn based on the theoretical background (Hirsjärvi et al., 2004). This whole process is depicted in detail in chapter 7. The design science research and information system research framework are introduced in chapter 7 as well. Several intermediate products (tables) are depicted to support the reasoning behind the conclusions. This builds reliability.

Procedural reliability in design science requires the theoretical background of the environment and descriptions of the methodological choices which were utilized (Flick, 2006). All of these are depicted in this chapter. Based on these claims the reliability of this study is at a reasonable level and the results can considered credible.

Important thing about validity in qualitative research is triangulation. (Hirsjärvi et al., 2004) In this study triangulation was used not only for different data sources for document analysis, but also for methods; DSRM, information systems research framework and Delphi method respectively. The use of multiple researchers creates researcher triangulation. Systematic triangulation is an efficient way to increase validity. (Flick, 2006; Denzin, 1978)

Most important tool for testing external validity, and to some extent reliability, is evaluation of the created construct with Delphi-method. Delphi SME's are security professionals, therefore intentional misleading is not foreseen. Researcher's own point of views do not affect the SME's in any way. Validity of the Delphi-method is assessed to be credible enough. (Denzin, 1978) Internal validity means that research method gives purposeful knowledge (Flick, 2006) DSRM was selected in conjunction with Information systems research framework for methodology because this study aims in creating new knowledge, which it did.

Transformability and confirmability can also be considered to measure validity. (Flick, 2006) The red teaming framework could be utilized outside information systems in physical security also, so transformability is possible. This supports the validity of the framework. Confirmability is harder because we have not been able to find previous research on the subject with this wide a scope.

7.7 Conclusions

The research was conducted in a clear and concise phases starting with the literature study. This was followed by the creation of the initial CART framework from the basis of initial survey. Survey results were supported by the information gathered from the literature study. After this the reliability and validity was tested in two rounds of Delphi-questionnaire.

Interest and commitment of the five companies was positive. Their participation was crucial for gaining practical knowledge, insight to red teaming activities, and finding out success factors and actual challenges for remediation. Critique can be subjected to the sample size of questionnaire. For practical reasons all companies were from Finland, and the group of operators is narrow. Second subject for critique is the conduct of first Delphi round via email. Background material needed to comprehend the model was extensive, and questions were understood from different perspectives which created misunderstandings with some issues. A need for red teaming lexicon was raised, which is beyond the scope of this study.

Initial survey and second Delphi round were successful as they were conducted with an onsite briefing beforehand. Delphi 2 was the most successful and interactive round. Possible misconceptions were sorted out immediately. Questionnaires did not receive critique from the respondents.

Initial survey produced the most valuable information as it detailed out real world success factors and challenges for remediation. First Delphi round was burdening for the respondents, but it highlighted the need for a simplified model which was created. However, main question was solved, the created model is comprehensive.

Second Delphi round's main result was that the framework is functional. However, it is heavy, which was intentional as it was created to solve the comprehensiveness problem. Framework is suitable for large scale engagements, but its implementation calls for training and adaption to different companies existing functionalities.

The design science together with information systems research framework created a functional framework for the study as they aim to build new knowledge and artifacts. Intermediate results were reported according to phases of DSRM and in context of IS research framework. The scope of this study is wide and therefore results can be considered only general. (Siponen & Klaavuniemi, 2019) Still the results can be considered reliable and valid for future work. Future work is needed in several areas such as implementing the model into practice.

8 RESULTS OF THE RESEARCH

> *"Well, we never promised comfort. You can choose comfort, or you can choose to win"*
>
> *-Vijay Govindarajan and Chris Trimble-*

This chapter presents the results and intermediate results from the study. Research problem was; How to create a comprehensive, agile red teaming model by combining adaptive planning and execution framework in information security context. The answer is the process of this study and the result is the comprehensive agile red teaming framework (CART) depicted in chapter 8.6. and ANNEX 6. Research questions are reviewed in the table below with the chapter number where the question was addressed and focus of the chapter.

TABLE 17 Research questions and results.

Research question	Chapter	Result
1. What are the factors that need to be considered when implementing red teaming into information security management?		
1.1. What is comprehensive red teaming?	Chapter 2 Knowledge	Creating better plans, policies, procedures and products in any domain by challenging the current ones.
1.2. What are the areas in information security management that can utilize red teaming?	Chapter 3 Environment	The entire security life cycle and risk management. Details in table 4 and 19.
1.3. How red teaming efforts could be adopted into information security management?	Chapter 4 Knowledge Environment	Diagnose, Challenge, Create. Integrate red teaming into processes. Details in table 18.
2. How can adaptive planning and execution framework together with agile methodology support the creation of better red teaming process?		
2.1. Which military processes or activities could be considered in red teaming?	Chapter 5 Knowledge Exaptation	Planning, execution, Intelligence and targeting. Details in tables 20-21.
1.1. How agile methodologies can support red teaming?	Chapter 6 Knowledge Exaptation	With several products and working principles. Details in table 22.
3. What kind of process is needed for comprehensive scalable red teaming, and how does it make red teaming better?		
3.1. What calls for improvement in current red teaming efforts?	Chapter 7 Improvement	Issues according to initial survey-Details in tables 6-11.
3.2. How does the study support the development of a better red teaming?	chapter 8 Improvement	Study makes red teaming structured and transparent. Details in tables 23-27.

First research question was answered by the chapters 2-4. Comprehensive red teaming is introduced along with information security management and risk management relation to red teaming. Possibilities to apply red teaming to information security life cycle was recognized.

Second research question was answered by chapters 5 and 6. Adaptive planning and execution framework, intelligence, targeting and agile methodology are introduced as means to support red teaming. Key findings for the framework creation were drawn from these chapters.

Third research question was answered by chapters 7 and 8. Initial survey presented the challenges to be solved. Challenges were remediated by creating a framework with support of the literature sources and evaluating it with two Delphi iterations.

8.1 Key findings from the literature study

The key findings presented in this chapter were applied as remediations to the challenges presented in tables 6-11. Findings are shortened versions of the chapters 2-6 and they try to present the thinking process of the researchers and manage traceability and reliability of the research process.

Red teaming was covered in chapters 2 and 4. Key findings that can be adopted to the framework creation are depicted in table 18 below. Details can be found from chapters 2.6 and 4.5. Conclusions are that red teaming is a cultural change which challenges the organization and its norms, and this is needed against adaptive adversaries and guard the against complacency. (Defense Science Board, 2003) This means that the red teaming is no longer considered a one-time consulting work but a continuous process within the organizations security life cycle. This requires the commitment of the management.

Diagnostic and creative aspects need to be emphasized (Development Concepts and Doctrine Centre, 2013) because red teaming is adversary emulation and a decision support element (Fleming, 2010). Purple teams that combine the red team and the defender's assets are the next evolution step which creates better understanding of threat in the defender-side. Red teaming is not supposed to be an audit mechanism, but sometimes it can also support auditing. (Caron, 2019)

Use of outsiders or changing the processes that insiders can act as outsiders can mitigate biases better (Kahneman et al., 2016). The process needs to be accepted in an organization to make it a success factor in mitigating own biases and noise.

The modern APT studies and technical red teaming studies bring forth the advanced technology like automated attack and simulation tools that can be used in planning or simulation of attacks. (Randhawa et al., 2018) Plethora of tools and attack planning repositories are available. (Bertoglio & Zorzo, 2017; Mitre, 2018) Social engineering and physical security testing need to merge with any red teaming activities in information security as well (Krombholz et al, 2015).

TABLE 18 Key findings from red teaming.

KEY FINDINGS – RED TEAMING
Red teaming is a process, not a project.
Support and empowerment by the management
The process needs to be formalized and enforced
Red team needs to be outside of the organization but still inside and aware.
Adopt the purple team – thinking
Divide actions to diagnostics, challenge and creative activities.
Red teaming can be adopted to all sections of security life cycle
Use of automated red teaming tools to plan the real world engagement
Can be used as part of assurance and auditing
Use versatile tooling and have a big repository of tools and TTPs
Social engineering and physical penetration testing as a force multiplier

Effective information security can bring net benefits for an organization. Therefore, the efforts must be reasoned for management which decides on investments and policies. Cyclical risk management can be used for creating a link to business objectives, which enables implementation of prudent managerial and technical controls. One needs to acknowledge that future risks cannot be derived from the past, adversary emulation is an example of a method to simulate evolving threats. User participation to creation of policies and controls is encouraged for better implementation of security. Training and awareness programs should address the realistic threats and threat landscape presented by the adversary emulation phase.

TABLE 19 Key findings from information security management

KEY FINDINGS – INFORMATION SECURITY MANAGEMENT
Net benefits can be achieved from information security efforts. Buy-in needs to happen
Cyclical nature of information security management and policies is a prerequisite
Risk driven policy development - closely related to business objectives
Identify threats, assets, vulnerabilites and business impacts.
Development and deployment of controls through risk assessment
Future risks cannot be derived from the past. External atttacker to simulate future risks.
Practical tools for implemention are technical and managerial controls
Effectiveness of controls has to be monitored
The necessity of Policy enforcement – No sanctions → No effects.
Training and awareness are needed support policy implementation
User participation in creating policies and controls is effective

Adaptive planning and execution framework brings versatility to management of a process which has several interdependent activities and phases. Phases and steps help to break down the problem and give structure to the operation. Structured activities bring common terminology which makes the communication and management easier. The framework and steps might seem cumbersome, but the framework is flexible, and completion of all steps slavishly is not the purpose.

Planning and execution of plans is based on continuous orientation of the changing situation. Planning horizon needs to be considered. There is no point in making detailed plans into far future. Longer the horizon, more general the plan. Planning is still needed, and various courses of action need to be considered to create options for execution. The execution is referred as mission command where leader drives the processes and team conducts the operations independently. Effective mission command requires a system of processes and networks to support the information management within the team.

TABLE 20 Key findings from adaptive planning and execution.

From	KEY FINDINGS
Adaptive planning and execution framework	Framework is better than process because it's more versatile than a process flowchart.
	Phases and steps help to break down the assignment
	Completion of all steps slavishly is not an intrinsic value
	Synchronization of continuous activities in every step creates the continuity for the framework
	Planning, intelligence, targeting and execution are interdependent
	Operational design and operational art needs to be remembered
Joint planning process	Terminology (COA, CONOPS, etc) needs to be defined
	Planning is a process that does not stop in creation of the plan
	Planning defines the endstate like scoping
	Structured planning enables better informed decision-making
	Several COA:s need to produced which add to the portfolio
	Planning horizon needs to be noted. More general further ahead.
Mission Command / Execution	Leader drives the process, team conducts the operations.
	Continuous knowledge and information management is needed for the command, control and communications
	Mission command requires a system to be efficient
	OODA-loop and importance of constant orientation change
	Leader needs to plan-prepare-execute and assess constantly
	Continuous assessment of all activities develops team and process

Intelligence and targeting are interlinked and structured activities that support planning and receive guidance from it. Both activities are structured and have predefined products to every phase of the assignments that can be used (JIPOE, ICP, FA, TSA, BDA, etc.) Intelligence and targeting products require a platform to be transparent. This also enables better situational awareness and reporting by pulling instead of just pushing.

Joint targeting cycle enables the target system analysis and target development attached to planning and intelligence. Target folder generation and weaponeering receive a proportional slot from the process and can be outsourced. Integration of the kill chains and battle damage assessment creates a transparent reporting function for the process.

TABLE 21 Key findings from intelligence and targeting

From	What
Intelligence	JIPOE as the business understanding and technical picture
	Intelligence planning, direction and collection management (ICP)
	Situational awareness activity and relation to intelligence
	Processing, exploitation, analysis activities defined
	Push & pull reporting and production requirements
Targeting	Joint Targeting cycle and relation to other activities
	Target system analysis and target development
	Target folder generation and weaponeering
	Integration of kill chain to joint targeting cycles
	Battle damage assessments

Agile methodologies are suitable for projects that utilize crossfunctional teams and adaptive planning. Agility, military planning and execution have several similarities and are possible to merge. Scrum and Kanban are useful in team level workflow management with backlogs and Kanban boards which make work visible and transparent. These boards can also be thought as collaboration platforms if used in networked environment. Sprints are an efficient way of controlling the change during planning and execution.

The continuous integration, delivery and development from agile scaling is efficient way of producing parallel products and processes like intelligence, targeting and plans. Scaling makes the portfolio, backlog and personnel management more transparent as well. Water-Scrum-Fall model relates better to the restrictions which red teaming engagements have than pure agile models.

The main idea of agile integration to the framework is not to slavishly follow any fixed agile method but a mix of them any which way the user sees fit. This means for example modifying the sprint lengths or adding to the backlogs during a sprint etc.

TABLE 22 Key findings from agility.

KEY FINDINGS – AGILE METHODOLOGY
Continuous; Integration – Delivery – Development (CI/CD) (Platforms)
Product backlogs and sprint planning to shape the task and make it transparent
Crossfunctional teams and usage of personnel flexibly in different phases
Retrospectives and sprint reviews as a means to communicate to client and improve
Water-Scrum-Fall emphasizing the need for planning and remediation of findings
Scalable enterprise framework to create portfolios and repositories for basis of the work
Similarities in agile and military methods are evident
Flexible adaptation of agile methods

8.2 Remediations to red teaming challenges

The framework was created based on results from the initial survey answers and findings from the literature study. Initial survey raised several challenges. Remediations are introduced from the literature sources and success factors from the initial survey answers.

From the five meetings during the initial survey the main notion was the unstructured way in managing red teaming efforts. This does not mean that the efforts are ill managed, however a process with clear steps, activities and products were missing from most organizations. This was the starting epiphany in creating a framework instead of plain process for comprehensive red teaming.

Issues from the initial survey were sorted and compared between challenges and success factors. Issues were then sorted to meet larger categories which are presented below in tables 23-27. Remediations are proposed to mitigate the issues. Remediations derive from the literature study notions from tables 18-22 and from success factors of the survey (tables 9-11).

Emphasis of the remediations were in the pre-engagement phase, which had most answers by the recipients. The pre-engagement phase was split into three parts; Internal development, scoping and mission analysis for the convenience of addressing issues. In the final model, this part is called as the plan-phase

First part of pre-engagement had to do with red teams' internal issues that need to be sorted out in order to provide a clear and concise picture to the client and sales personnel about red team capabilities and product portfolio. Team also needs to create functional TTPs, tools and repositories to manage their efforts. Issues are presented in detail with remediation suggestions in table 23 below. These are the issues that need to be addressed in a company to have a red team with suitable TTPs, tools and a management process in place. When a clear red teaming service portfolio with supporting information system is in place it is simpler to communicate that to the client side and support team development.

TABLE 23 Analysis and remediations of the pre-engagement phase 1(3).

Internal development Issues	
Issue	Remediation
Adversary simulation method	1. Create various courses of actions for adversaries
	2. Company Internal threat intel process needs to be combined with red teaming adversary emulation.
Technique, tactic and procedure generation	1. Create repositories for sharing tools
	2. Establish target architecture attack lab
	2. Create attack matrixes that can be automated
	3. Operations and campaigns to be saved and developed to for later use.
Documentation and reporting	1. Use living documents and publish products in every phase of the process to support information sharing

	2. Red team leader designated to oversee documenting and fixed templates.
Sales challanges	1. Train sales personnel internally
	2. Involve sales personnel to RT retrospectives and LI/LL – events.
	3. Create understandable service packages for the sales.
Team capability	1. No restrictive process or management model to maintain agility and initiative of red teamers.
	1. Assign “product ownership” responsibilities to activities for most qualified personnel
	2. Use crossfunctional teams to enable sharing of knowledge
	4. Organize “Lesson learned / trainings” - repository
Communication	1. Develop initial meetings with client to involve more personnel to share information
	2. Communicate red teaming efforts internally
Planning process and tooling	1. Create a flexible process with distinctive phases. Preferably phasing is aligned with service portfolio.
	2. Use a management tool for command and control of your red team activities to enable transparency and information sharing.

Second part of pre-engagement was the scoping issue. The internal issues for example a service portfolio is needed to support the success of scoping phase. Preliminary knowledge about clients’ business domains needs intelligence effort and crossfunctionality to be addressed properly in both technical and businesswise. Technical security is too a narrow view to support business goals.

The maturity level of clients’ security is a dictating factor on where to start the security consulting. If maturity is low, there is no need for complex attacks due to lacking controls and the effort needs to start from thorough assessment and support rather than attack. Communication is the key element in defining the means and ends of an engagement in order to let the red team figure out the ways themselves in how to execute the task. Issues are presented in detail with remediation suggestions in table below.

TABLE 24 Analysis and remediations of the pre-engagement phase 2(3).

Scoping issues	
Issue	Remediation
Business domain understanding / Preliminary knowledge	1. Intel gathering before client meeting about business domain and market status and generally from target systems
	2. Involve business and technical personnel to the scoping meeting
	3. Learn business specific models (Like ECB TIBER-EU for Finance)
	4. Compliance and legal status in business domain needs to be clear before planning actions.
Client maturity review	1. Start by review of client security if maturity is low. Do not start red teaming engagement if protection is not mature enough.

