National Defence University
Department of Military Technology
Report series 1: No 36

CRITICAL INFRASTRUCTURE PROTECTION AGAINST CYBER THREATS

Editor Jouko Vankka

CRITICAL INFRASTRUCTURE PROTECTION AGAINST CYBER THREATS

Editor, professor Jouko Vankka

Series 1, No 36
National Defence University
Department of Military Technology
HELSINKI 2014

Prof. Jouko Vankka (ed.): *Critical Infrastructure Protection against Cyber Threats*
Maanpuolustuskorkeakoulu, Sotatekniikan laitos
Julkaisusarja 1: N:o 36
National Defence University, Department of Military Technology
Report series 1: No 36

Most recent publications in pdf-format:
http://www.doria.fi/handle/10024/72633

Maanpuolustuskorkeakoulu – National Defence University
Sotatekniikan laitos – Deparment of Military Technology

ISBN 978-951-25-2599-7 (nid.)
ISBN 978-951-25-2600-0 (PDF)
ISSN 1796-4059

Juvenes Print
Tampere 2014

Preface

A postgraduate seminar series with a title Critical Infrastructure Protection against Cyber Threats held at the Department of Military Technology of the National Defence University in the fall of 2013 and 2014. This book is a collection of some of talks that were presented in the seminar. The papers address origin of critical infrastructure protection, wargaming cyberwar in critical infrastructure defence, cyber-target categorization, supervisory control and data acquisition systems vulnerabilities, electric power as critical infrastructure, improving situational awareness of critical infrastructure and trust based situation awareness in high security cloud environment. This set of papers tries to give some insight to current issues of the network-centric critical infrastructure protection.

The seminar has always made a publication of the papers but this has been an internal publication of the Finnish Defence Forces and has not hindered publication of the papers in international conferences. Publication of these papers in peer reviewed conferences has indeed been always the goal of the seminar, since it teaches writing conference level papers. We still hope that an internal publication in the department series is useful to the Finnish Defence Forces by offering an easy access to these papers.

Editor

Contents

Origin of Critical infrastructure Protection

-

Analyse of Ted G Lewis

Sakari Ahvenainen
Finnish National Defence University
sakari.ahvenainen@kolumbus.fi

Abstract

Purpose

This article is a report for Finnish Defence University course “Critical Infrastructure protection 2013” for post graduate students. This article analyses the chapter “Origin” of the course book by professor Ted G Lewis “Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation” [1] in order to find some new insight to the origin of critical infrastructure protection (CIP) and to find some new ideas for Finnish CIP activity.

The objective of this article is to answer the following question:

> *What is the origin of critical infrastructure protection based on (1) professor Ted G Lewis’s course book, (2) formal concept analysis and (3) evolution?*

Methodology

The process used in this article is evolutionary induction introduced by Karl Popper, Austrian-British professor and philosopher of science. It condenses to a process of (1) a starting point, an interesting problem, (2) its first interpretations, tentative theories, (3) processing information (critical thinking and sorting out of mistakes) and finally (4) output, new interpretation of the starting point and birth of new problems. [2, p. 287]

Findings

It is found in the article that science of critical infrastructure protection is a very new phenomenon but that critical infrastructure protection is as old as critical infrastructure itself. The first critical infrastructure for humans was the territory. Its protection was the origin of infrastructure protection, not National Communications System (NCS) in 1963. For Homo sapiens, modern man, this means at least some 100,000 years. And basically territory is the critical infrastructure for all animals and plants. It is also found in the article that the critical infrastructure protection and its science have more than ten evolutionary phases.

Originality/value

Even though “critical infrastructure protection” as a word is quite new, the phenomenon of “critical infrastructure protection” is old. The origin of critical infrastructure protection is farther away in history and has more steps in this article than presented by Lewis. This is according to evolution, the idea that all things have history, the only possible exception being Big Bang as a part of our universe.

Paper type

Research paper

Keywords

CIP, evolution, evolutive induction, infrastructure, formal concept analysis

1 Introduction

The process used in this article is evolutionary induction introduced by Karl Popper, Austrian-British professor and philosopher of science. It condenses to a process of (1) a starting point, interesting problem, (2) its first interpretation, tentative theories, (3) processing information (critical thinking and sorting out of mistakes) and finally (4) output, new interpretation of the starting point and birth of new problems. [2, p. 287]

Popper’s evolutive induction is itself a tentative theory to a problem: How to make science? Popper’s evolutive induction is also much like a cybernetic process: sensor (input, tentative theories), decision making unit (information processing; critical thinking and sorting out of mistakes) and action (output; new interpretation of the starting point and birth of new problems) [3, p. 155].

The objective of this article is to answer the following question:

> *What is the origin of critical infrastructure protection based on (1) professor Ted G Lewis's course book, (2) formal concept analysis and (3) evolution?*

In chapter 2 ("Origin") Professor Ted R Lewis briefly reviews the history of scientific infrastructure protection from 1962 to 2003. He maintains that his book is the first scientific presentation of critical infrastructure protection.