	2. Define applicable COAs to present for the client pending on the results of initial information gathering.
	3. Client presentation about company and security policies and 3rd party involvements
Communication	1. Provide information about red teaming in advance
	2. Create understandable and flexible service portfolio to offer (COAs) with initial timeframes.
	3. Create shared understanding with transparent and living documents, plans and reports.
	4. Involve business and security personnel
Defining scope	1. Set the objectives and timeline. After this make the mission analysis and propose with a plan.
	2. Support user participation from client side in setting the scope

Third part of pre-engagement is the mission analysis prior to engaging in the assignment. Mission analysis can be done as part of the scoping or after the scoping with the client. It's imperative that mission analysis results are presented to the client before actions are initiated in order the client to understand the red teams' future actions.

The mission analysis derives mostly from the military side in preparing the battlefield which is described as the JIPOE – Joint intelligence preparation of the environment. JIPOE creates the basic understanding of the operating environment and supports to target system analysis which supports to factor analysis that defines business impacts from different systems affected. Intelligence collection plan (ICP) drives the intelligence. Environment assessment creates basis for plan and team generation. These are needed to produce the courses of actions that can be delivered. To ease the execution and manage effort a product backlog is formed to state clearly the deliverables. These artifacts need to be available to the team and the client and therefore a collaboration platform and a management tools is needed to support the working. Importance of communication is stressed again and permanent points of contacts (PoC) should be established to handle the communication between the team and the client. Issues are presented in detail with remediation suggestions in table below.

TABLE 25 Analysis and remediations of the pre-engagement phase 3(3).

Mission analysis issues	
Issue	Remediation
Technique, tactic and procedure generation	1. Choose Adversary simulation method (COA)
	2. Intelligence collection plan and collection matrix
	3. Target system analysis and factor analysis
	4. Define business impact through factor analysis
	5. Mitigate legal issues and how to simulate effects
Planning process and tooling	1. Review previous assignments
	2. Develop the modified concept of operations refined from COA.
	3. Use management and execution tool
	1. Create product backlog

Documentation and reporting	2. Establish continuous online reporting channel to client PoC.
	3. Document all products
Communication	1. Define a PoC from client and RT
	2. Support clients' internal communication
Team generation	1. Assign personnel and plan use in different phases
	2. Partnering and outsourcing if needed
	3. Involve junior consultants to crossfunctional teams

Engagement phase needs a clear and concise process with fixed sprints and product backlog to be manageable and avoid time thievery. Transparent reporting system is key in upholding the situational awareness and documenting actions. Internal and external communication systems need to establish to manage team and client issues as they arise. Planning needs to be flexible and revised throughout the engagement and this requires constant assessment of own and opponents' actions. Continuous integration of activities and continuous delivery of products eases the final reporting phase. Issues are presented in detail with remediation suggestions in table below.

TABLE 26 Analysis and remediations of the engagement phase 1.

Engagement	
Issue	Remediation
Process management	1. Create framework process with continuous activities, phases and product backlogs.
	2. Red team leader drives the process, team conducts activities
	3. Define Fixed Sprints with goals to manage time and resources.
	3. Establish daily meetings to support teams' situational awareness (and clients').
	5. Develop assessment activity which is supported in sprint retrospectives
	6. Build transparent workflows and share them with client
	7. Assign one sprint for closure activities
Documentation and reporting	1. Continuous collection / reporting platform in use
	2. Need to publish reports from platform – Continuous delivery
	3. Reporting about own TTPs and Malware used (storyboards) with battle damage assessment
	4. Transparency in reporting. Client is given good visual on RT and participated in Retrospectives
	5. Business impact evaluation
	6. Remediation plan produced for hot washup.
External communication	1. Dedicated POC for the RT (RT leader) and client
	2. Increase awareness about RT to client
	3. Need for intermediate reviews after sprints
Internal communication	1. Red team leader facilitates activities
	2. Clear management structure
	3. Collaboration platform in use
	4. Tooling platform in use
	5. Reporting platform in use
	1. Develop reachback capability in your company

Team, technique, tactics and procedure generation	2. Prepare risk management plan for the assignment
	3. Prepare to simulate effects
	4. Emphasize on mission analysis to mitigate problems pre-emptively
Client maturity	1. STOP testing if there's nothing to be tested and be honest to customer --> Recommend Review and support functions instead
Flexibility of work	1. Support agile working environment
Continous learning	1. Develop assessment activity which is supported in sprint retrospectives
	2. Create storyboard templates and populate them during engagement. Supports to reporting as well.

Post-engagement is named as security implementation because it gives a more meaningful description of the goal of the phase, which is to provide for the client, not just present. Red teaming should aim to fix things, not just to point out flaws. This is the main idea of the post-engagement phase. Ending presentation should be just a hot washup where an intermediate result from flaws is presented along with a remediation plan with a timeline and proposed action items. The communication of results needs to start from the business impact which makes it easier for the C-level leaders to understand the needs for corrective measures if there are any. In the final model, the phase is called as the provide-phase.

Documentation and reporting along the assignment need to be communicated in small pieces that in the end the client does not receive information avalanche which is hard to digest. Constant flow of information is easier to receive, and corrective issues can already be sent to risk analysis process or other assessment functions which the client has. Follow-on activities should be tailored by the needs of the company and if policies or controls are altered, they should be communicated and trained to the clients' employees as well. Red teaming activities should raise security awareness and therefore internal and external communication needs to be considered.

Final issue is the continuous development of the red team or the red teams of the company. This requires a lessons-learned and internal training function in the red teaming company. Training should be a way to increase the capabilities of the team and not as a secondary function which is done if there is no engagement work in the backlog. This mindset requires that the red teaming effort includes the internal development phase which is between engagements. Issues are presented in detail with remediation suggestions in table below.

TABLE 27 Analysis and remediations of the post-engagement phase.

Security implementation	
Issue	Remediation
Presentations	1. Involve right personnel from all levels
	2. Use Demos and storyboards from engagements
	3. Deliver both technical and business presentation
	4. Provide presentations in retrospectives throughout the assignment so that final presentation is not too heavy

	5. Provide remediation plan with phases and actions, not just controls to be implemented or problems to be solved.
Reporting and documentation	1. Create a connection between technical findings and business impact.
	2. Report corrective technical measures.
	3. Continuous reporting, keeps client informed and end report is already largely known previously.
	4. Provide reports to different levels (report structure)
	5. Constant logs of malware used in order to clean the environment after the assignment
	6. Use crossfunctional team with understanding of business impact
Follow ups and remediations	1. Support customer in risk analysis and management
	2. Provide implementation support for controls and monitoring and removal of outdates controls.
	3. Provide awareness program from engagement lessons
	4. Provide training simulations and tabletop exercises from engagement lessons in different levels.
	5. Debrief on social engineering & other effects in order to clean systems up and inform clients' personnel
	6. Show business impact on reports and briefings.
	7. Support customer in implementing controls
	8. Show impact with exploit demos.
	9. Demonstrate how several small problems can accumulate to fatal errors.
	10. Support in internal auditing.
Team development	1. Share knowledge through lessons identified and lessons learned workshops / storyboards.
	2. Document different tools purpose and functions
	3. Support multifunctional team development.
	4. Draft reports as team effort.
	5. Create a living process framework that is developed constantly
	6. Reserve time for own development. Ending sprint.
	7. Red team and assess your own actions
Red teaming awareness	1. Give non-confidential briefings on seminars etc.
	2. Plan media coverage beforehand.

Issues and remediation suggestions from these five tables were analysed and a preliminary framework was created with activities and phases. The product backlog was drafted but it is not complete. A single product was placed in every activity during every step to show the incremental nature of products.

8.3 Initial CART-Framework

The initial model was formed with the purpose of solving the comprehensiveness problem in red teaming. Model is simple and does not include all the recognized challenges and remediations because the first goal was to see if the framework idea is conceivable. Initial model is depicted in detail in ANNEX 4. CART framework version 0.1 consists of:

- Five continuous **activities**
- 1 baseline and 3 active **Phases**
- 13 **steps** that are divided under the phases
- **Products** that are defined in the backlogs

The model is constructed with the following ideas:

1. A framework needs to be produced with continuous activities, flexible phases and product backlog to gain comprehensiveness.
2. Consecutive phases receive input from the previous ones. This emphasizes the importance of structured process, initial analysis and planning.
3. Structured problem solving requires defined steps inside phases with fixed activities and products in order to be understandable and repeatable.
4. Red teaming cannot stop in presentation of the engagement results.
5. Nothing happens if management does not buy-in the red teaming idea. Therefore, the framework needs to be easily communicable.

8.4 Refinement of the framework after Delphi 1

As presented in the chapter 7.4. Delphi-survey round 1 proved that the initial model solves the comprehensiveness problem. Maybe too well, being a bit overwhelming. Therefore, major changes are not implemented to the next version in substance, but of visualization and training.

The initial model was communicated poorly to the recipients and their backgrounds were not noted enough. The lack of understanding in military planning, intelligence, targeting and agility was unforeseen by the researchers. This will be remediated because the goal hasn't changed to produce a comprehensive model as a framework. Remediations for the model are as follows:

1. Build two models.
    a. Simple for the customer, ("The Trick…") Figure 43.
    b. Complex for the team, ("…and how it's done") ANNEX 6
2. Present the model more clearly to avoid the misconceptions.
3. Implement the feedback loops to the model and explain the existing process better.
4. Drop the internal development step from the simple model but have it as the baseline capability in the complex model.
5. Assign minor alterations as suggested by the respondents.
6. Accept that the framework needs a training session which clarifies terminology, products and the essence of the framework.

The refined model was formed with the purpose of communicating the model in a better way. The overall model was changed with according to remediations above. The model is constructed with the following ideas:

1. A framework needs to be produced with continuous activities, flexible phases, steps and product backlog to gain comprehensiveness.
2. Consecutive phases receive input from the previous ones. This emphasizes the importance of structured process, initial analysis and planning.
3. Structured problem solving requires defined steps inside phases with fixed activities and products in order to be understandable and repeatable. Steps control the change during process and scope can be altered.
4. Provide is the most important phase for creating better security. Engage and Planning phases are tools to provide.
5. Management needs to buy-in the red teaming idea. Therefore, the framework needs to be easily communicable and to right personnel.
6. Red teams need to be educated in use of the complete framework.

The refined framework is depicted in ANNEX 6.

8.5 Results from Delphi round 2

As presented in the chapter 7.5. Delphi-survey round 2 proved that the communication is the key factor in presenting such a novel solution. The framework was understood by the respondents with some questions about implementation of the framework into practice, details of the products and terminology. Most of the open issues are out of scope and subjesct to future studies. They do not hinder the presentation of the model. The framework was considered heavy, but comprehensible if given some training about the details of military methods and agilty.

Several benefits were recognized from the model compared to current practices. The most common comment was the structural nature of the framework and activities aligned with incremental products. Military methods were seen useful in creating common taxonomy and structured processes. Agility was commended by transparency, backlogs, scaling and adaptation of water-scrum-fall model. The cyclical nature of the model and emphasis on the provide phase was valued, due to current efforts focus more on the engage phase.

The Delphi-survey round 2 was welcomed by the respondents due to clear and concise presentation which was easier to digest than Delphi 1 with reading package. Possibility to ask questions and comment was a clarifying factor during the Delphi 2.

It is evident based on the Delphi 2 responses that the presented framework is conceivable and adaptable to practice. This adaptation requires training for the red teams because lacking knowledge of the basis of the framework which are the military methods and agility. The frameworks usability is best when several red teams are working in the same company, because this creates the added value from assessment and tool development. This also makes the training of new personnel easier when there is a model to train.

The framework was only slightly modified due to results from the Delphi 2 because the model serves its purpose as is. Agility was emphasized in the principles and some visual alterations were made. Model is a conceivable, comprehensive, agile and scalable process for red teaming using adaptive planning and execution framework. Therefore, we can see that red teaming has been militarized according to headline.

8.6 Finalized CART framework

This chapter presents the final version of the comprehensive agile red teaming framework. The model is constructed with the following ideas:

1. A framework needs to be produced with continuous activities, flexible phases, steps and product backlog to gain comprehensiveness.
2. Agile Water-Scrum-Fall mentality needs to be followed when executing the framework.
3. Consecutive phases and steps receive input from the previous ones. This emphasizes the importance of structured process and planning.
4. Structured problem solving requires defined steps inside phases with activities and products in order to be understandable and repeatable. Steps control the change during process and scope can be altered adaptively.
5. Provide is the most important phase for creating better products, policies and processes. Engage and Planning phases are tools to provide.
6. Management needs to buy-in the red teaming idea. Therefore, the framework needs to be easily communicable and to the right personnel.
7. Red teams need to be educated in use of the framework effectively.

CART framework declares that a company has a baseline capability. **The BASELINE is the prerequisite for all the other phases**. Baseline is constantly developing. Baseline has only one step; The internal development which creates the baseline capability. Internal development consists of adopting the idea of comprehensive agile red teaming framework. This adaptation includes preparation of platforms for communication, intelligence, tooling and a service portfolio which has predefined product backlogs and courses of actions. These reusable components are the building blocks of the framework. Internal development includes the active business domain and threat intelligence efforts. These are needed to build realistic adversary emulation methods and business environment picture. Development and training of the own red teams' and affiliated personnel is continuous.

CART framework has five continuous activities which are driven by the red team leader and conducted by the team;

1. **Planning** is a structured activity to scope, define and solve a given assignment (problem). Planning defines the objective (what), timeline (when), environment (where), resources (who) and rationale (why) for the execution of the assignment. Plan describes how the assignment is conducted, including breakdown of product backlog, tasks and responsibilities.
2. **Intelligence** is a systematic methodology to collect, analyse and disseminate information from several sources and domains. It builds the situational awareness, which is prerequisite for planning, targeting and conducting red team efforts.
3. **Targeting** is a structured process to analyse systems and create means to deliver effects to those systems. Targeting receives inputs from planning and intelligence. System analytics is used in describing target system architecture and break down the system to a component level.
4. **Communication** – Internal communication is an essential element of leading and developing the red team through all phases of the assignment. External communication with client is prerequisite in order to define objectives and raise awareness. It is needed for co-ordination and reviews during engagement and has a significant role for successful follow-on activities during provide phase. Collaboration platforms provide the technical capabilities for communication in all activities.
5. **Assessment** is a continuous activity that supports decision-making by analysing progress towards objectives and changes in the environment. Assessment consists of monitoring, evaluation and feedback to all other activities. Reviews and retrospective are the main tools for assessment.

CART framework has three phases which are divided into steps as depicted in figure 43 below. Detailed framework with product examples is in ANNEX 6.

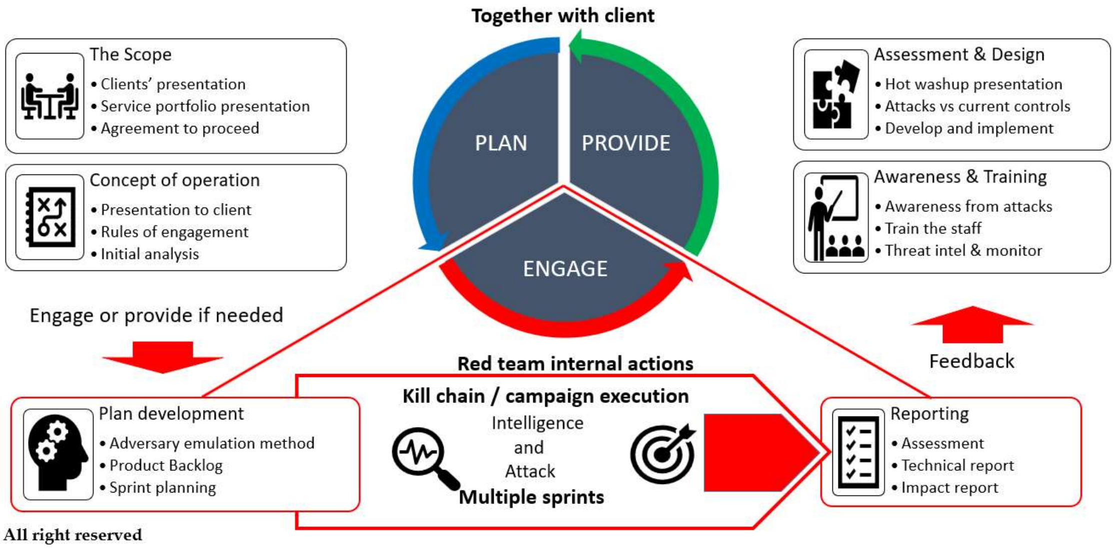


FIGURE 43 Simple CART Framework.

1. **PLAN** – This phase includes intelligence preparation of the environment and analysing the future assignments scope. Concept of operation (CONOPS) is created to manage the future assignment. Planning phase has three steps.
   1.1. SCOPE – During this step an initial scope is defined with client. Scope is based on the maturity and needs of the client.
   1.2. CONOPS – Environment and initial factor analysis are done. These create the basis of choice between courses of actions and plans for the engagement. CONOPS is presented to the client for adjustment and approval.
   1.3. PLAN – Detailed planning and analysis are done along with product backlog and sprint planning. This includes the intelligence collection plan and target system analysis.
2. **ENGAGE** – During this phase the active intelligence gathering, social engineering, network operations and other actions are commenced. Engagement phase does not have fixed step number, but it's dependent on the depth and breadth of the assignment.
   2.1. INTEL 1 – Collection focused step which builds the understanding of the comprehensive target architecture. This might include initial entries.
   2.2. INTEL X – Several intel steps can be taken depending on the complexity and size of the target. Following steps should be more focused on analysis and post initial compromise activities like lateral movement and persistence.
   2.3. ATTACK – This step aims to launch the attacks to provide the effects needed for the target (DDoS, Locker, Wiper, Manipulation, Physical, etc). If production environment is not in use a simulation needs to be conducted which aids in the presentation.
   2.4. CLOSE – Removal of modifications and malware from the clients' systems and remediation of social engineering effects. Sufficient time slot reserved for team reporting and preparation of the next phase.
3. **PROVIDE** – This is the phase where results of the engagement are reported to the client along with a remediation plan which includes the consecutive steps. Goal is to reassess, design and implement better security. Training and raising awareness of clients' employees supports the implementation. This phase has five steps.
   3.1. PRESENT – During this step the results are presented to the client in meetings, workshops and reports. A remediation plan is also introduced.
   3.2. ASSESS – First step in remediation is the comprehensive assessment of current policies, risk management and controls to provide overview of the security situation and corrections.
   3.3. DESIGN – Step is taken to improve the previous assessments artifacts with corrective measures. User participation from client-side non-security branches is encouraged to increase commitment to security.
   3.4. TRAIN – Various training initiatives are carried out in all levels of the company. Training supports the implementation of newly designed security items, raises awareness and teaches the employees to mitigate crisis situations in simulations and tabletop games.

3.5. IMPLEMENT – Support the client in technical and policy implementation issues along with monitoring and threat intel.

The framework consists of products that are created during the steps i.e. Intelligence collection plan, concept of operation, target system analysis, etc. Products are only examples in the framework. Product backlog is created and tied to the steps. Some products are refined constantly during multiple steps and considered as living documents/products. Detailed products and descriptions call for future research. Example of products is depicted in Annex 6.

The scope of this study is wide and therefore results can be considered only general (Siponen & Klaavuniemi, 2019). The significance of this framework lies in its novelty and possibilities to adapt it to any red teams' purposes due to general outcome. There are existing standards for penetration testing (PTES, 2014) and attack generation (Mitre, 2018) as well as kill chain completion (Hutchins et al., 2011) but none of them give a picture of the actual process how the entire operation could be planned and executed.

Usability of the military and agile methods is proven in the business world and in the battlefield. Framework delivers a good base for future work like building the taxonomy and product catalogue for red teaming effort. Platforms to communicate and manage red teaming operations need to be developed as well.

The supporting literature base for the framework comes from the information security research and standards. (ISO, 2018; NIST, 2013; The Institute of Risk Management, 2002) Information security lifecycle and risk management principles support the frameworks cyclical nature, phases and steps (Raggad, 2010; Baskerville, 1991; Baskerville, 1993; Tsohou et al., 2006). Knapp et al. (2009) provided an information security policy process model to extend to the field of red teaming for this study.

Military adaptive planning and execution framework, mission command, intelligence cycle and targeting are results of combat proven best practices coined with scientific studies. These methods deliver the structured problem-solving techniques and basis for various deliverables to the framework. (US Joint Chiefs of Staff, 2017; US Joint Chiefs of Staff, 2013; US Joint Chiefs of Staff, 2013b; Department of the Army, 2012)

Agile methodologies have been removing bureaucracy and hierarchy from teamwork by creating productivity, quality, speed and better morale for the personnel for decades. (Hilbert, 2017; Beck et al., 2001; Sutherland & Schwaber, 2011; Sugimori et al., 1977) Agile scaling methods create possibilities to optimize the value chains for the whole enterprise, not just the single agile team. (Laanti, 2012; Leffingwell, 2007)

9 CONCLUSIONS

"The road to wisdom? Well, it's plain and simple to express:

Err

and err

and err again

but less

and less

and less."

- Piet Hein-

Mistakes were made during this research process, but we learned from them. Selfcriticism is the opposite of overconfidence, which is the road to complecency. Red teaming if properly adapted can be a structural way of avoiding complacency in organizations by a constructive method for exposing organization and its functions to critique and improvement.

The research problem was to create a comprehensive, agile red teaming framework by combining adaptive planning and execution framework in information security context. Design science research methodology was used to solve this problem (Peffers et al., 2007). Solid knowledge base and environment description about red teaming and information security was completed in accordance with information systems research framework. (Hevner et al., 2004) Adaptive planning and execution framework, intelligence, targeting and agile methodologies were introduced to support the creation of the framework in information security management context. Challenges in current red teaming operations were identified by a survey to five cyber security companies. Challenges were remediated by success factors identified from literature and survey. The initial framework was created, and it underwent two Delphi iterations with subject matter experts and was refined according to responses. This study presented interesting connections between military and agile practices and how they can be adapted together in red teaming.

9.1 Implications for research and practice

This study has added a piece to the complicated nature of information security research puzzle and shown how red teaming fits to the research domain. The interlinkage of red teaming and support to risk management is displayed clearly through adversary emulation approach. The scope of red teaming can also vary in tiers. This means different planning horizons and goals for organizations. Red teaming research can be adapted to lifecycle models and standards used in information security that are in common use.

Red teaming research scope should be broadened in the information security research. Red teaming research has focused in adversary emulation and penetration testing practices disregarding the remediations which are the key in building better security. The planning and providing of security should be an integral part of red teaming. Risk management includes the future risks that cannot be derived from the past which requires an external attacker to simulate future risks. APT research supports red teaming activities in creating threat matrixes for attack simulation that can also simulate future risks.

The adaptation of military planning, execution, intelligence and targeting to new domains requires understanding of the principles behind the military methodology. They are not just best practices but derive from problem-solving theories, behavioural sciences and multidisciplined domains like system science. These need to be recognized before trying to adapt military thinking into new domains.

The practical implications include introduction of the adaptive planning and executions framework as a problem-solving and managing technique for red team operations. Military processes are historically combat proven, and due to formalized structure, they can be practical tools to reduce biases and inconsistency in decision-making. Mental models are created during planning process. Decision-making happens in a loop, which calls for constant destruction and creation of mental patterns. (Boyd, 1976b)

Mission command is a way to execute operations and it takes several notions from OODA-loop. Purpose of mission command is to create disciplined initiative within teams by empowering agility and adaptivity. It emphasizes leader's centralized intent, which is combined to decentralized execution of tasks by teams. (Department of the Army, 2012) Intelligence and targeting are activities that support the overall mission. Mission accomplishment is built by planning and executing tasks which are supported by intelligence. Processes need to be separated due to their different functionality but communicated effectively between practitioners in order to be interlinked and aligned towards a common goal through mission command. Continuous assessment of all activities is the orientation that OODA-loop emphasizes.

Agile methods have several similarities with adaptive planning and execution framework. Both deal with complex adaptive system environments and need the constant OODA-loop running. The agile scalability is based on different planning horizons which has resemblance to military strategic, operational and tactical planning which are parallel processes supporting each other with feedback mechanisms. Crossfunctionality is comparable to JOINT, where different professionals combine their efforts in one team.

Agile enterprise transformations are harder to embrace than agile team practices. Therefore, a model addressed as Water-Scrum-Fall was also introduced. (West, 2011) Water-Scrum-Fall model tries to balance between the corporate reality, which is bound by funding, plans, compliance and other factors versus optimal theoretical agile methodology.

Agile practices emphasize incremental product delivery where iterative feedback is quick from the iterations (Sutherland & Schwaber, 2011). Key enablers include prioritized backlogs, continuous integration, increments, iterations, retrospectives and empowered teams (Laanti, 2012). Backlogs resemble planning, intelligence and targeting products which are produced in different steps of the process that can be interpreted as sprints or iterations.

Mission command emphasises the subordinate's responsibility of solving problems independently within limits and leader is more driving the process and fostering the team like a scrum master. Naturally there are difference between the world of military and agile, but the idea is to take the best of both worlds into the framework creation in this study. Both military and civilian worlds try to increase quality, productivity and morale by cutting down to bureaucracy and hierarchical management structures.

The scope of this study was wide and therefore results can be considered general. The significance of the created framework lies in its novelty and possibilities to adapt it to any red teams' purposes due to general outcome. Several different methods were studied and merged together to form a comprehensive structured but agile framework with deliverables as examples on how the framework could be adapted. Usability of the military and agile methods is proven in the business world and in the battlefield. Framework delivers a good base for future work.

Implications for practice remain to be seen. This calls for some brave red teamers to adapt the framework for their work and deliver results. At least now there is a framework for use to everyone in the red teaming community to make it better.

9.2 Discussion

Design science in the context of information systems framework was suitable for this study, because it aims to create a solution for a problem and new knowledge is created during the process. Methodological triangulation was used in creating novelty and validity for the study.

The literature study covering chapters 2-6 was extensive, and references in total surpass 200 pieces. Challenge was to cover four different areas; red teaming, information security management, military methods and agile practices simply, but at the same time concisely. This effort was both intentional and mandatory in order to create knowledge base and describe research environment. Literature study was a team effort which included data and investigator triangulation. Assessment, peer reviews and writing support was a constant cyclical process between researchers.

Scope of the study was wide. Therefore, all possible references could not be utilized, but the chosen ones should cover the topics sufficiently Military references were mainly US doctrines as they are publicly available. Military and agile chapters had to be generalized to keep final report in scope, due to this some case specific exceptions were left in omission. One example of this is implementation of the CART model into practice. Created model might be suitable for red teaming also in the domain of physical security or other domains. However, this cannot be proven as the environment section covered information security only.

The survey consisted only five different companies. All the companies that participated were from Finland. Research in multinational environment might provide different results, especially as the knowledge accumulates from practical experiences of red teaming operations.

Delphi-method is a consensus driven technique which promotes group communication between subject matter experts. It is not a statistical study, but more like a confined group decision mechanism. It is possible that consensus was reached too easily in the final Delphi round. This is due to a fact that novel knowledge presented in the form of military methods mixed with agility might have be seemed better than it is. Therefore, model should be considered as a preliminary starting point for further studies to be conducted. Constructed framework is intentionally heavy and comprehensive to allow a basis for a change.

9.3 Future work

The results of this study create several possibilities for future studies. The most intersting future vision would be to adapt the CART framework to a process for a real red teaming organization and study the implications. This would require a creation of a training program to implement the framework.

The implementation of the framework in theory and practice would require further studies of creating suitable products and backlogs for respective phases of the framework. Mission command was introduced but the real-life management of red teaming also needs further work. Management needs a collaboration system. There are several technical networked collaboration platforms available but further studies are needed to find out the most suitable in managing red teaming plans, workflow, intelligence, targeting and reporting.

Personnel in red teaming genre mostly consist of penetration testers and hackers. If the scope of red teaming is widened to cover the entire plan-engage-provide framework, this presents a challenge for the personnel usage. Different competences are needed in a red teaming organization starting from scrum master-style managers, penetration testers, security developers and instructors.

Need for common taxonomy and lexicon for red teaming activities would benefit the entire information security community. This would enable professionals to communicate with consistent terminology. Terminology is closely tied to the deliverable products.

If red teaming scope would be broadened it would require an organizational change in most organizations. Currently in most organizations there are stovepipes between sales, red teaming, compliance management and security consulting. These artificial walls would have to be made transparent and tied to a comprehensive security posture creation where red teaming could be the philosophical background. This requires further studies.

The realization of similarities of agile methods and practices with military planning and execution was an interesting notion and should be studied more. The reduction of hierarchical and bureaucratic restraints would benefit military leadership as well and agile practices give tools for this transformation.

REFERENCES

9-11 Commission. (2004). *The 911 Commission report.* The National Commission on Terrorist Attacks Upon the United States. Washington: The National Commission on Terrorist Attacks Upon the United States. Retrieved March 4, 2019, from https://www.9-11commission.gov/report/

Abrahamsson, P., Warsta, J., Siponen, M., & Ronkainen, J. (2003). New Directions on Agile Methods: A Comparative Analysis. *25th International Conference on Software Engineering* (pp. 244-254). Portland: IEEE. doi:10.1109/ICSE.2003.1201204

Ackoff, R. L. (1999). *Ackoff's best: His classic writings on management.* New York: John Wiley & Sons.

Adorno, T. W. (1973). *Negative dialectics.* London: Routledge.

Algarni, A., & Malaiya, Y. (2014). Software vulnerability markets: Discoverers and buyers. International Journal of Computer. *International Journal of Computer, Information Science and Engineering, 8*(3), 71-81. Retrieved March 29, 2019, from https://pdfs.semanticscholar.org/2d8a/9d88cf83993c1774ddc66f30b086b6f300ab.pdf

Algra, K., Barnes, J., Mansfeld, J., & Schofield, M. (1999). *The Cambridge history of Hellenistic philosophy.* Cambridge: Canbridge University press.

Antunes, N., & Vieira, M. (2009). Comparing the effectiveness of penetration testing and static code analysis on the detection of sql injection vulnerabilities in web services. *2009 15th IEEE Pacific Rim International Symposium on Dependable Computing* (pp. 301-306). Shanghai: IEEE. Retrieved April 11, 2019, from https://ieeexplore.ieee.org/abstract/document/5369093

Asch, S. E. (1956). Studies of Independence and Conformity: I . A Minority of One Against a Unanimous Majority. *Psychological Monographs: General and Applied, 70*(9), 1-70. doi:10.1037/h0093718

Averch, H., & Lavin, M. M. (1964). *Simulation of Decisionmaking in Crises: Three Manual Gaming Experiments (No. RM-4202-PR).* Santa Monica: RAND corporation. Retrieved March 15, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/605476.pdf

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems, 1*(2), 121-130. doi:https://doi.org/10.1057/ejis.1991.20

Baskerville, R. (1993, December). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys (CSUR), 25*(4), 375-414. doi:10.1145/162124.162127

Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2010). State of the art: Automated black-box web application vulnerability testing. *2010 IEEE Symposium on Security and Privacy* (pp. 332-345). Berkeley: IEEE. doi: 10.1109/SP.2010.27

Beck, K., & all, e. (2001, November 13). *Agile manifesto.* Retrieved January 20, 2018, from Agile manifesto web site: http://agilemanifesto.org

Bertoglio, D. D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society, 23*(2), 1-16. doi:https://doi.org/10.1186/s13173-017-0051-1

Binde, B. E., McRee, R., & O'Connor, T. J. (2011). *Assessing Outbound Traffic to Uncover Advanced Persistent Threat.* Betsheda: SANS Technology Institute. Retrieved March 4, 2019, from https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf

Bishop, M. (2007). About penetration testing. *IEEE Security & Privacy, 5*(6), 84-87. Retrieved April 11, 2019, from https://ieeexplore.ieee.org/abstract/document/4402456

Boell, S. K., & Cecez-Kecmanovic, D. (2015). What is an Information System? *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2015)* (pp. 1530-1605). Kauai: IEEE. doi: 10.1109/HICSS.2015.587

Böhme, R. (2005). Vulnerability Markets. What is the economic value of a zero-day exploit? *Paper held at the 2005 Chaos Communication Congress* (pp. 1-5). Berlin: CCC. Retrieved March 6, 2019, from https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf

Boyd, J. (1976, August 4). *New conception for air-to-air combat.* Retrieved April 29, 2019, from The John Boyd Library: https://danford.net/boyd/fast_transients.pdf

Boyd, J. (1976b, September 3). *Destruction and creation.* Retrieved April 29, 2019, from The John Boyd Library: https://danford.net/boyd/destruct.htm

Boyd, J. (1992, August 1). *Conceptual spiral.* Retrieved April 29, 2019, from The John Boyd Library: https://danford.net/boyd/conceptual.pdf

Boyd, J. (1996, January 1). "*The essence of winning and losing.*" *Unpublished lecture notes 12.23 (1996): 123-125.* (c. Richards, & C. Spinney, Eds.) Retrieved April 29, 2019, from Defence and the national interest: https://fasttransients.files.wordpress.com/2010/03/essence_of_winning_losing.pdf

Brangetto, P., Çalişkan, E., & Rõigas, H. (2015). *Cyber Red Teaming.* Tallinn: CCDCOE. Retrieved December 10, 2018, from https://ccdcoe.org/multimedia/cyber-red-teaming-organisational-technical-and-legal-implications-military-context.html

Breindenbach, L., Daian, P., Tramèr, F., & Juels, A. (2018). Enter the hydra: Towards principled bug bounties and exploit-resistant smart contracts. *27th {USENIX} Security Symposium ({USENIX} Security 18* (pp. 1335-1352). Baltimore: Usenix. Retrieved March 29, 2019, from https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-breidenbach.pdf

Bush, G. H. (1976). *Memorandum From the Director of Central Intelligence (Bush) to Recipients of National Intelligence Estimate 11–3/8–76.* CIA. Washington: Office of the historian US. Retrieved March 3, 2019, from https://history.state.gov/historicaldocuments/frus1969-76v35/d170

Calvi, A., & Viganò, L. (2016). An automated approach for testing the security of web applications against chained attacks. *Proceedings of the 31st Annual ACM Symposium on Applied Computing (pp. 2095-2102). ACM.* (pp. 2095-2102). Pisa: ACM. doi:10.1145/2851613.2851803

Cambridge University Press. (2019, March 5). *Cambridge dictionary*. Retrieved from Cambridge dictionary: https://dictionary.cambridge.org/dictionary/english/cyber

Caron, F. (2019). Obtaining reasonable assurance on cyber resilience. *Managerial Auditing Journal*. Retrieved February 8, 2019, from https://doi/10.1108/MAJ-11-2017-1690

Cavusoglu, H., Raghunathan, S., & Wei, T. Y. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems, 25*(2), 281-304. doi:https://doi.org/10.2753/MIS0742-1222250211

Chen, P., Desmet, L., & Huygens, C. (2014). A Study on Advanced Persistent Threats. In B. D.´uquete (Ed.), *IFIP International Federation for Information Processing CMS 2014* (p. 63/72). Springer. Retrieved March 5, 2019, from https://link.springer.com/content/pdf/10.1007/978-3-662-44885-4_5.pdf

CIA. (1982). *A statistical overview of terrorist skyjackings from January 1968 through June 1982*. CIA. Washington D.C.: CIA. Retrieved March 3, 2019, from https://www.scribd.com/doc/53824134/Terrorist-Skyjackings-A-CIA-Report#download

CIA. (2016, January 16). *History of CIA*. Retrieved March 5, 2019, from CIA homepages: https://www.cia.gov/offices-of-cia/intelligence-analysis/history.html

Ciancarini, P., & Gasparro, A. (2012). Priority Level Planning in Kriegspiel. *11th International Conference ICEC 2012* (pp. 33–340). Bremen: IFIP International Federation for Information Processing .