Based on my previous articles I believe that taking some new theories or views as tools to analyze the target, I will find new insight to the problem. Here the target of analyse is the origin of critical infrastructure protection. Lewis has not used widely the formal concept analysis or the notion of evolution in his book.

2 Abstract and comments of the subchapter "Origin"

I will present in this chapter the abstract of the chapter "Origin" (p. 29 – 48) of professor Ted R Lewis's book "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation" [1]. Lewis's own view is here introduced as a starting point and to analyze the origin of critical infrastructure protection. Because of the lenght of this article, all view points are quite basic. Subchapters in this chapter are named accoding to Lewis's book.

Lewis: The dawn of critical infrastructure protection

The CIP began with the creation of the (NCS) in 1963 after communication problems between the United States and the Soviet Union during the Cuban missile crises in 1962. [1, p. 30]

The objective of NCS was "to provide necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack". It was the first US act on governmental communication organization and there were many more to came [1, pp. 30 - 31]

The importance of communication continued in CIP because National Security Telecommunications Advisory Committee (NSTAC), established 1982, was perhaps the first organization to advise the president on critical infrastructure protection [1, p. 31].

It would take some twenty years before CIP would form as a notion after these "communication acts" [1, p. 31].

As the author of this article I have the following comments to the above mentioned quotations:

1. CIP started in USA 1963 with securing communication. This is not a surprise, because communication is the glue that binds parts of system together [4, pp. 156 and 160 - 1] to make synergy. Communication is not just a part of system; it is the part that builds up a system.
2. Communication was two decades the only CIP domain in CIP. Why? Was it because the need for CIP had not risen as USA felt to be safe in its continent, as Lewis also noticed.

Lewis: Dawn of terrorism in the United States

The Federal Emergency Management Agency (FEMA) was created in 1978 to fight hurricanes and earthquakes and soon also terrorism [1, p. 31]. FEMA is a powerful and large emergency organization in USA. It has some 7000 workers.

FEMA’s first act on terrorism was in 1984, when “Bhagwan Shree Rajneesh” cult poisoned salad bars in 10 restaurants in The Dalles, sickening 751 people with salmonella bacteria, forty-five of whom were hospitalized. It is still the largest germ warfare attack in U.S. history. [1, p. 32]

The importance of infrastructure was beginning to dawn on the federal government when in 1988 President Reagan issued Executive Order 12656 (about assignment of emergency preparedness responsibilities) [1, p. 32].

Terrorism was rising in 1990’s. The 1993 attack on the World Trade Centre by Ramzi Yousef, the capture of the Unabomber (1995), the devastating attack on the Federal Building in Oklahoma City, Oklahoma (1995), and the Sarin gas attack in a Tokyo subway in 1995 suggested a trend. Within five to six years, this would become known as the Global War on Terrorism (GWOT). [1, p. 33]

As the author of this article I have following comments to the above mentioned quotations:

1. FEMA and its work on fighting hurricanes and earthquakes and soon also terrorism was the second domain of CIP in USA after realising the importance of communication systems
2. The Dalles salmonella case with over 700 sick people is maybe not very widely known in Finland, although it is still the largest germ warfare attack in U.S. history.

Lewis: What is a critical infrastructure?

The modern origin of homeland security, and its corollary, CIP, can be placed somewhere between 1993 and late 1995 [1, p. 33].

Decision Directive 39 (PDD-39) issued by President Clinton in 1995 set the stage for what was to come a new Federal Department of Homeland Security. PDD-39 essentially declared war on terrorists [1, p. 33].

The criticality of national infrastructure and corresponding assets became an important issue when President Clinton issued Executive Order EO-13010 in 1996. It established a Presidential Commission on Critical Infrastructure Protection (PCCIP). Its first chairman was Robert March, hence "Marsh Report" [1, p. 34].

"Marsh Report" defines "critical infrastructure" in terms of "energy, banking and finance, transportation, vital human services, and telecommunications." It was the first publication to use the term "critical infrastructure" and has become one of the foundational documents of CIP history [1, p. 34].

The "Marsh Report" and Executive Order EO-13010 provided the first definition of infrastructure and loosely described an infrastructure as "a network of independent, mostly privately-owned, man-made systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services." And a Cl as "an infrastructure so vital that its incapacity or destruction would have a debilitating impact on our defence and national security." [1, p. 34]

Threats to these critical infrastructures fall into two categories: physical threats to tangible property, and threats of electronic, radio frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats") [1, p. 34].

Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation [1, p. 34].

Definition of critical infrastructure in PDD-63 went through rapid evolution and expansion after the attacks of 9/11 [1, p. 35].

Control of most public utility infrastructure was in the hands of corporations. Thus, in 1999, President Clinton established National Infrastructure Assurance Council (NIAC) to bring industry and government closer together [1, p. 36].