Cohn, M. (2010). *Succeeding with agile: software development using Scrum.* Ann Arbor, Michigan: Pearson Education.

Curphey, M., & Arawo, R. (2006). Web application security assessment tools. *IEEE Security & Privacy, 4*(4), IEEE Security & Privacy, 4(4), 32-41. Retrieved April 11, 2019, from https://ieeexplore.ieee.org/abstract/document/1668000

Dalkey, N. (1967). *DELPHI.* Santa Monica: The RAND Corporation. retrieved from (https://www.rand.org/pubs/papers/P3704.html) 29.11.2018.

Daly, M. K. (2009, November 1). *The Advanced Persistent Threat.* Retrieved from Usenix Website: https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf

Davis, P. K. (1984). *RAND's experience in applying artificial intelligence techniques to strategic-level military-political war gaming (No. RAND/P-6977).* Santa Monica: RAND Corporation. Retrieved March 15, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a147272.pdf

Davis, R. H. (1962). *Arms control: the search for an acceptable research methodology.* Armed Services Technical Information Agency. Arlington: Armed Services Technical Information Agency. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/297454.pdf

Davis, R. H. (1963). Arms Control Simulation: The Search for an Acceptable Method. *Journal of Conflict Resolution, 7*(3), 590–603. doi:https://doi.org/10.1177/002200276300700341

Defense Science Board. (2003). *Defense Science Board Task Force on The Role and Statusof DoD Red Teaming Activities.* Washington, D.C.: Defense Science Board (DSB). Retrieved March 3, 2019, from https://fas.org/irp/agency/dod/dsb/redteam.pdf

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success: The Quest for the Dependent Variable. *Information Systems Research 3:1*, 60-95. Retrieved April 15, 2019, from https://pdfs.semanticscholar.org/a041/45f1ca06c61f5985ab22a2346b788f343392.pdf

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems, 19*(4), 9-30. Retrieved February 25, 2019, from https://www.iuj.ac.jp/faculty/kucc625/itis/reading/DeLone_McLean_2003_DeLone.pdf

Denzin, N. K. (1978). Denzin, N. K. (1978). Triangulation: A case for methodological evaluation and combination. *Sociological methods*, 339-357.

Department of defence, Australia. (2017). *A Simple Handbook for Non-Traditional Red Teaming.* Edinburgh: Defence Science and Technology Group National Security and ISR Division. Retrieved March 4, 2019, from https://www.dst.defence.gov.au/publication/simple-handbook-non-traditional-red-teaming

Department of the Army. (1951). *FM 30-5 Combat Intelligence.* Washington: United States Government printing office. Retrieved May 27, 2019, from https://www.scribd.com/document/341576118/Combat-Intelligence-Fm-30-5-1951

Department of the army. (2010, March 23). *FM 2-0 Intelligence.* Washington: Department of the army. Retrieved March 3, 2019, from US army website: https://fas.org/irp/doddir/army/fm2-0.pdf

Department of the army. (2010b, March). *FM 5-0 The operations process.* Washington: Department of the army. Retrieved March 13, 2019, from US Army web site: https://fas.org/irp/doddir/army/fm5-0.pdf

Department of the Army. (2012). *ADRP6-0 Mission command.* Washington: Department of the Army. Retrieved March 3, 2019, from https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/adp6_0.pdf

Department of the army. (2015). *FM3-60 Targeting.* Washington: Department of the army. Retrieved February 2, 2019, from https://fas.org/irp/doddir/army/atp3-60.pdf

Development Concepts and Doctrine Centre. (2013, January). *Red Teaming Guide.* Retrieved December 18, 2018, from Second Edition: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf

Development, Concepts and Doctrine Centre. (2019, 2 14). *Development, Concepts and Doctrine Centre.* Retrieved March 5, 2019, from Development, Concepts and Doctrine Centre: https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre

DHS. (2004, May 1). *Homeland security exercise and evaluation program.* (T. Ridge, Ed.) Retrieved April 8, 2019, from Homeland security digital library: https://www.hsdl.org/c/

Diamant, J. (2011). Resilient security architecture: A complementary approach to reducing vulnerabilities. *IEEE Security & Privacy, 9*(4), 80-84. Retrieved April 11, 2019, from https://ieeexplore.ieee.org/abstract/document/5968094

Dilhac, J.-M. (2001). *The telegraph of Claude Chappe -an optical telecommunication network for the xviiith century.* Institut National des Sciences Appliquées de Toulouse. Toulouse: Institut National des Sciences Appliquées de Toulouse. Retrieved 2 26, 2019, from https://pdfs.semanticscholar.org/cd81/f199759c240608d433b47131f9ea22a7804b.pdf

Dimkov, T., Van Cleeff, A., Pieters, W., & Hartel, P. (2010). Two methodologies for physical penetration testing using social engineering. *ACSAC '10 26th annual computer security applications conference* (pp. 399-408). Austin: ACM. Retrieved April 11, 2019, from https://dl.acm.org/citation.cfm?id=1920319

Director of the national intelligence. (2018). *Worldwide threat assessmentof the us intelligence community.* Washington D.C.: Office of the director of the national intelligence. Retrieved March 4, 2019, from https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Dragos Inc. (2017). *CRASHOVERRIDE Analysis of the Threatto Electric Grid Operations.* Hanover: Dragos Inc. Retrieved March 4, 2019, from https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

Duggan, D. P., Thomas, S. R., Veitch, C. K., & Woodard, L. (2007). *Categorizing threat: Building and using a generic threat matrix.* Albuquerque: Sandia National Laboratories. Retrieved April 11, 2019, from https://www.smartgrid.gov/document/categorizing_threat_building_and_using_generic_threat_matrix

Duran, F., Conrad, S. H., Conrad, G. N., Duggan, D. P., & Held, E. B. (2009). Building A System For Insider Security. *Security. IEEE Security & Privacy, 7*(6), 30-38. doi:10.1109/MSP.2009.111.

E-ISAC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Bethesda: SANS Industrial Control Systems. Retrieved March 5, 2019, from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Erridge, T. (2018). True colours of red teaming. *Network security, 2018*(4), 20. Retrieved April 10, 2019, from https://www.sciencedirect.com/journal/network-security/vol/2018/issue/4

EUROPOL. (2018). *Internet Organised Crime Threat Assessment (IOCTA) 2018.* European cybrcrime centre. The Hague: European Union Agency for Law Enforcement Cooperation. Retrieved March 4, 2019, from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Financial Times. (2019, 2 14). *Financial times lexicon.* Retrieved March 2, 2019, from Financial times website: http://lexicon.ft.com/term?term=red-team

Finifter, M., Akhawe, D., & Wagner, D. (2013). An Empirical Study of Vulnerability Rewards Programs. *Proceedings of the 22nd USENIX Security Symposium.* (pp. 1-17). Washington, D.C., USAISB N: Usenix. Retrieved March 6, 2019, from https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf

FireEye Inc. (2014). *APT28: A Window Into Russia'S Cyber Espionage Operations?* Milpitas: FireEye, Inc. Retrieved March 4, 2019, from https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

Fleming, J. M. (2010). *Playing the Bad Guy: How Do Organizations Develop, Apply, and Measure Red Teams?* faculty of the Virginia Polytechnic Institute and State University. Alexandria: Virginia tech. Retrieved 2 26, 2019, from https://vtechworks.lib.vt.edu/handle/10919/77095

Flick, U. (2006). *An introduction to qualitative research.* London: SAGE Publications Ltd.

Frini, A., & Boury-Brisset, A.-C. (2011). An intelligence process model based on a collaborative approach. *16th International Command and Control Research and Technology Symposium* (pp. 1-47). Quebec: Defence Research And Development Canada Valcartier (Quebec). Retrieved April 17, 2019, from https://apps.dtic.mil/docs/citations/ADA547105

F-Secure. (2015). *The Dukes 7 years of Russian cyberespionage.* F-Secure Labs. Helsinki: F-Secure. Retrieved March 4, 2019, from https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

F-Secure. (2018). *Attack landscape H12018.* Helsinki: F-Secure. Retrieved March 4, 2019, from F-Secure blog: https://blog.f-secure.com/attack-landscape-2018-far/

GAO. (2000). *Aviation Security Long-Standing Problems Impair Airport Screeners' Performance.* United States General Accounting Office (GAO). Washington D.C.: United States General Accounting Office (GAO). Retrieved March 4, 2019, from https://www.gao.gov/assets/160/156968.pdf

Geer, D. (2010). Are companies actually using secure development life cycles? *Computer, 43*(6), 12-16. Retrieved March 6, 2019, from https://ieeexplore.ieee.org/abstract/document/5481927

George Washington University. (2018, August 1). *Eligible Receiver 97: Seminal DOD Cyber Exercise Included Mock Terror Strikes and Hostage Simulations.* Retrieved december 1, 2018, from National security archive: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations

Ghafir, I., & Prenosil, V. (2014). Advanced Persistent Threat Attack Detection: An Overview. *International Journal of Advancements in Computer Networks and Its Security– IJCNS, 4*(4), 50-54. Retrieved March 5, 2019, from https://www.researchgate.net/publication/305956804_Advanced_Persistent_Threat_Attack_Detection_An_Overview

Gill, P., & Phythian, M. (2016). What is intelligence studies? *The International Journal of Intelligence, Security, and Public Affairs, 18*(1), 5-19. Retrieved April 16, 2019, from https://www.tandfonline.com/doi/abs/10.1080/23800992.2016.1150679

Glumich, S., Riley, J., Ratazzi, P., & Ozanam, A. (2018). BP: Integrating Cyber Vulnerability Assessments Earlier into the Systems Development Lifecycle: A Methodology to Conduct Early-Cycle Cyber Vulnerability Assessments. *2018 IEEE Cybersecurity Development (SecDev)* (pp. 77-84). Cambridge: IEEE. Retrieved March 6, 2019, from https://ieeexplore.ieee.org/abstract/document/8543390

Goldhamer, H., & Speier, H. (1959). Some Observations on Political Gaming. *World Politics, 12*(1), 71-83. Retrieved March 2, 2019, from https://www.jstor.org/stable/pdf/2009213.pdf?refreqid=excelsior%3A3bc2682a47c815e385e41dc05d386b71

Gotztepe, K., & Kahraman, C. (2015). A New Approach to Military Decision Making Process: Suggestions from MCDM Point of View. *International Conference on Military and Security Studies 2015* (pp. 118-12). Istanbul: Turkish War College. Retrieved April 16, 2019, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.741.5622&rep=rep1&type=pdf

Govindarajan, V., & Trimble, C. (2010). *The other side of innovation: Solving the execution challenge.* . Boston: Harvard Business Press.

Granåsen, M., & Andersson, D. (2016). Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. *Cognition, Technology & Work,, 18*(1), 121-143. Retrieved April 10, 2019, from https://link.springer.com/article/10.1007/s10111-015-0350-2

Gray, J. A. (2015). *The Evolution of the Promoter of the Faith in Causes of Beatification and Canonization: a Study of the Law of 1917 and 1983.* Diritto Canonico. Rome: Pontificia universitas lateranense.

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly, 37*(2), 337-355. Retrieved January 3, 2018, from https://www.jstor.org/stable/43825912

Guetzkow, H. (1959). A use of simulation in the study of inter-nation relations. *Behavioral Science, 4*(3), 183-191. doi:10.1002/bs.3830040302

Haines, O. L. (1926). *A proposed revision of TR 210-5, Combat intelligence regulations.* Fort Leavenworth: The command and general staff school.

Hansen, A. P. (2008). *Cyber Flag A Realistic Cyberspace Training Construct.* Air Force Institute of Technology, Department of Electrical and Computer Engineering . Ohio: Air University. Retrieved 2 26, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a479931.pdf

Helmer, O. (1967). *Analysis of the future: The Delphi method.* Santa Monica: The RAND Corporation. Retrieved February 2, 2018, from https://www.rand.org/pubs/papers/P3558.html

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterky, 28*(1), 75-105. doi:10.2307/25148625

Hilbert, M. (2017, October 20). *Redgate Blog*. Retrieved May 29, 2019, from The real origins of the Agile Manifesto: https://www.red-gate.com/blog/database-devops/real-origins-agile-manifesto

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2004). *Tutki ja kirjoita.* Jyväskylä: Gummerus Kirjapaino Oy.

Hu, P., Li, H., Fu, H., Cansever, D., & Mohapatra, P. (2015). Dynamic defense strategy against advanced persistent threat with insiders. In IEEE (Ed.), *2015 IEEE Conference on Computer Communications (INFOCOM) Hu, Pengfei v:2015 s:747 -755* (pp. 747-755). Hong Kong: IEEE. Retrieved March 5, 2019, from https://ieeexplore.ieee.org/document/7218444

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In J. Ryan (Ed.), *Leading Issues in Information Warfare & Security Research* (pp. 80-106). Reading, UK: Academic Publishing International Limited. Retrieved March 5, 2019, from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

INB. (2013, November 1). *ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements.* Retrieved February 11, 2019, from https://trofisecurity.com/assets/img/iso27001-2013.pdf

ISACA Germany Chapter e.V. (2013, January 1). *Implementation Guideline ISO/IEC 27001:2013.* Retrieved February 11, 2019, from ISACA Germany chapter: https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf

ISO. (2018, February 1). *ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary.*

Retrieved February 26, 2019, from https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS quarterly, 39*(1), 113-134. Retrieved April 18, 2019, from http://disknet.org/DISKNET/media/pdfs/2019/03/21/document5_Kopie_3.pdf

Johnston, R. (2005). *Analytic culture in the US intelligence community: An ethnographic study.* Washington D.C.: Central Intelligence Agency, center for study of intelligence. Retrieved April 17, 2019, from https://apps.dtic.mil/docs/citations/ADA507369

Just, S., Premraj, R., & Zimmermann, T. (2008). Towards the next generation of bug tracking systems. *2008 IEEE Symposium on Visual Languages and Human-Centric Computing* (pp. 82-85). Herrsching am Ammersee: IEEE. doi:10.1109/VLHCC.2008.4639063

Kahneman, D., Rosenfield, A. M., Gandhi, L., & Blaser, T. (2016). Noise: How to overcome the high, hidden cost of inconsistent decision making. *Harvard Business Review, 94*(10), 38-46. Retrieved March 15, 2019, from http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=2&sid=c201711b-b335-4036-9fef-65ba7aab1efa%40sdc-v-sessmgr03

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyberwar.* . New York: Simon & Schuster.

Kesan, J. P., & Hayes, C. M. (2016). Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities. *Arizona Law Revew, 58*, 753-829. Retrieved March 29, 2019, from http://arizonalawreview.org/pdf/58-3/58arizlrev753.pdf

Knapp, K., Morris, F., Marshall, T., & Byrd, T. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493-508. Retrieved January 13, 2019, from https://www.researchgate.net/publication/304494363_Information_security_policy_development_and_implementation_The_what_how_and_who/download

Kniberg, H., & Skarin, M. (2010). *Kanban and Scrum making the most of both.* United States of America: C4Media. Retrieved June 6, 2019, from http://www.agileinnovation.eu/wordpress/wp-content/uploads/2010/09/KanbanAndScrum_MakingTheMostOfBoth.pdf

Knuth, D. E. (1989). The Errors of TEX. *Software-Practice And Experience, 19*(7), 607-68. Retrieved March 6, 2019, from https://yurichev.com/mirrors/knuth1989.pdf

Kraemer, S., Carayon, P., & Duggan, R. (2004). Red team performance for improved computer security. *Human Factors and Ergonomics Society Annual Meeting. 48*, pp. 1605-1609. Los Angeles: Sage publications. Retrieved

April 10, 2019, from https://journals.sagepub.com/doi/abs/10.1177/154193120404801410

Krombholz, K. H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications, 22,* 113-122. doi:https://doi.org/10.1016/j.jisa.2014.09.005

Laanti, M. (2012). *Agile Methods In Large-Scale Software Development Organizations -Applicability and model for adoption.* Oulu: University of Oulu. Retrieved December 10, 2018, from http://jultika.oulu.fi/files/isbn9789526200347.pdf

Laanti, M. (2014). Characteristics and Principles of Scaled Agile. *International Conference on Agile Software Development.* (pp. 9-20). Cham: Springer. doi:10.1007/978-3-319-14358-3_2

Lane, G. (2008). The use of red teaming in the corporate environment: A study of security management, vulnerabilities and defence. *Proceedings of the 1st Security & Intelligence Conference* (pp. 77-83). Perth: SECAU - Security Research Centre. Retrieved March 6, 2019, from https://www.researchgate.net/profile/David_Brooks11/publication/49284817_The_Use_of_Red_Teaming_in_The_Corporate_Environment_A_Study_of_Security_Management_Vulnerabilities_and_Defence/links/00b7d524b8c6e3d0b2000000.pdf#page=77

Laribee, L. (2006). *Development of methodical social engineering taxonomy project.* Monterey: Naval postgraduate school. Retrieved April 11, 2019, from https://apps.dtic.mil/docs/citations/ADA457544

Leffingwell, D. (2007). Scaling software agility: best practices for large enterprises. Boston: Pearson education.

Lipka, M., & Townsend, T. (2014, 4 14). *Papal saints: Once a given, now extremely rare.* Retrieved 2 15, 2019, from PEW research center wesite: http://www.pewresearch.org/fact-tank/2014/04/24/papal-saints-once-a-given-now-extremely-rare/

Lipner, S. (2014). The trustworthy computing security development lifecycle. *20th Annual Computer Security Applications Conference* (pp. 2 -13). Tucson: IEEE. Retrieved March 6, 2019, from https://ieeexplore.ieee.org/document/1377211

Lowenthal, M. M. (2016). *Intelligence: From secrets to policy.* Washington: CQ press.

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity, 3*(2), 81-90. Retrieved March 6, 2019, from https://academic.oup.com/cybersecurity/article/3/2/81/4524054

Malone, T. G., & Schaupp, R. E. (2002). The" Red Team": forging a well-conceived contingency plan. *Air & Space Power Journal, 16(2), 22., 16*(2), 22-23. Retrieved April 8, 2019, from http://fetch.mhsl.uab.edu/login?url=http://search.proquest.com/docview/217781295?accountid=8240

Mandiant. (2013). *APT1 Exposing One of China's Cyber units.* Part of FireEye Inc . Alexandria: Mandiant. Retrieved March 4, 2019, from https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

March, S., & Smith, G. (1995). *Design and natural science research on information technology.* Elsevier: Decision Support Systems. Vol 15. pp. 251-266. retrieved from (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.826.5567&rep=rep1&type=pdf) 21.11.2018.

Marr, J. J. (2001). *The Military Decision Making Process: Making better decisions versus making decisions better.* Monograph, Army command and general staff coll, School of advanced military studies, Fort Leavenworth KS. Retrieved April 16, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a387136.pdf

McCloskey, M. J., & Stanard, T. (1999). A Red Team Analysis of the Electronic Battlefield: A Cognitive Approach to Understanding How Hackers Work in Groups. *In Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 179-183). Los Angeles: Sage Publications. Retrieved March 6, 2019, from https://journals.sagepub.com/doi/abs/10.1177/154193129904300311

Meeham, M. K. (2007). Red Teaming for Law Enforcement. *Police Chief Volume, 74*(2), 22,25,28. Retrieved March 6, 2019, from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=239129

Mehta, A. (2018, July 18). *The Pentagon is gearing up to red team industry cybersecurity*. Retrieved March 4, 2019, from https://www.fifthdomain.com/industry/2018/07/16/the-pentagon-is-gearing-up-to-red-team-industry-cybersecurity/

Merriam Webster. (2019, March 4). *Merriam Webster dictionary*. Retrieved March 4, 2019, from Merriam Webster website: https://www.merriam-webster.com/dictionary/cyber

Ministry of Defence. (2018). *Defence White Paper - Investing in our people, capabilities and visibility.* Amsterdam: Ministry of Defence, Netherlands. Retrieved January 15, 2019, from https://english.defensie.nl/downloads/policy-notes/2018/03/26/defence-white-paper

Mitchell, G. R. (2006). Team B Intelligence Coups. *Quarterly Journal of Speech, 92*(2), 144-173. Retrieved March 3, 2019, from http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=1&sid=e0020be6-8fb6-4e86-a7cd-9869770300b6%40pdc-v-sessmgr05

Mitnick, K., & Simon, W. (2003). *The art of deception: Controlling the human element of security.* Indianapolis: Wiley publishing inc.

Mitre. (2018, January 1). *Mitre ATTCK*. Retrieved March 5, 2019, from Mitre web site: https://attack.mitre.org/

Moisescu, F., Boscoianu, M., Prelipcean, G., & Mariana, L. (2010). Intelligent agents in military decision making. *Science & Military, 5*(1). Retrieved April 17, 2019, from http://www.aos.sk/casopisy/science/dokumenty/archiv/2010_1/cl11.pdf

Molok, N. N., Chang, S., & Ahmad, A. (2010). Information leakage through online social networking: Opening the doorway for advanced persistence threats. *Proceedings of the 8th Australian Information Security Mangement Conference* (p. online). Perth: School of Computer and Information Science, Edith Cowan University, Perth, Western Australia. doi:10.4225/75/57b673cf34781

Moore, J. W. (2010). From Phishing To Advanced Persistent Threats: The Application Of Cybercrime Risk To The Enterprise Risk Management Model. *The Review of Business Information Systems, 14*(4), 27-36. doi:https://doi.org/10.19030/rbis.v14i4.358

Morris, J. (2001, February 19). Since Pan Am 103, a 'facade of security.'. *U.S. News & World Report, 130*(7), p. 28. Retrieved March 3, 2019, from http://web.a.ebscohost.com/ehost/detail/detail?vid=1&sid=fbb9583c-8773-4909-a365-a217dbd1708d%40sdc-v-sessmgr06&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=4069124&db=afh

National Academy of Engineering. (2019). *NAE Grand Challenges for Engineering.* Retrieved February 9, 2019, from Secure Cyberspace: http://www.engineeringchallenges.org/challenges/cyberspace.aspx

National Civil Aviation Review Commission. (1997). *Avoiding aviation gridlock and reducing the accident rate a consensus for change.* Washington: National Civil Aviation Review Commission. Retrieved March 3, 2019, from www.library.unt.edu/gpo/NCARC/reports/summary.doc

NATO. (2017). *The NATO Alternative Analysis Handbook.* Brussels: NATO. Retrieved April 17, 2019, from https://www.act.nato.int/images/stories/media/doclibrary/alta-handbook.pdf

NIST. (2009, September 1). *Technical Guide to Information Security Testing and Assessment.* Retrieved March 13, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

NIST. (2013, February 10). *Special Publication 800-53 revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.* Retrieved December 10, 2018, from https://doi.org/10.6028/NIST.SP.800-53r4

NIST. (2013b, April 30). *Security Controls and Assessment Procedures for Federal Information Systems and Organizations.* Retrieved February 3, 2019, from NIST website: https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf

NIST. (2017, January 10). *Framework for Improving Critical Infrastructure Cybersecurity (draft).* Retrieved April 10, 2019, from NIST: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

Norman, W. M. (2015). *BSS5: The Battle Staff SMARTbook, 5th Ed.* (5.0 ed.). Totowa, NJ, US: Lightning press.

Oakley, J. G. (2019). Purple Teaming. In J. G. Oakley, *Professional Red Teaming* (pp. 105-115). Berkeley: Apress.

Okoli, C., & Pawlowski, S. (2004). *The Delphi Method as a Research Tool: An Example, Design Considerations and Applications.* Information & Management. Vol 42:1. pp 15–29. retrieved from: (https://spectrum.library.concordia.ca/976864/1/OkoliPawlowski2004 DelphiPostprint.pdf) 24.11.2018.

Osgood, C. E. (1960). Cognitive Dynamics in the Conduct of Human Affairs. *The Public Opinion Quarterly, 24*(2 Special Issue: Attitude Change), 341-365. Retrieved from https://www.jstor.org/stable/2746409

Oxford dictionary. (2019, March 4). *Oxford living dictionary*. Retrieved March 4, 2019, from Oxford living dictionary: https://en.oxforddictionaries.com/definition/cyber

Pappas, N. (1995). *Plato and the Republic.* London: Routledge.

Paul, R. J. (2007, December 19). Challenges to information systems: time to change. *European journal of information systems, 16*(3), pp. 193-195. doi:https://doi.org/10.1057/palgrave.ejis.3000681

Peake, C. (2003, July 16). *Red Teaming: The Art of Ethical Hacking.* SANS: SANS Institut. Retrieved from https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodogy for Information Systems Research. *Journal of Management Information Systems, 24:3*, 45-77. Retrieved November 6, 2018, from https://doi.org/10.2753/MIS0742-1222240302

PTES. (2014, August 16). *The Penetration Testing Execution technical guide.* Retrieved March 6, 2019, from Pentest standard: http://www.pentest-standard.org/index.php/Main_Page

PwC UK and BAE. (2017). *Operation Cloud Hopper.* London: Price Waterhouse Cooper. Retrieved March 4, 2019, from https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

R0lan. (2018, January 1). *Awesome red teaming*. Retrieved from GitHub yeyintminthuhtut: https://github.com/yeyintminthuhtut/Awesome-Red-Teaming#-training--free-

Raggad, B. G. (2010). *Information security management: concepts and practice.* England: www.printondemand-worldwide.com.

Randhawa, S., Turnbull, B., Yuen, J., & Dean, J. (2018). Mission-Centric Automated Cyber Red Teaming. *In Proceedings of the 13th International Conference on Availability, Reliability and Security ARES 2018* (pp. 1-11). Hamburg: ACM. doi:0.1145/3230833.3234688

Ray, H. T., Vemuri, R., & Kantubhukta, H. R. (2005). Toward an Automated Attack Model for Red Teams. *Security and Privacy, IEEE Symposium on [1540-7993], 3*(4), 18-25. Retrieved March 6, 2019, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1492336

Renzi, A. B., & Freitas, S. (2015). *The Delphi method for future scenarios construction.* 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015: Elsevier B.V. retrieved from (https://www.sciencedirect.com/science/article/pii/S2351978915008276) 29.11.2018.

Robertson, D. (2010). *The Philosophy of Cognitive Behavioural Therapy: Stoic Philosophy as Rational and Cognitive Psychotherapy.* Abingdon-on-Thames: Routledge.

Robson, C. (2002). *Real World Research.* Great Britain: Blackwell Publishing.

Royce, W. W. (1970). Managing the development of large software systems. *Proceedings IEEE WESCON* (pp. 1-9). IEEE Computer Society Press, originally published by TRW. Retrieved June 10, 2019, from https://leadinganswers.typepad.com/leading_answers/files/original_waterfall_paper_winston_royce.pdf

RTJ. (2016, January 1). *The Annoying Red Teamer: A Philosophical Approach to the Problem.* (M. Mateski, Editor) Retrieved December 1, 2018, from Red team journal: https://redteamjournal.com/2016/12/the-annoying-red-teamer-a-philosophical-approach-to-the-problem/

Runyon, T. C. (2004, May 26). *A MDMP For All Seasons: Modifying The MDMP For Success.* Monograph, Army command and general staff coll, School of advanced military studies, Fort Leavenworth KS. Retrieved March 12, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a435830.pdf (12.3.2019)

Sandia national laboratories. (2000, 7 24). *Keep telling yourself: "The Red Team is my friend...".* Retrieved March 2, 2019, from Sandia national laboratories news releases: https://www.sandia.gov/media/NewsRel/NR2000/redteam.htm

Sandoz, J. F. (2001). *Red Teaming: Shaping the Transformation Process.* Alexandria: Institute for defense analyses. Retrieved April 10, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a398285.pdf

Scaled Agile INC. (2018, december 1). *SAFe by Scaled Alliance.* Retrieved March 4, 2019, from Scaled alliance home page: https://www.scaledagileframework.com/

Schlauderer, S., Overhage, S., & Fehrenbach, B. (2015). Widely Used but also Highly Valued? Acceptance Factors and Their Perceptions in Water-Scrum-Fall Projects. *Thirty Sixth International Conference on Information Systems.* Fort Worth: Association for information systems. Retrieved from https://aisel.aisnet.org/icis2015/proceedings/ManagingIS/7/

ScrumAlliance. (2018, January 1). *Scrum Alliance.* Retrieved March 4, 2019, from Scrum Alliance web page: https://www.scrumalliance.org/

Siponen, M. (2006). Information Security Standards Focus on the Existence of Process,Not Its Content. *Communications of ACM, 49*(8), 97-100. Retrieved January 13, 2019, from https://www.researchgate.net/profile/Mikko_Siponen/publication/220422725_Information_security_standards_focus_on_the_existence_of_process_not_its_content/links/5564a83b08ae94e957204ef2/Information-security-standards-focus-on-the-existence-of-process-not-i

Siponen, M., & Baskerville, R. L. (2018). Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example. *Journal of the Association for information Systems, 19*(4), Article 4. doi:10.17705/1jais.00491

Siponen, M., & Klaavuniemi, T. (2019). Narrowing the Theory's or Study's Scope May Increase Practical Relevance. *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019)* (pp. 6260-6269). Manoa: University of Hawai'i at Manoa. Retrieved May 29, 2019, from http://hdl.handle.net/10125/60060

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270. doi:https://doi.org/10.1016/j.im.2008.12.007

Skroch, M. J. (2009). *Modeling and simulation of Red Teaming. Part 1, Why Red Team M&S?* . Office of Scientific and Technical Information. Washington D.C.: U.S. Department of Energy.

Solymar, L. (1999). *Getting the Message: A History of Communications.* Oxford: Oxford University Press.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*(34), 503-522. Retrieved February 11, 2019, from https://pdfs.semanticscholar.org/387f/288a218a3e9c075c193910cd09f9b6874d88.pdf

Stoll, C. (1988). Stalking the wily hacker. *Communication of the ACM, 31*(5), 484-497. Retrieved February 25, 2019, from https://dl.acm.org/citation.cfm?id=42412

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York: Doubleday.

Stuttard, D., & Pinto, M. (2008). *The web application hacker's handbook: Finding and exploiting security flaws.* Indianapolis: Wiley Publishing, Inc.

Sugimori, Y., Kusunoki, K., Cho, F., & Uchikawa, S. (1977). Toyota production system and Kanban system Materialization of just-in-time and respect-for-human system. *The International Journal of Production Research, 15*(6), 553-564. Retrieved June 6, 2019, from https://doi.org/10.1080/00207547708943149

Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences, 11*(5), 23-29. Retrieved January 23, 2019, from https://s3.amazonaws.com/academia.edu.documents/30294093/113505-6969-ijecs-ijens.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1555492924&Signature=%2B23zdbsgriz5V8bBUMBICMPbSLo%3D&response-content-disposition=inline%3B%20filename%3DInformation_security

Sutherland, J., & Schwaber, K. (2011, January 29). *The Scrum Papers.* Retrieved June 5, 2019, from Nut, Bolts, and Origins of an Agile Framework: https://klevas.mif.vu.lt/~adamonis/pkp/1415p/lit/ScrumPapers.pdf

Symantec. (2011). *Advanced Persistent Threats: A Symantec Perspective.* Mountain View: Symantec. Retrieved March 5, 2019, from https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

Takanen, A., Demott, J., Miller, C., & Kettunen, A. (2018). *Fuzzing for software security testing and quality assurance second edition.* Norwood: Artech House.

Tan, T., Porter, S., Tele, T., & West, G. (2014). Computational Red Teaming for physical security assessment. *Tan, T., Porter, S., Tan, T., & West, G. (2014, June). Computational Red Teaming for physical security assessment. In The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent* (pp. pp. 258-263). Hong Kong: IEEE. Retrieved March 6, 2019, from https://ieeexplore.ieee.org/abstract/document/6917471

Taws, R. (2017). *Wargaming: Visualizing Conflict in French Printed Boardgames.* (P. S. Satish Padiyar, Ed.) London: Routledge.