As the author of this article I have the following comments to the above mentioned quotations:

1. The third phase of CIP in USA after securing communication and establishing FEMA was homeland security, and its corollary, CIP, between 1993 and late 1995
2. The first publication to use the term "critical infrastructure" was the March report in 1996. It also had the first definition of infrastructure.
3. Infrastructure was defined as man-made. This excludes for example territory and rivers, which I consider infrastructures based on formal concept analysis made in this article.
4. There are old physical threats and new cyber threats in CIP. This is according to one effect of evolution: Nothing old disappears; they are just a part of the new.
5. CIP is owned mostly by private sector; hence Public-Private-Partnership (P3) is vital. This is interesting for Finland because we have a 60 years history of P3P meaning the predecessor of NESA (National Emergency Supply Agency), the PTS (PuolustusTaloudellinen Suunnittelukunta; Defence-Economical Planning Committee)[1].
6. Lewis does not use the obvious choice of formal concept analysis to analyse the meaning of origin, or critical or infrastructure or protection.

Lewis: CIP is recognized as being a core component

By Executive Order 13231 (October 2001) President Bush created the President's Critical Infrastructure Protection Board (PCIPB), with the primary responsibility to protect the information infrastructure of the federal government. Without information systems, the U.S. Federal Government could not continue to operate in the event of an attack. [1, p. 37]

In 2002 President Bush signed the Homeland Security Bill, establishing the new DHS. It began operation in February 2003 and incorporated 22 agencies that had been spread throughout the federal bureaucracy. Thus, protection of critical infrastructure is now the responsibility of the DHS [1, p. 38].

In December 2003, President Bush replaced PDD-63 with HSPD-7 (Homeland Security Presidential Directive #7), which rewrote the list of sectors and who is responsible [1, p. 38]

[1] PTS was established in 1955 (http://www.huoltovarmuus.fi/organisaatio/huoltovarmuuskeskus/lyhyt-historia/)

It appears that HSPD-7 was written to address in-fighting among departments and agencies that may have felt left out of the National Strategy [1, p. 38].

As the author of this article I have the following comments to the above mentioned quotations:

1. This US problem solving principle of putting existing organization together is interesting.
2. When something becomes important and gets new recourses, it will become a battlefield in politics.

Lewis: Analysis

CIP has grown to encompass most of the U.S. economy. It is difficult to identify sectors that are not critical. Indeed, CIP has come to embrace just about every aspect of society, from communications, power, and health care, to the food we eat, water we drink, and work we do. If CIP embraces nearly everything, perhaps it has lost its focus [1, p. 39].

The first objective of this Strategy is to identify and assure the protection of those assets, systems, and functions that we deem most ”critical” ... [1, p. 39]

Uncertainty remains at the national and local levels of government as to what is critical and what is not [1, p. 39].

President Bush signed HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection. At the time of this writing, HSPD-7 was the latest declaration by the federal government on CIP [1, p. 39].

For the first time, HSPD-7 declared that it is impractical to protect everything and focused effort on major incidents. [1, p. 39]

CIP has come of age. It is now at the core of homeland security. It has evolved over several decades and gone through several phases: (1) Recognition (The 1962 Cuban Missile Crises) (modern telecommunications technology), (2) Natural Disaster Recovery (FEMA starting from 1978→), (3) Definitional Phase (1997→), (4) Public-Private Cooperation (2004→) and (5) Federalism (2003→). [1, pp. 40 - 41]

As the author of this article I have the following comments to the above mentioned quotations:

1. In the 2000's the whole complexity of CIP is revealed. Modern technological society consists of many intertwined systems and it is difficult to say which part of the main system is more important than the other. This is also a central conclusion of National Emergency Supply Agency's two year project "SOPIVA"[2] (SOPImuksiin perustuva VArautuminen, Preparedness Based on Agreements) 2006 – 2007.
2. Centring ones protection of critical infrastructure is a good idea in principle. But it calls for prioritizing, which is not straightforward.

3 Formal concept analysis: Definition of key words

Formal concept analysis is the first tentative theory in this article. Because of the lenght of this article, the discussion of this tentative theory is quite basic.

About origin

The chapter of Lewis book under my scrutiny is entitled "Origin". Origin in the meaning we are interested in here[3] is connected to ancestry and parentage, for example history, passing of time. It means also rise, beginning, or derivation from a source. Origin is the point at which something begins or rises or from which it derives.[4]

> *So the origin of critical infrastructure protection is its ancestry and parentage, e.g. history or the rise, beginning, or derivation of it from its source. Origin of CIP is the point at which it begins or rises or from which it derives. Origin of CIP has "parents", pre-phases.*

[2] General information about SOPIVA – recommendation (some in English)
http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/sopiva/
Report of the 2nd part of the project (2007) (in Finnish): http://www.huoltovarmuus.fi/static/pdf/225.pdf
Report of the 1st part of the project (2006) (in Finnish): http://www.huoltovarmuus.fi/static/pdf/230.pdf

[3] Origin is also the more fixed, central, or larger attachment of a muscle and the intersection of coordinate axes (http://www.merriam-webster.com/dictionary/origin)

[4] http://www.merriam-webster.com/dictionary/origin

About critical

Critical in the meaning we are interested in here[5] means crucial, decisive and indispensable.[6]

We can live without bicycles or motorcycles, but not without some kind of transportation. We can live without bananas or oranges, but not very long without some kind of food. This means that, if needed, we can give away lots of thing but there is a gray limit that is not crossable. So critical means that in many cases there is something not-critical that we can live without, if we choose so.

The type of society is also important. One human of small group of humans can live without roads. But modern technological society cannot live without road. There is an analogous relationship with computer systems and post modern information society.

> *So critical in critical infrastructure protection means an infrastructure without which we cannot live (the life we want) and without which our systems will not function.*

About infrastructure

Infrastructure in the sense that we are interested in here[7] means the underlying foundation or basic framework of a system or an organization. Infrastructure as a word is very new. It was first used in 1927.[8]

Infra is Latin and means underneath, below. Structure means permanence of pattern, something that has some shape and the shape is permanent. So infrastructure is something underneath that has some shape and the shape is permanent. Adding to this foundation or basic framework we get:

> *Infrastructure is something underneath that has some shape and the shape is permanent and this infrastructure is a foundation to many things.*

[5] Critical is also relating to or being the stage of a disease at which an abrupt change for better or worse may be expected and : inclined to criticize severely and unfavorably or exercising or involving careful judgment or judicious evaluation (critical thinking) or including variant readings and scholarly emendations (a critical edition) or of sufficient size to sustain a chain reaction (a critical mass) or sustaining a nuclear chain reaction (the reactor went critical) (http://www.merriam-webster.com/dictionary/critical)

[6] http://www.merriam-webster.com/dictionary/critical

[7] Other uses are the permanent installations required for military purposes and the system of public works of a country, state, or region; also : the resources (as personnel, buildings, or equipment) required for an activity (http://www.merriam-webster.com/dictionary/infrastructure)

[8] http://www.merriam-webster.com/dictionary/infrastructure

According to this definition, what are infrastructures? Energy, banking and finance, transportation, vital human services, and telecommunications. Yes. Even critical. But there is no hint in this analyze to the word “man-made”. I will continue with this idea in the chapter “Evolution”.

Take for example transportation. It is not a 21st century invention. Rivers as transport system were very critical infrastructure for the first civilizations some 5000 years ago. These civilizations were river-based, for example in Egypt, China and India [5, p. 58 and 63].

It is also clear that communication *per se* is an infrastructure, a permanent shape that is foundation to many things. This means that language [6], writing [7] and printing[9] [8] are infrastructures.

About protection

Protection in the meaning that we are interested in here[10] means the act of protecting, the state of being protected, one that protects or supervision or support of one that is smaller and weaker.[11]

> *So the protection in critical infrastructure protection means the act of protection or the state of being protected.*

Protected against what? Against an attack, extreme weather condition, misuse, bad design, its own complexity, foreign influence (language). In military this is called defense.

About origin of critical infrastructure protection

According to the short formal concept analysis made in this article, the origin of critical infrastructure protection was:

> *the birth of protection of something underneath that has some shape and the shape is permanent and this something is a foundation to many things and without which we cannot live (the life we want to live) and without which our systems will not function.*

[9] Professor Bosse Sundin calls printing ”The Greatest Invention of All Times”. (http://koivu.oulu.fi/~histwww/aoh/6.htm) (in Finnish)

[10] Protection means also a contraceptive device (as a condom) or : the freeing of the producers of a country from foreign competition in their home market by restrictions (as high duties) on foreign competitive goods or anchoring equipment placed in cracks for safety while rock climbing or immunity from prosecution purchased by criminals through bribery or money extorted by racketeers posing as a protective association (http://www.merriam-webster.com/dictionary/origin)

[11] http://www.merriam-webster.com/dictionary/origin

One such critical infrastructure was and is one's territory. At the very beginning it was a piece of land under one's or one's clan's foots. It contains everything one's clan needed, for example water sources, games[12], trees to collect fruits, caves to sleep, plants to use as a drugs and stones to build weapons. It was also one of the oldest reasons for war (defense, protection!) already in the prehistory of mankind [9, pp. 23, 37] and still is.

So the origin of critical infrastructure protection is quite far away in the history, when analyzed this way. It started with the protection of one's territory. The word "infrastructure" itself is just some 80 years old.

4 Evolution

The word "origin" hints quite directly to evolution. Evolution is the second tentative theory in this article. Because of the lenght of this article, the discussion of this tentative theory is quite basic.

Evolution as a whole

The great idea of evolution is based on the notion of time and change of system states. In biology the latter is called variation. All things have history and pre-phases, maybe excluding Big Bang. All systems also change, maybe excluding stable atoms and their parts (proton) [10, pp. 332 - 4].

This is well presented in professor Eero Paloheimo's book "Megaevoluutio" (Megaevolution), which starts from Big Bang and processes through time having following states or systems that build up each other: quarks (and electron), subatomic particles, light atoms, stars and supernovas, heavy atoms, living cell (life), multicellular organs, man and his organization and technology [11].

Evolution of man

Man has always been living in groups and had societies and this has shaped his brains considerably [12, p. 29 and 34]. In the long history of mankind there have been the following organizations and phases: clan (animal, before 50,000 BC), tribe (primitive, after 50,000 BC), state (historical, after 3000 BC), culture[13] (modern, after 1500 AD) and global mankind (postmodern, 2000 AD) [5], [9, pp. 29 - 33 and 37], [13].