The Holy See. (2019, 2 15). *CANONIZZAZIONI DEL SANTO PADRE GIOVANNI PAOLO II.* Retrieved from The Holy See website: http://www.vatican.va/news_services/liturgy/saints/ELENCO_SANTI_GPII.htm

The Institute of Risk Management. (2002). *A Risk Management Standard.* Retrieved February 26, 2019, from https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf 26.02.2019

The President's Commission on Aviation Security and Terrorism. (1990). *President's Commission on Aviation Security and Terrorism (the "Pan Am 103 Report").* Washington D.C.: The White house. Retrieved March 3, 2019, from https://archive.org/details/PCASTreport

Theocharis, G., Kuhrmann, M., Munch, J., & Diebold, P. (2015). Is Water-Scrum-Fall Reality? On the Use of Agile and Traditional Development Practices. *Product-Focused Software Process Improvement: 16th International Conference, PROFES 2015* (pp. 149-166). Bolzano: Springer. doi:10.1007/978-3-319-26844-6_11

TRADOC. (2019, February 14). *US Army training and doctrine command.* Retrieved February 14, 2019, from US Army training and doctrine command: https://www.tradoc.army.mil/

Tropotei, T. O. (2018). Criticism against the intelligence cycle. *Scientific Research & Education in the Air Force-AFASES* (pp. 77-88). Brasov: Publishing House of “Henri Coanda” Air Force Academy Str. Mihai Viteazu. doi:10.19062/2247-3173.2018.20

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security, 14*(3), 198 - 217. Retrieved from http://dx.doi.org/10.1108/09685220610670378

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *science, 185*(4157), 1124-1131. Retrieved March 15, 2019, from http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf

U.S. Department of Transportation. (2000). *Semiannual Report to Congress.* Office of Inspector General,, U.S. Department of Transportation. Washington: U.S. Department of Transportation. Retrieved March 3, 2019, from https://www.hsdl.org/?abstract&did=24905

University of Foreign Military and Cultural Studies. (2015). *The applied critical thinking handbook* (7 ed.). Fort Leavenworth: University of Foreign Military and Cultural Studies. Retrieved March 5, 2019, from https://fas.org/irp/doddir/army/critthink.pdf

University of Foreign Military and Cultural Studies. (2019, February 14). *University of Foreign Military and Cultural Studies*. Retrieved February 14, 2019, from University of Foreign Military and Cultural Studies home page: https://usacac.army.mil/organizations/ufmcs-red-teaming

US DOD. (2017, November 15). *Cybercom Challenges Industry: Be Agile, Precise.* Retrieved March 3, 2019, from US Department of defence: https://dod.defense.gov/News/Article/Article/1373397/cybercom-challenges-industry-be-agile-precise/

US Joint Chiefs of Staff. (2013). *Joint publication 2-0 Joint Intelligence.* Washington: US Joint Chiefs of Staff. Retrieved March 2, 2019, from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

US Joint Chiefs of Staff. (2013b). *Joint Publication 3-60 Joint Targeting.* Washington: US Joint Chiefs of Staff. Retrieved March 3, 2019, from https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf

US Joint Chiefs of Staff. (2016). *Joint Doctrine Note 1-16 Command Red Team.* Washington: US Joint Chiefs of Staff. Retrieved March 3, 2019, from https://fas.org/irp/doddir/dod/jdn1_16.pdf

US Joint Chiefs of Staff. (2017, July 12). *Joint Publication 1-0.* Washington: US Joint chiefs of staff. Retrieved April 18, 2019, from Doctrine for the Armed Forces of the United States: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2019-02-11-174350-967

US Joint Chiefs of Staff. (2017, June 16). *Joint Publication 5-0. Joint Planning.* Washington: US Joint Chiefs of Staff. Retrieved March 11, 2019, from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf

US Joint Chiefs of Staff. (2018, December 1). *Doctrines*. Retrieved March 3, 2019, from Joint Chiefs of Staff home page: http://www.jcs.mil/Doctrine/Joint-Doctine-Pubs/ (12.3.2019)

US Joint Chiefs of Staff. (2018, October 22). *Joint Publication 3-0. Joint Operations.* Washington: US Joint Chiefs of Staff. Retrieved April 27, 2019, from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910

US Navy. (2018, August 3). *SSC Atlantic Red Team: The Good 'Bad Guys'*. Retrieved April 10, 2019, from Official Website of the United States Navy: https://www.navy.mil/submit/display.asp?story_id=104650

US Senate. (1996, septmeber 17). Federal Aviation Reauthorization Act of 1996. *Law*. Washington D.C., Virginia, US: US senate. Retrieved March 3, 2019, from https://www.govinfo.gov/content/pkg/CREC-1996-09-17/pdf/CREC-1996-09-17-senate.pdf

USAF. (2012a, July 6). *Facts about 414th Combat Training Squadron "Red Flag"*. Retrieved March 5, 2019, from Nellis air force base website: https://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284176/414th-combat-training-squadron-red-flag/

USAF. (2012b, June 2). *Facts about Red Flag - Alaska*. Retrieved March 5, 2019, from Eielson Air Force Base website: https://www.eielson.af.mil/About-Us/Fact-Sheets/Display/Article/382359/red-flag-alaska/

USAF. (2017, October 1). *Nellis Airforce base website (USAF)*. Retrieved March 3, 2019, from 57th wing: https://www.nellis.af.mil/Units/57-WG/

Vance, A., Anderson, B., Kirwan, B. C., & Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). *Association for Information Systems*, 679-772. Retrieved February 11, 2019, from https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=2986&context=facpub

Veerasamy, N. (2009). High-level Methodology for Carrying out Combined Red and Blue Teams. *Second International Conference on Computer and Electrical Engineering (Vol. 1, pp. 416-420). IEEE.* (pp. 416-420). Dubai: IEEE. Retrieved March 6, 2019, from https://ieeexplore.ieee.org/abstract/document/5380465

VersionOne Inc. (2018, April 1). *12th annual State of Agile (tm) report.* Retrieved May 30, 2019, from State of Agile Report: https://agilebb.nl/wp-content/uploads/2018/04/versionone-12th-annual-state-of-agile-report.pdf

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of management journal, 15*(4), 407-426. Retrieved April 17, 2019, from https://www.jstor.org/stable/255139?origin=JSTOR-pdf&seq=1#page_scan_tab_contents

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security, 7*(1), 50-58. Retrieved February 19, 2019, from https://doi.org/10.1108/09685229910255223

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security, 38,* 97-102. doi:https://doi.org/10.1016/j.cose.2013.04.004

Vukalović, J., & Delija, D. (2015). Advanced Persistent Threats –Detection and Defence. *2015 38th International Convention on Information and*

Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1324-1330). Opatija: IEEE. doi: 10.1109/INFOCOM.2015.7218444

West, D. (2011). *Water-Scrum-Fall Is The Reality Of Agile For Most Organizations Today.* Cambridge: Forrester research inc. Retrieved March 3, 2019, from https://www.forrester.com/report/WaterScrumFall+Is+The+Reality+Of+Agile+For+Most+Organizations+Today/-/E-RES60109

Wikipedia. (2019a, May 23). *Lockheed P-80 Shooting Star*. Retrieved May 29, 2019, from Wikipedia: https://en.wikipedia.org/wiki/Lockheed_P-80_Shooting_Star

Wikipedia. (2019b, May 14). *Skunk Works*. Retrieved May 29, 2019, from Wikipedia: https://en.wikipedia.org/wiki/Skunk_Works

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM, 52*(9), 133-137. doi:10.1145/1562164.1562198

Wintjes, J. (2015, November 3). Europe's Earliest Kriegsspiel? Book Seven of Reinhard Graf zu Solms' Kriegsregierung and the 'Prehistory' of Professional War Gaming. *British Journal for Military History, 2*(1), 15-33. Retrieved January 4, 2019, from https://www.researchgate.net/publication/283461658_Europe%27s_Earliest_Kriegsspiel_Book_Seven_of_Reinhard_Graf_zu_Solms%27_Kriegsregierung_and_the_%27Prehistory%27_of_Professional_War_Gaming

Wood, B. J., & Duggan, R. A. (2000). Red teaming of advanced information assurance concepts. *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00. 2*, pp. 112-118. Hilton Head: IEEE. Retrieved April 10, 2019, from https://ieeexplore.ieee.org/abstract/document/821513

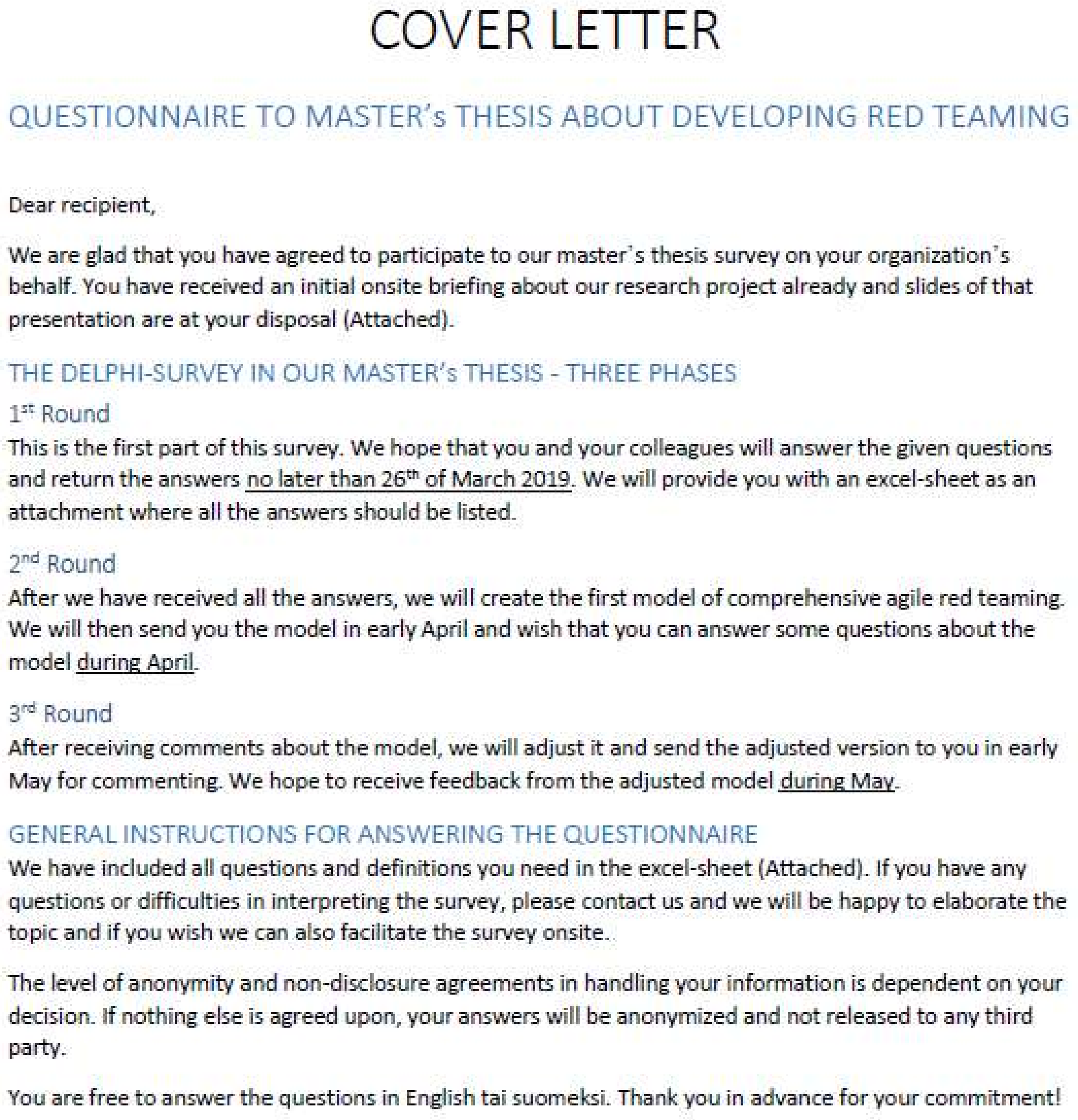
World of skunkworks. (2013, January 27). *How to Manage A Successful Skunk Works Project: Exploration of Kelly's Principles at Lockheed Martin*. Retrieved May 29, 2019, from World of skunkworks: http://worldofskunkworks.blogspot.com/2013/01/how-to-manage-successful-skunk-works.html

Zachman, J. A. (1987). A Framework for Information Systems Architecture. *IBM Systems Journal, 26*. Retrieved January 17, 2018, from http://www.zachman.com/images/ZI_PIcs/ibmsj2603e.pdf

Zenko, M. (2015). *Red Team: How to Succeed By Thinking Like the Enemy.* New York: Basic Books.

Zhao, M., Grossklags, J., & Liu, P. (2015). An Empirical Study of Web Vulnerability Discovery Ecosystems. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1105-1117). Denver: ACM. doi:10.1145/2810103.2813704

ANNEX 1: COVER LETTER FOR INITIAL SURVEY



COVER LETTER

QUESTIONNAIRE TO MASTER's THESIS ABOUT DEVELOPING RED TEAMING

Dear recipient,

We are glad that you have agreed to participate to our master's thesis survey on your organization's behalf. You have received an initial onsite briefing about our research project already and slides of that presentation are at your disposal (Attached).

THE DELPHI-SURVEY IN OUR MASTER's THESIS - THREE PHASES

1st Round

This is the first part of this survey. We hope that you and your colleagues will answer the given questions and return the answers no later than 26th of March 2019. We will provide you with an excel-sheet as an attachment where all the answers should be listed.

2nd Round

After we have received all the answers, we will create the first model of comprehensive agile red teaming. We will then send you the model in early April and wish that you can answer some questions about the model during April.

3rd Round

After receiving comments about the model, we will adjust it and send the adjusted version to you in early May for commenting. We hope to receive feedback from the adjusted model during May.

GENERAL INSTRUCTIONS FOR ANSWERING THE QUESTIONNAIRE

We have included all questions and definitions you need in the excel-sheet (Attached). If you have any questions or difficulties in interpreting the survey, please contact us and we will be happy to elaborate the topic and if you wish we can also facilitate the survey onsite.

The level of anonymity and non-disclosure agreements in handling your information is dependent on your decision. If nothing else is agreed upon, your answers will be anonymized and not released to any third party.

You are free to answer the questions in English tai suomeksi. Thank you in advance for your commitment!

The contact information of the researchers and the supervisor has been removed from this letter.

ANNEX 2: INITIAL SURVEY QUESTIONNAIRE

RED TEAMING QUESTIONNAIRE - INITIAL SURVEY 1.-26.3.2019 You may answer in English tai sitten suomeksi.

1. Please answer the three questions below as a group and think of the top five issues in every question and their explanations (Three tables below Q1, Q2, Q3)
2. Please explain your group composition with the level of details you prefer (Table below, GROUP COMPOSITION)
3. If you have any additional questions or comments about this questionnaire, please add them to your answer sheet to additional comments part.
4. Please submit your answer sheet no later than 26 March 2019

RED TEAMING - is a methodology that enables organisations to identify their own vulnerabilities and challenge products, plans, policies or procedures. It involves any activity when someone attempts to understand, challenge, or test a system, plan, or perspective through the eyes of an adversary or competitor. The expected outcome of red teaming is the development of more robust products, plans, policies and procedures in any domain

PRE-ENGAGAMENT PHASE - Activities that are conducted before the actions against customer are initiated. This could be for example marketing, setting the scope, forming your team, planning the tasks and schedule, etc.

ENGAGEMENT PHASE - Activities that start after signing a deal with the customer. Includes planning, information collection, team leadership, infiltrations, attacks, etc. Engagement ends when activities against customer cease.

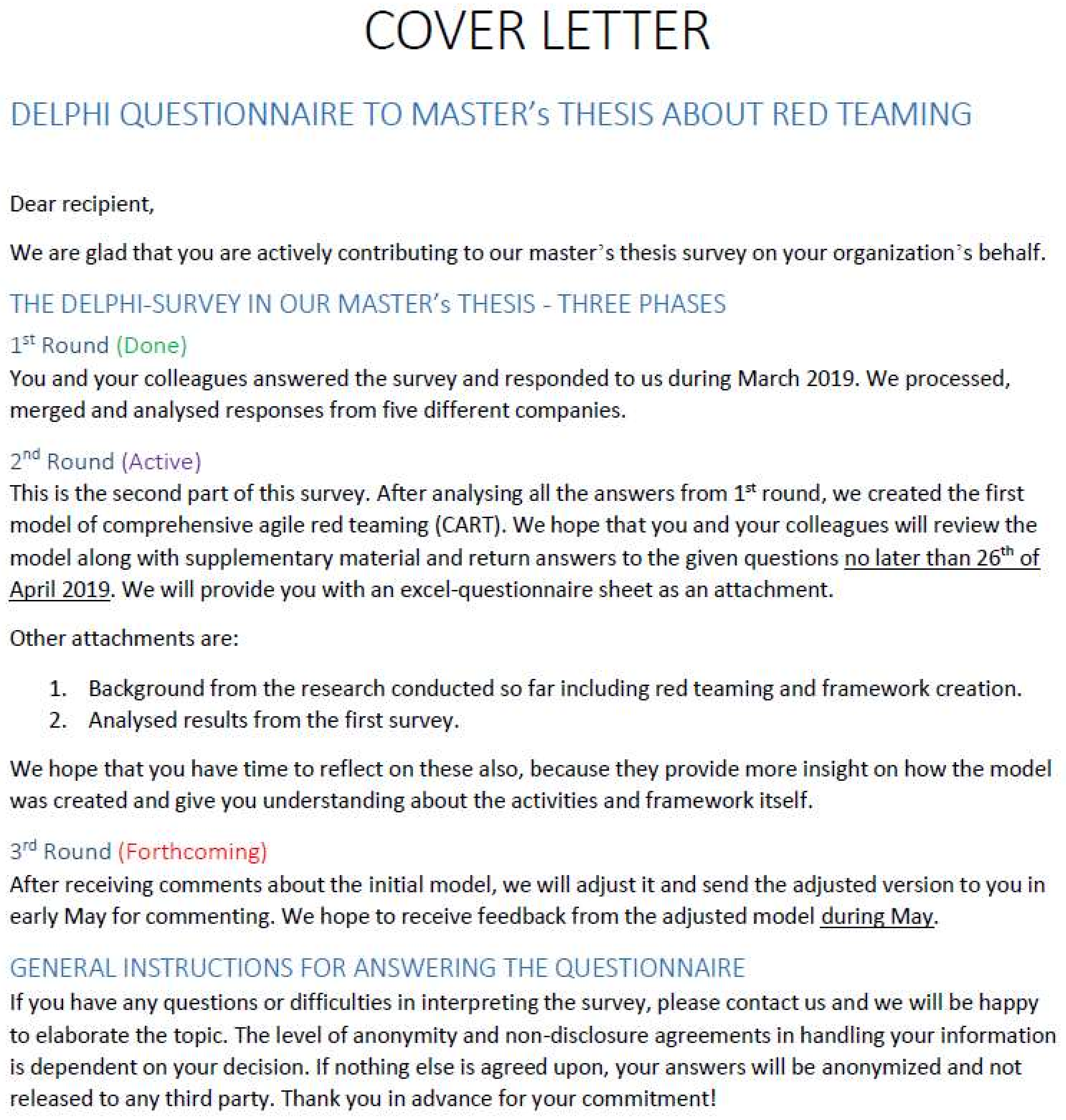
POST-ENGAGEMENT PHASE - Activities such as analysing the results, writing the reports, briefing of results to customer and possible corrective measures conducted together with customer.

Question 1. Please list the top five challenges you face in red teaming from every phase of the engagement. Please provide a short title and rationale for each of your issues

Question 2. Please list the top five success factors / Good things / Easy to do / etc issues from every phase. Please provide a short title and rationale for each of your issues

Question 3. Please list Maximum of five additional general issues about red teaming, positive or negative or things that should be developed in general (Disregard phases in this question)

ANNEX 3: DELPHI 1 COVER LETTER



COVER LETTER

DELPHI QUESTIONNAIRE TO MASTER's THESIS ABOUT RED TEAMING

Dear recipient,

We are glad that you are actively contributing to our master's thesis survey on your organization's behalf.

THE DELPHI-SURVEY IN OUR MASTER's THESIS - THREE PHASES

1st Round (Done)

You and your colleagues answered the survey and responded to us during March 2019. We processed, merged and analysed responses from five different companies.

2nd Round (Active)

This is the second part of this survey. After analysing all the answers from 1st round, we created the first model of comprehensive agile red teaming (CART). We hope that you and your colleagues will review the model along with supplementary material and return answers to the given questions no later than 26th of April 2019. We will provide you with an excel-questionnaire sheet as an attachment.

Other attachments are:

1. Background from the research conducted so far including red teaming and framework creation.
2. Analysed results from the first survey.

We hope that you have time to reflect on these also, because they provide more insight on how the model was created and give you understanding about the activities and framework itself.

3rd Round (Forthcoming)

After receiving comments about the initial model, we will adjust it and send the adjusted version to you in early May for commenting. We hope to receive feedback from the adjusted model during May.

GENERAL INSTRUCTIONS FOR ANSWERING THE QUESTIONNAIRE

If you have any questions or difficulties in interpreting the survey, please contact us and we will be happy to elaborate the topic. The level of anonymity and non-disclosure agreements in handling your information is dependent on your decision. If nothing else is agreed upon, your answers will be anonymized and not released to any third party. Thank you in advance for your commitment!

The contact information of the researchers and the supervisor has been removed from this letter.

ANNEX 4: CART FRAMEWORK VERSION 0.1

These is the material that was sent to the recipients during round 1 of the Delphi-questionnaire.

The initial model was formed with the purpose of solving the comprehensiveness problem in red teaming. Model is simple and does not include all the recognized challenges and remediations because the first goal is to see if the framework idea is conceivable.

CART framework version 0.1 consists of:

- Five continuous **activities**
- 1 baseline and 3 active **Phases**
- 13 **steps** that are divided under the phases
- **Products** that are defined in the backlogs

The model is constructed with the following ideas:

1. A framework needs to be produced with continuous activities, flexible phases and product backlog to gain comprehensiveness.
2. Consecutive phases receive input from the previous ones. This emphasizes the importance of structured process, initial analysis and planning.
3. Structured problem solving requires defined steps inside phases with fixed actions and products in order to be understandable and repeatable.
4. Red teaming cannot stop in presentation of the engagement results.
5. Nothing happens if management does not buy-in the red teaming idea. Therefore, the framework needs to be easily communicable.

CART - model has five continuous activities;

1. **Planning** is a structured activity to scope, define and solve a given assignment (problem). Planning defines the objective (what), timeline (when), environment (where), resources (who) and rationale (why) for the execution of the assignment. Plan describes how the assignment is conducted, including breakdown of products, tasks and responsibilities.
2. **Intelligence** is a systematic methodology to collect, analyse and disseminate information from several sources and domains. It builds the situational awareness, which is prerequisite for planning, targeting and conducting red team efforts.
3. **Targeting** is a structured process to analyse systems and create means to deliver effects to those systems. Targeting receives inputs from planning and intelligence. System analytics is used in describing target system architecture and break down the system to a component level.

4. **Communication** – Internal communication is an essential element of leading and developing the red team through all phases of the assignment. External communication with client is prerequisite in order to define objectives and raise awareness. It is needed for co-ordination and reviews during engagement and has a significant role for successful follow-on activities during provide phase. Collaboration platforms provide the technical capabilities for communication in all activities.
5. **Assessment** is a continuous activity that supports decision making by analysing progress towards objectives and changes in the environment. Assessment consists of monitoring, evaluation and feedback to all other activities.

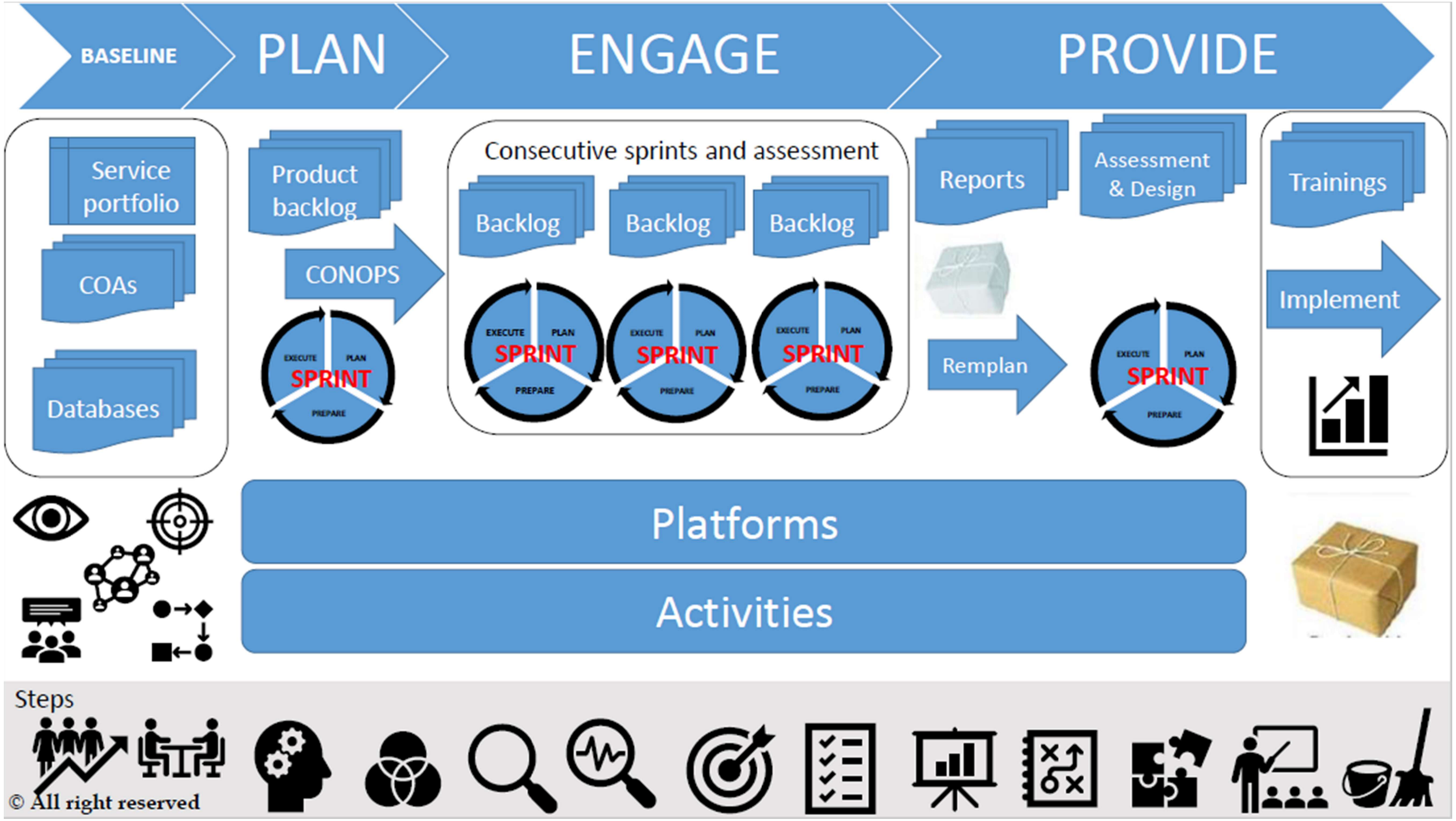
and 1 baseline + 3 active phases which are divided into steps;

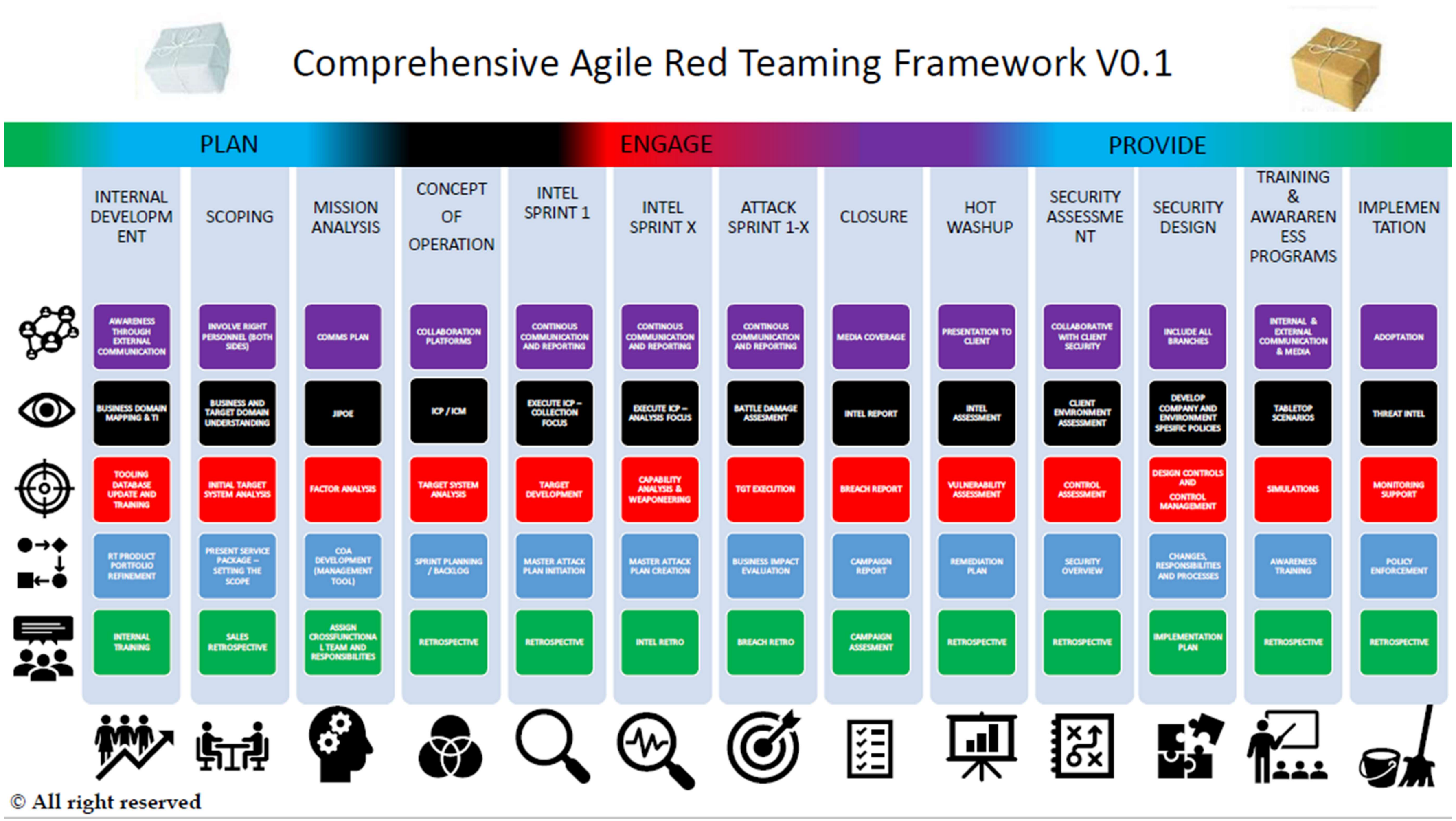
The BASELINE is the prerequisite for all the other phases. Baseline is constantly developing. Baseline has only one step; The Internal development which creates the baseline capability. Internal development consists of adopting the idea of comprehensive agile red teaming framework. This adaptation includes preparation of platforms for communication, intelligence, tooling and service portfolio which has predefined product backlogs and courses of actions. These reusable components are the building blocks of the framework. Internal development includes the active business domain and threat intelligence efforts to build realistic adversary emulation methods. Development and training of the own red teams' and affiliated personnel is continuous.

1. **PLAN** – This phase includes intelligence preparation of the environment and analysing the future assignments scope. Concept of operation (CONOPS) is created to manage the future assignment. Planning phase has three steps.
   - 1.1. Scoping – During this step an initial scope is defined with client. Scope is based on the maturity and needs of the client.
   - 1.2. Mission analysis – Environment and initial factor analysis are done. These create the basis of initial courses of actions and plans for the engagement. COA is presented to the client for adjustment and approval.
   - 1.3. Concept of operation – After course of action is approved by client it is refined to a more detailed CONOPS. Detailed planning and analysis are done along with product backlog and sprint planning.
2. **ENGAGE** – During this phase the active intelligence gathering, social engineering, network operations and other actions are commenced. Engagement phase does not have fixed step number. Steps are defined in the CONOPS.
   - 2.1. Intel Sprint 1 – Collection focused step which builds the understanding of the comprehensive target architecture. (Not just technical)
   - 2.2. Intel Sprint x – Several intel steps can be taken depending on the complexity and size of the target. Following steps should be more focused on analysis and post initial compromise activities like lateral movement and persistence.

   2.3. Attack Sprint x – This step aims to launch the attacks to provide the effects needed for the target (DDoS, Locker, Wiper, Manipulation, Physical, etc). If production environment is not in use a simulation needs to be conducted which aids in the presentation.
   2.4. Closure – Removal of modification and malware from the clients' systems and remediation of social engineering effects. Sufficient time slot reserved for team reporting and preparation of the next phase.
3. **PROVIDE** – This is the phase where results of the engagement are reported to the client along with a remediation plan which includes the consecutive steps. Goal is to reassess, design and implement better security. Training and raising awareness of clients' employees supports the implementation. This phase has five steps.
   3.1. Hot washup – During this step the results are presented to the client in meetings, workshops and reports. A remediation plan is also introduced.
   3.2. Security Assessment – First step in remediation is the comprehensive assessment of current policies, risk management and controls to provide overview of the security situation and corrections.
   3.3. Security design – Step is taken to improve the previous assessment artifacts with corrective measures. User participation from client-side non-security branches is encouraged to increase commitment to security.
   3.4. Training & awareness – Various training initiatives are carried out in all levels of the company. Training supports the implementation of newly designed security items, raises awareness and teaches the employees to mitigate crisis situations in simulations and tabletop games.
   3.5. Implementation – Support the client in technical and policy implementation issues along with monitoring and threat intel.