[12] Ref. Killing of the buffalos in USA in the 1870's to fight the plain Indians
[13] Cultures of technology and science meaning Western, Arabic, Chinese, …

All great communication revolutions in the evolution of mankind have also been revolutions in the infrastructure, because information is a very basic necessity to many, if not all human activities. These communication revolutions have been birth of language, invention of writing, printing and global computer technology [14].

The birth of modern language some 50,000 years ago was a great leap forward in the human evolution. With modern language came new rapidly advancing stone technology, art and first commerce [6, pp. 58 - 60]. The last can be seen as a new kind of infrastructure that made precious items like stone weapons, ideas and luxury items to flow.

First great civilizations emerge from great rivers [15, p. 74], because rivers are not just water sources for drinking and fishing, but also irrigation systems for agriculture and very efficient transport system, therefore infrastructures.

Evolution of technology

Also technology has advanced in phases that are building up each other. These have been tools, machines, systems and systems of systems [16]. Internet is a fine example of the last ones.

Before aircraft, ballistic missiles and internet there was no other way to attack critical infrastructure of the enemy (state) than to move an army to the target area. In the era of precision guided weapons, especially cheap JDAM-type weapons and Stuxnet-type more expensive weapons, hitting hubs of critical infrastructure became easy.

For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict. [17, p. 796]

This is why cyber is so important in our time and even more important in the future. It means also that cyber meaning computer based information systems is a new kind of critical infrastructure of information.

Conclusions from evolution

The origin of critical infrastructure protection is quite far away in the evolution, as analyzed in this article.

Now we have an evolutionary timeline of scientific critical infrastructure protection:

1. critical basic infrastructure (territory, always with life)
2. the birth of modern language (some 50,000 years ago)
3. commerce as a new networking application and an infrastructure (some 50,000 years ago)
4. the invention of writing (some 5000 years ago)
5. first applied critical infrastructure (rivers, some 5000 years ago) and then others like basic roads, harbors, cities, …
6. the invention printing (500 years ago)
7. critical scientific-technological infrastructure (steam, petrol, electrical power; roads, railroads, harbors, airports, …) (some 150 years ago)
8. critical scientific-electronic information infrastructure (telegraph and telephone systems and computers (some 150 years ago)
9. the introduction of the word “infrastructure” (1927)
10. the introduction of the term “critical infrastructure protection” (1997) [1, p. 2]
11. the birth of global computer infrastructure, for example internet (some 20 years ago)
12. science of critical infrastructure protection (Lewis [1, p. vii]) (about 10 years ago)

5 Information processing

As mentioned earlier, Lewis does not use the obvious choice of formal concept analysis to analyse the meaning of origin, critical, infrastructure or protection. The use of formal concept analysis was found out to be productive in this article. It widened the history of origin of critical infrastructure protection. This wider interpretation considers territory and rivers as infrastructures.

The great idea of evolution is the notion of time, history or pre-state for a latter state. For CIP this means that it had some pre-phase or birth, before becoming CIP.

Starting points, the tentative theories, should according to Popper, give rise to the deepest and most unexpected problems and of course solve the problem well [2, pp. 287 - 8]. It is interesting that Popper does not produce any list of such theories. One view of what these theories could be is presented for example in

Peter Atkin’s book “Galileo’s Finger – The Great Ideas of Science”. These “ideas” are evolution, DNA, energy, entropy, atoms, symmetry, quanta, cosmology, spacetime and arithmetic [4]. Finnish physicist and professor Kari Enqvist lists three great ideas of physical science: energy, entropy and emergence [19, p. 7].

I have used General Systems Theory [20] in recent years [3], [14] as a “great idea”. It is very much connected in the above lists to evolution, DNA and emergence. I would personally list General Systems Theory and its applications e.g. cybernetics to the list of great ideas.

6 Conclusion

Conclusions about the chapter “Origin”

The research question of this article was to answer the following question: What is the origin of critical infrastructure protection based on (1) professor Ted G Lewis’s course book, (2) formal concept analysis and (3) evolution?

The answers are: (1) According to professor Ted G Lewis, the origin of critical infrastructure protection (in USA) was the creation of the National Communications System (NCS) in 1963 after communication problems between the United States and the Soviet Union during the Cuban missile crises in 1962. [1, p. 40]

(2) According to the formal concept analysis made in this article, the origin of critical infrastructure protection was the birth of protection of something underneath that has some shape and the shape is permanent and this something is a foundation to many things and without which we cannot live and without which our systems will not function. First this kind of infrastructure found in the article was territory.

(3) According to evolution, the origin of critical infrastructure protection has a long history and over ten principal phases from physical infrastructures to social infrastructures to technological infrastructures and lastly to information technological infrastructures (cyber). Revolutions in the communication technology of mankind have also been always revolutions in the critical infrastructure of mankind.

Conclusions for the Finnish CIP

The origin of CIP (in USA) was the communication needs for US Government in time of global crises [1, p. 30]. This is interesting for Finnish emergency work or emergency work in general: the first item needed in times of crises is communication capacity.[14]

Prioritizing is a problem in Finland as a part of CIP[15]. It is interesting that it grow up as a problem also in the birth of US CIP history. The importance of prioritizing can be noticed from the fact that later on it was as a word in the title in one of the presidential orders in USA.

The other interesting point regarding the president of USA is his many advice organs. Is this an application to use also in Finland?

Public-Private-Partnership also grow up to an item in 1990's in the USA CIP history. In Finland we have used this idea in CIP protection for at least 60 years.

7 Discussion

More information processing on this subject, meaning critical thinking and error elimination is needed, like always, to have better science. It is still presented in the article, that extra theories, even if presented shortly, give always extra insight. This confirms Popper's idea of evolutionary induction.

As a very new theory of CIP, Lewis's book is not widely used and widely tested theory, although used and tested as presented within the book. Still I did not find anything to correct, but that is not a big statement, because the chapter under my scrutiny was not the heart of Lewis's theory.

In this article formal concept analysis did give a more theoretical notion of CIP, not just list of things that are in the public or in documents of US Government nowadays considered to be part of CIP. The integrated concept presented in this article can be used to determine what CIP is and what is not. This is not done in this version of the article.

The idea of evolution proved to be effective, ones again. Now we have in this article a bit longer history of CIP and its pre-phases.

[14] Ref. In Finland government's Tetra based Virve mobile network from 1990's and the new 2010's government's TUVE – security communication network.

[15] There have been seven regional exercises in Finland 2008 – 2012 that were focused on co-operation of telecommunication, power supply and contractor firms. One of six major problems found in the series of these exercises was the priorization in case of bigger emergencies.

As modern experimental and mathematical science was born in the Renaissance, it is probable that critical infrastructure protection has its scientific “parentage” in that period.

It is presented in the article that commerce was a new networking application and an infrastructure introduced some 50,000 years ago. This is at least the time to go back if we want to be really independent and in no contact with other far away people.

It was noticed in the process of writing this article, that Popper’s evolutive induction, used as a basic analyzing tool in this article, is actually a cybernetic, information processing process. This confirms both cybernetics [21] and Popper’s evolutive induction according to best practises of Popper’s evolutive induction!

8 New problems

The use of Popper’s evolutive induction requires that one has deep theories as a starting point. It is interesting that Popper does not provide such a list in his book. Some starting points are discussed in the article for these theories.

The phases that Lewis presents as the history of CIP were importance of communication systems, protection for natural disasters, birth of homeland security and the notion of CIP, definition of CIP, Public-Private-Partnership, prioritization, and federalism. Is there something evolutionary in these phases?

Prioritization in CIP and emergency situations is a major problem. Lewis solves this for CIP in his book by the network analyze, but is it also a solution for emergency situations?

References

[1] T. G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Kindle Edition ed., Hoboken, New Jersey: John Wiley & Son Inc., 2006.

[2] K. R. Popper, Objective Knowledge - An Evolutionary Approach, Clarendon Press Oxford, 1979 (Revised).

[3] S. Ahvenainen, “What Can We Say About Cyberwar Based on Cybernetics,” in *The Fog of Cyber Defense*, Tampere, Juvenes Print Oy, 2013, pp. 154 - 168.

[4] N. Wiener, Cybernetics: or Control and Communication in the Animal and the Machine, 10 (1. painos 1948) ed., Cambridge (USA): The MIT Press, 2000 (alunperin 1948).

[5] A. M. Taylor, “Some Political Implications of the Forrester World System Model,” in *World System – Models – Norms – Variations. International Library of Systems Theory and Philosophy*, New York, Braziller, 1973, pp. 29 - 68.

[6] R. K. Logan, The Extended Mind: The Emergence of Language, the Human Mind and Culture, University of Toronto Press, 2007.

[7] D. Schamandt-Basserat, How Writing Came About, Austin: University of Texas press, 2006.

[8] B. Sundin, “Teknologia ja ihminen - Historiallinen katsaus,” [Online]. Available: http://koivu.oulu.fi/~histwww/aoh/sundin.htm. [Accessed 19 Huhti 2013].

[9] Q. Wright, *A Study of War*, Midway Reprint ed., The University of Chicago Press, 1983.

[10] K. Enqvist, Monimutkaisuus – Elävän olemassaolomme perusta, WSOY, 2007.

[11] E. Paloheimo, Megaevoluutio, WSOY, 2002.

[12] F. Fukuyama, The Origin of Political Order - From Prehuman Times to the French Revolution, Kindle 2011 ed., New York: Ferrar Straus and Giroux, 2011.

[13] T. E. Currie, S. J. Greenhill, R. D. Gray, T. Hasegawa and R. Mace, “Rise and fall of political complexity in the island South-East Asia and Pacific,” *Nature,* pp. 801 - 804, 14 Lokakuu 2010.

[14] S. Ahvenainen, “Informaatioteknologia ja ihmiskunta - systeeminen ja evolutiivinen tarkastelu,” in *Informaatioteknologian filosofia*, Rovaniemi, Lapin Yliopistokustannus, 2011, pp. 113 - 138.

[15] W. H. McNeill and R. J. McNeill, Verkottunut ihmiskunta – Yleiskatsaus maailmanhistoriaan, Vastapaino, 2006.