The model consists of several different products that are produced during the steps i.e. Intelligence collection plan, Concept of operation, target system analysis, HWU-brief, etc. For the planning purpose a product backlog is created and tied to the steps which is easy to follow by clients. Some products are refined constantly during multiple steps and considered as living documents/products. Products are not presented yet in the initial framework. The CART framework version 0.1 is depicted below.


BASELINE
PLAN
ENGAGE
PROVIDE
Service portfolio
COAs
Databases
Product backlog
CONOPS
SPRINT
EXECUTE
PLAN
PREPARE
Consecutive sprints and assessment
Backlog
Backlog
Backlog
SPRINT
EXECUTE
PLAN
PREPARE
SPRINT
EXECUTE
PLAN
PREPARE
SPRINT
EXECUTE
PLAN
PREPARE
Reports
Remplan
Assessment & Design
SPRINT
EXECUTE
PLAN
PREPARE
Trainings
Implement
Platforms
Activities
Steps
© All right reserved



Comprehensive Agile Red Teaming Framework V0.1

	PLAN				ENGAGE					PROVIDE		
INTERNAL DEVELOPM ENT	SCOPING	MISSION ANALYSIS	CONCEPT OF OPERATION	INTEL SPRINT 1	INTEL SPRINT X	ATTACK SPRINT 1-X	CLOSURE	HOT WASHUP	SECURITY ASSESSME NT	SECURITY DESIGN	TRAINING & AWARAREN ESS PROGRAMS	IMPLEMEN TATION
AWARENESS THROUGH EXTERNAL COMMUNICATION	INVOLVE RIGHT PERSONNEL (BOTH SIDES)	COMMS PLAN	COLLABORATION PLATFORMS	CONTINOUS COMMUNICATION AND REPORTING	CONTINOUS COMMUNICATION AND REPORTING	CONTINOUS COMMUNICATION AND REPORTING	MEDIA COVERAGE	PRESENTATION TO CLIENT	COLLABORATIVE WITH CLIENT SECURITY	INCLUDE ALL BRANCHES	INTERNAL & EXTERNAL COMMUNICATION & MEDIA	ADOPTATION
BUSINESS DOMAIN MAPPING & TI	BUSINESS AND TARGET DOMAIN UNDERSTANDING	JIPOE	ICP / ICM	EXECUTE ICP – COLLECTION FOCUS	EXECUTE ICP – ANALYSIS FOCUS	BATTLE DAMAGE ASSESMENT	INTEL REPORT	INTEL ASSESSMENT	CLIENT ENVIRONMENT ASSESSMENT	DEVELOP COMPANY AND ENVIRONMENT SPESIFIC POLICIES	TABLETOP SCENARIOS	THREAT INTEL
TOOLING DATABASE UPDATE AND TRAINING	INITIAL TARGET SYSTEM ANALYSIS	FACTOR ANALYSIS	TARGET SYSTEM ANALYSIS	TARGET DEVELOPMENT	CAPABILITY ANALYSIS & WEAPONEERING	TGT EXECUTION	BREACH REPORT	VULNERABILITY ASSESMENT	CONTROL ASSESSMENT	DESIGN CONTROLS AND CONTROL MANAGEMENT	SIMULATIONS	MONITORING SUPPORT
RT PRODUCT PORTFOLIO REFINEMENT	PRESENT SERVICE PACKAGE – SETTING THE SCOPE	COA DEVELOPMENT (MANAGEMENT TOOL)	SPRINT PLANNING / BACKLOG	MASTER ATTACK PLAN INITIATION	MASTER ATTACK PLAN CREATION	BUSINESS IMPACT EVALUATION	CAMPAIGN REPORT	REMEDIATION PLAN	SECURITY OVERVIEW	CHANGES, RESPONSIBILITIES AND PROCESSES	AWARENESS TRAINING	POLICY ENFORCEMENT
INTERNAL TRAINING	SALES RETROSPECTIVE	ASSIGN CROSSFUNCTIONA L TEAM AND RESPONSIBILITIES	RETROSPECTIVE	RETROSPECTIVE	INTEL RETRO	BREACH RETRO	CAMPAIGN ASSESMENT	RETROSPECTIVE	RETROSPECTIVE	IMPLEMENTATION PLAN	RETROSPECTIVE	RETROSPECTIVE

© All right reserved

ANNEX 5: DELPHI QUESTIONNAIRE 1

RED TEAMING QUESTIONNAIRE - 1st DELPHI ROUND 7.-26.4.2019 You may answer in English tai sitten suomeksi.

1. Please answer the five questions based on the material you've read as a group. Open comments are valued.
2. Please explain your group composition with the level of details you prefer (Table below, GROUP COMPOSITION)
3. If you have any additional questions or comments about this questionnaire, please add them to your answer sheet to additional comments part (Table below ADDITIONAL COMMENTS)
4. Please submit your answer sheet no later than 26 April 2019 to jussi.t.tuovinen@student.jyu.fi and kimmo.j.frilander@student.jyu.fi

Q1 - How are you acquainted with the background material? Answer from (1) to (5) with the help of reference grading below.

(1) I just read the Basic material (Framework abstract and 6 slides)
(2) x
(3) I looked through the background and initial survey material once to get overall picture.
(4) x
(5) I studied the material thoroughly and understood it.

Q2 - Is the CART framework conceivable? Can you understand and differentiate the purpose of continuous activities, phases, steps and products?

(1) Framework is obscure.
(2) x
(3) Framework is understandable, but it needs changes.
(4) x
(5) Yes, I could utilise CART framework for red teaming assignments in my organization.

Q3 - Give grade for the continuous activities from (1) to (5), with the help of reference grading below.

(1) I cannot understand purpose of the activities.
(2) x
(3) Activities are needed, but they call for improvement.
(4) x
(5) Activities are justified and their role in different phases and steps is easy to understand.

ANNEX 5: DELPHI QUESTIONNAIRE 1

Q4 - Give grade for the phases from (1) to (5), with the help of reference grading below.

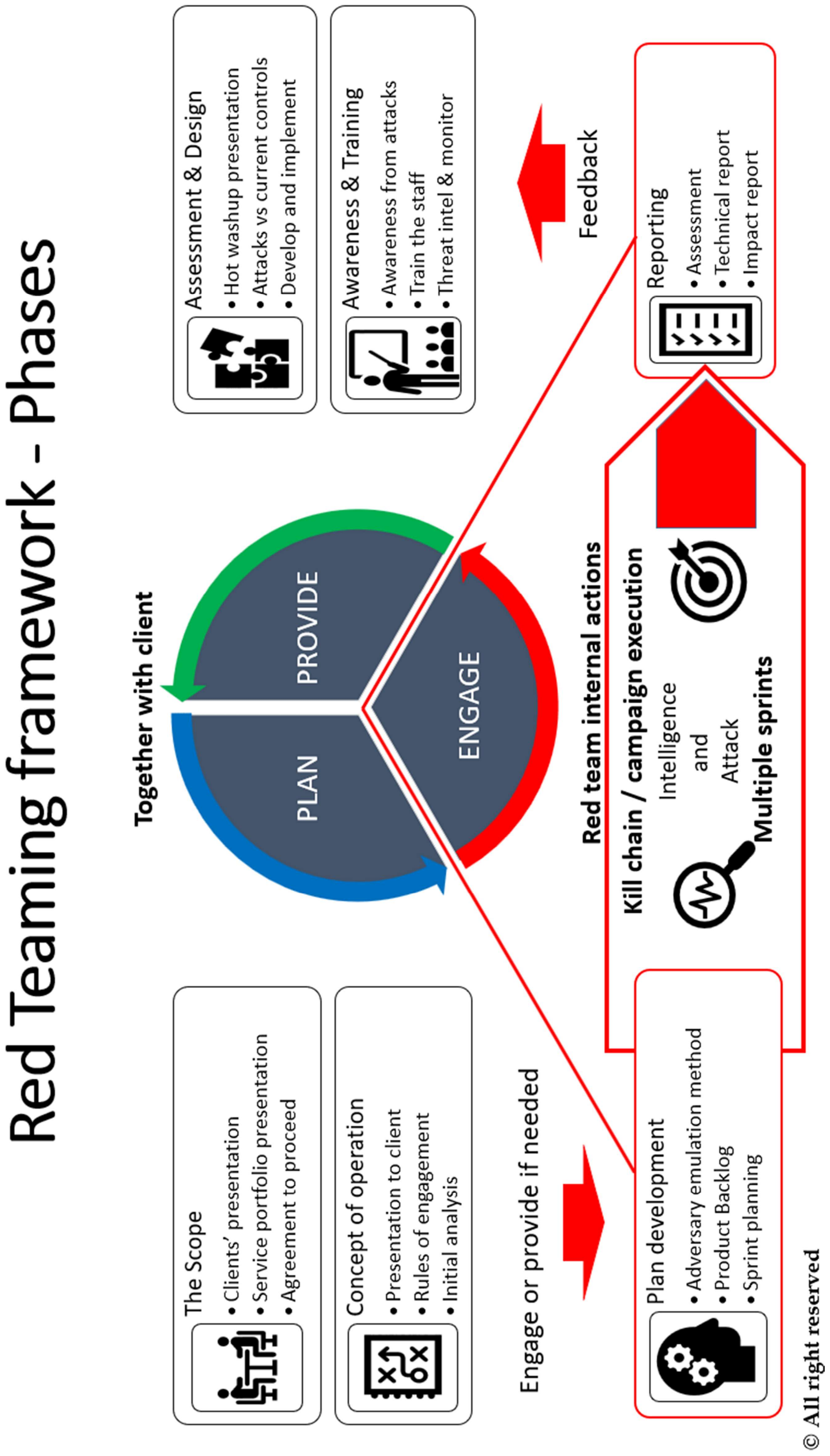
(1) I cannot understand purpose of the phases.
(2) x
(3) Phases are needed, but their sectioning in relation to steps calls for improvement.
(4) x
(5) Phases are justified and they are convergent with activities and steps.

Q5 - Give grade for steps from (1) to (5), with the help of reference grading below.

(1) I cannot understand purpose of the steps.
(2) x
(3) Steps are needed, but they call for improvement.
(4) x
(5) Steps are justified and their relation to activities and phases is easy to understand.

ANNEX 6: CART FRAMEWORK

These are the pictures that were explained during the second Delphi round as a part of the presentation.



Red Teaming framework - Phases

The Scope
- Clients' presentation
- Service portfolio presentation
- Agreement to proceed

Concept of operation
- Presentation to client
- Rules of engagement
- Initial analysis

Together with client

PLAN

PROVIDE

ENGAGE

Assessment & Design
- Hot washup presentation
- Attacks vs current controls
- Develop and implement

Awareness & Training
- Awareness from attacks
- Train the staff
- Threat intel & monitor

Engage or provide if needed

Feedback

Plan development
- Adversary emulation method
- Product Backlog
- Sprint planning

Red team internal actions

Kill chain / campaign execution

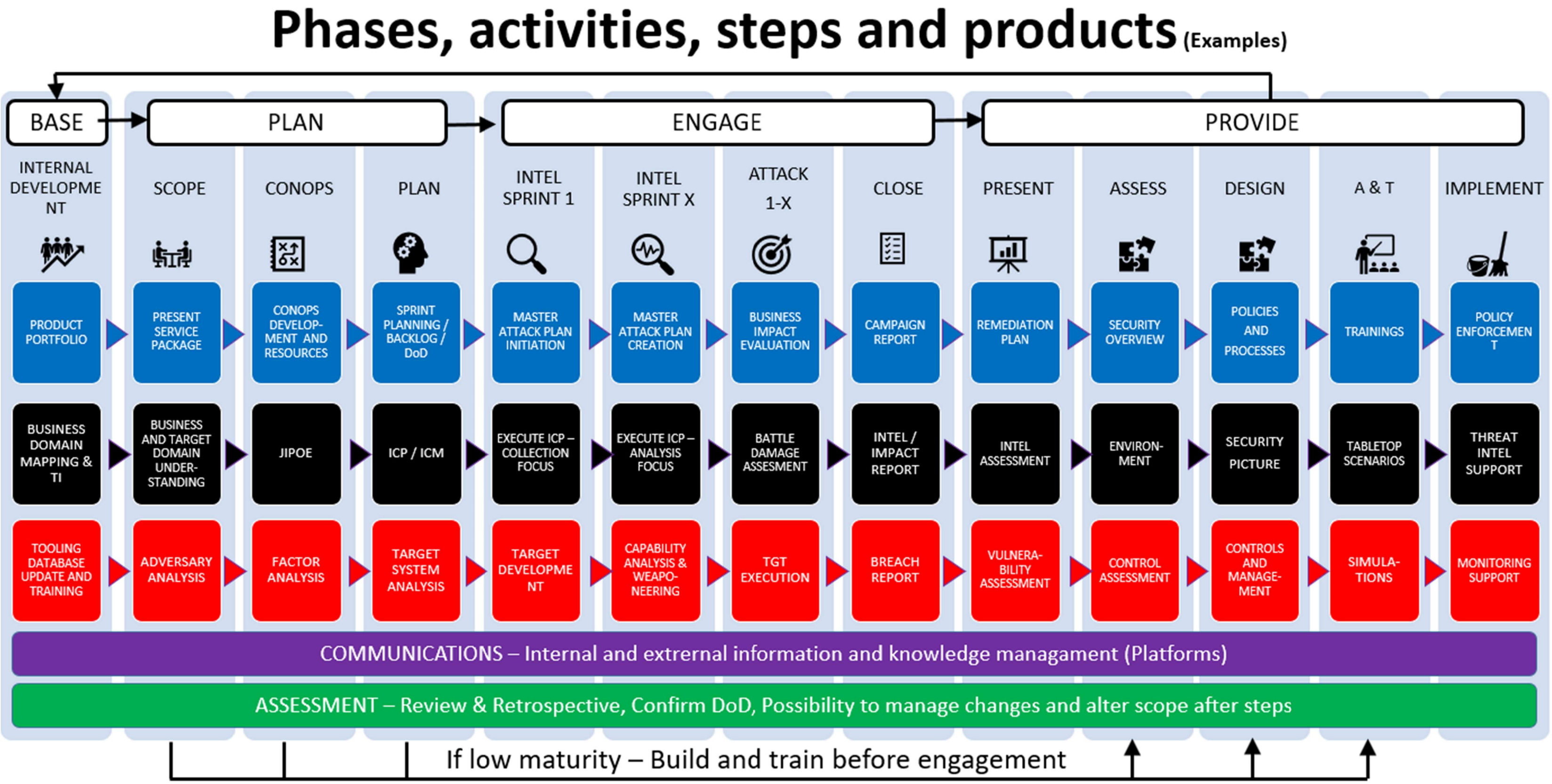
Intelligence and Attack

Multiple sprints

Reporting
- Assessment
- Technical report
- Impact report

© All right reserved

SIMPLE CART FRAMEWORK.



Phases, activities, steps and products (Examples)

BASE	PLAN			ENGAGE				PROVIDE				
INTERNAL DEVELOPMENT	SCOPE	CONOPS	PLAN	INTEL SPRINT 1	INTEL SPRINT X	ATTACK 1-X	CLOSE	PRESENT	ASSESS	DESIGN	A & T	IMPLEMENT
PRODUCT PORTFOLIO	PRESENT SERVICE PACKAGE	CONOPS DEVELOP-MENT AND RESOURCES	SPRINT PLANNING / BACKLOG / DoD	MASTER ATTACK PLAN INITIATION	MASTER ATTACK PLAN CREATION	BUSINESS IMPACT EVALUATION	CAMPAIGN REPORT	REMEDIATION PLAN	SECURITY OVERVIEW	POLICIES AND PROCESSES	TRAININGS	POLICY ENFORCEMENT
BUSINESS DOMAIN MAPPING & TI	BUSINESS AND TARGET DOMAIN UNDER-STANDING	JIPOE	ICP / ICM	EXECUTE ICP – COLLECTION FOCUS	EXECUTE ICP – ANALYSIS FOCUS	BATTLE DAMAGE ASSESMENT	INTEL / IMPACT REPORT	INTEL ASSESSMENT	ENVIRON-MENT	SECURITY PICTURE	TABLETOP SCENARIOS	THREAT INTEL SUPPORT
TOOLING DATABASE UPDATE AND TRAINING	ADVERSARY ANALYSIS	FACTOR ANALYSIS	TARGET SYSTEM ANALYSIS	TARGET DEVELOPMENT	CAPABILITY ANALYSIS & WEAPO-NEERING	TGT EXECUTION	BREACH REPORT	VULNERA-BILITY ASSESSMENT	CONTROL ASSESSMENT	CONTROLS AND MANAGE-MENT	SIMULA-TIONS	MONITORING SUPPORT

COMMUNICATIONS – Internal and extrernal information and knowledge managament (Platforms)

ASSESSMENT – Review & Retrospective, Confirm DoD, Possibility to manage changes and alter scope after steps

If low maturity – Build and train before engagement

COMPREHENSIVE CART FRAMEWORK with product examples.