[16] M. v. Creveld, Technology and Warfare, New York: The Free Press, 1991.

[17] M. Warner, “Cybersecurity - A Pre-history,” *Intelligence and National Security*, vol. 27, no. 5, pp. 781 - 799, 5 Lokakuu 2012.

[18] P. Atkins, Galileo's Finger- Ten Great Ideas of Science, New York: Oxford University Press, 2003.

[19] L. Bertalanffy, General Systems Theory – Foundations, Development, Applications, New York: George Braziller, 2003 (alunperin 1968).

[20] V. F. Turchin, The Phenomenon of Science - a cybernetic approach to human evolution, Abobe Reader, pdf ed., New York: Principia Cybernetica Project, 1977.

[21] Q. Wright, A Study of War, The University of Chicago Press, 1942.

[22] A. Roland, “Technology and War,” 1997. [Online]. Available: http://www.unc.edu/depts/diplomat/AD_Issues/amdipl_4/roland.html. [Accessed 12 Kesäkuu 2010].

[23] R. P. Feynman, Six Easy Pieces - Essentials of Physics Explained by Its Most Brilliant Teacher, Basic Books, 1995.

Wargaming Cyberwar in Network-Centric Critical Infrastructure Defence

Heikki Lantto
Finnish National Defence University
heikki.lantto@mil.fi

Abstract

Purpose and approach

The role of critical infrastructure protection in the information society has increased steadily. Critical infrastructure systems have increased their dependence on information systems and communication networks. Critical infrastructure systems are built on a complex and interdependent networks and nation security and defence are based on society critical infrastructure. Cyberwar against nations critical infrastructure currently represents a major threat to national security.

The national security authorities make plans and prepare to fight against cyberwar attacks. A great challenge is to make defence plans and preparations in this complex field of cyberwar threats. And the challenge is even greater because the responsibilities and the mandates are split between various authorities. Wargaming can be used as a tool to gain insight, experiences, and to find in advance potential problems of cyberwar element in critical infrastructure defence. The purpose of this article is to analyse cyberwar capabilities from a wargaming point of view, focusing on network-centric critical infrastructure defence. The aim is to find out how cyberwar elements can be used in wargaming of critical infrastructure defence.

Cyberwar is approached in this article from the perspective of wargaming and analysing of cyberwar impact on the ways of assimilating them to the traditional means of influencing in wargaming. The article is based on literature study.

Findings and orginality

Cyberwar components can be a part of impact categories of wargaming, but it should be taken into account already in the design of the wargame. The cyberwar components in wargames that are dealing with the critical infrastructure in network-centric defence can be used to create estimates on the impact of the cyberwar components in critical infrastructure defence.

The article content consists of well-known cyberwar capabilities that are examined from wargaming perspective. The article outlines cyberwar capabilities from a perspective not so common. The article can be used as a basis for a more detailed examination on the effects that cyberwar brings to the traditional wargaming.

Keywords

Wargame, Wargaming, Cyberwar, Cyber Defence, Critical Infrastructure

1 Introduction

The protection of national critical infrastructures has gained a central role in western emergency planning because new asymmetric security threats have evolved to information based societies. Information technology has brought new ways to manage critical infrastructures but has also created new ways to affect warfare and terrorism. The benefits of information technology are vast and nowadays there are not many critical infrastructure services that could cope without information systems and communication networks. The different parts of national critical infrastructures are interdependent and create complicated chains of dependence. [1; 2; 3]

An infrastructure is considered critical when it is vital to national security. A critical infrastructure is that part of nations infrastructure that it’s incapacity or destruction would have a debilitating impact on a nation defence and national security. Critical infrastructure defence is to protect, prevent, and respond to attacks on critical infrastructure. [1]

Cyber defence means actions combining information assurance, computer network defence (including response actions), and critical infrastructure protection with enabling capabilities to prevent, detect, and ultimately respond to an adversary’s ability to deny or manipulate information and/or infrastructure [4]. Cyberwar attacks are becoming more frequent and more organized. The damage they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure are more costly. They can reach a threshold that threatens national security and stability. Foreign militaries and intelligence services, organized criminals, terrorist and/or extremist groups can each be a source of such attacks. [5]

A great challenge is make defence plans and preparations in these very complex systems to prevent cyberwar attacks. And the challenge is even greater because the responsibilities and the mandates are split between various authorities. Wargaming can be used as a tool to gain insight, experiences, and to find potential problems in advance of cyberwar element in critical infrastructure defence.

Geographically dispersed forces maintaining a high level of situational awareness characterize network-centric warfare, allowing increased combat effectiveness [6]. Network-centric warfare is a military doctrine that seeks to translate an information advantage, enabled in part by information technology; into a competitive warfighting advantage through the robust networking of well informed geographically dispersed forces [7]. Network-centric warfare, cyber defence and critical infrastructure together form a very hard-modelled environment, which is very challenging to perceive a whole.

Wargaming can be used to many purposes, for training, education, research and analysis, and discovery. Wargaming can be used to discover some previously unknown problems from highly complex situation, like critical infrastructure defence in network-centric warfare. Other discovery methods, like modelling and simulation or operations research, with the same resources (money, time, etc) are not adequate. In critical infrastructure defence in network-centric warfare wargaming is used to find problems in defence plans, preparations, and mandates. Wargaming can also be used to training purposes. [8; 9]

2 Research work

2.1 Critical infrastructure defence

Critical infrastructure networks are key targets for cyberwar. Networks have grown to the point where they run the command and control systems, manage to logistics, enable the staff planning and operations, and are the backbone of the intelligence capabilities. [10]

Critical infrastructure defence’s definition in Finland is: “The overall objective is the safety of the population and the basic functions of the sufficient supply to maintain. Security of supply is dimensioned so that the livelihood of the population, society functions necessary for the defence and material conditions are not compromised.” [11; 12]

Critical infrastructure in Finland is [11]:

1) Society technical infrastructure, which includes energy networks, telecommunication networks, the key information systems, mass communications, financial services, payment transactions, and cash management, information technology maintenance, water supply, and the other main civil engineering basic services.
2) Transport, storage, and distribution systems, which include maritime transport, basic food and energy transportations, ice-strengthened vessels, air transportation, and the main logistic chains.
3) Food supply, which includes intended for human consumption of cereals, protein, seed grain, and clean water.
4) Security of energy supply, which includes heat and power production, fuels, distribution and transmission networks, and imported fuels.
5) Health and social care, which includes pharmaceutical, medical and vaccine maintenance, equipment, and its maintenance and spare parts.
6) National defence supporting production and system maintenance, which includes defence equipment industry, technically sophisticated weapons system maintenance and repair, ammunition maintenance, building capacity, research and development, and international compatibility.

All infrastructure, production and management are dependent on information systems and communication networks, which form a complex network. It is possible that the problems can switch from one system to another, and can cause cumulative risks. The complexity of systems lays high demands to the operative staff.

To defence critical infrastructure it must be determined which functions are essential to the nation, and which infrastructure systems are essential to the functioning of these. Then there must be identified the critical parts and components of various infrastructure systems that are critical to the functioning of the systems individually and with each other. It must be examined the critical points and components relationships with each other, and on this basis the critical points are sorted to an order of importance. There may be the problem that there are so many critical points. When the infrastructure develops, the critical points are increasing and changing so rapidly, that it is not possible to make complete list. On the other hand interdependencies are impossible to determine without knowing the critical points. [2]

In the defence of critical infrastructure individuals and their professionalism plays an important role, concerning both the leaders and the experts. Individual’s know-how development and emergency planning and preparation form a bases to critical infrastructure defence.

Surveillance plays important role of critical infrastructure defence. If is possible to monitoring on the various means of communications moving area of interest, it can give a warning when coordinated activities, such as attacks may be taking place in the immediate future. When designing the wargame, there need to think every operator and/or system capability to reconnoitre and to surveillance.

2.2 Military wargaming

"The general who wins a battle makes many calculations in his temple before the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat; how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose."
Sun Tzu, "The Art of War"

Wargame is a simulation, by whatever means, of a military operation involving two or more opposing forces using rules, data, and procedures designed to depict an actual or assumed real life situation. [13; 14; 15] Military wargaming in Finland is understood as a part of a military exercise, a part of the planning process, or as training for military simulators and games [16]. Wargaming can also be used as a tool to analyze own operational possibilities [17]. A wargame is a warfare model or simulation in which the flow of events is shaped by decisions made by human players representing the opposing sides, during the course of those events. [8]

Typically in wargames there are used a game board or map, where the counters are placed and moved as the game progresses. The counters are describe units or others entities whose activities are played. Typically wargame is executed in steps. The execution of wargame starts with an introduction to a situation. Then every step is carried out in sequences consisting of cycles with the move of action, reaction, and counteraction. The execution is a strict, disciplined process with explicitly defined functions and rules for usage. When all steps have been run through, the execution of wargame is over. [17]

In a military exercise wargaming is used to create events and to plays the troops, which are not on the battlefield [16]. Full-scale war exercises in large scale, that involve all the potential actors, sets, and systems are very expensive. Wargaming is also used to create events and resolve battle situations what normally cannot be done; for example, the weapons effect simulation on the troops. Cyberwar effects are described to the forces same manner that traditional wargaming effects in a military exercise wargaming.

As a discovery tool wargame provides a systematic method to analyze many varied factors. It forces decisions to be made, and permits the interactions and relationships among the factors to appear in concrete form. [18] The discovery wargaming is especially useful when examining a new type of troops and / or equipment. In this case, there can be obtained from observations of the things, which usually can be observed only in the first field trials.

In the planning process and the training wargaming is a way to simulate battles or events according to the rules. The scale of wargaming and modeling accuracy varies. By roughly divided there are four different formats of wargaming in Finland [16]:

1) the map exercise,
2) the wargame,
3) the computer simulation and,
4) the analytical model.

In a map exercise the simulation accuracy is typically the least accurate. Usually the events, the battles and, their consequences will be determined by the debate of experts in front of the map. [8; 19; 20] In many cases, map exercises will cover the pre-prepared situations in which experts form a coherent opinion.

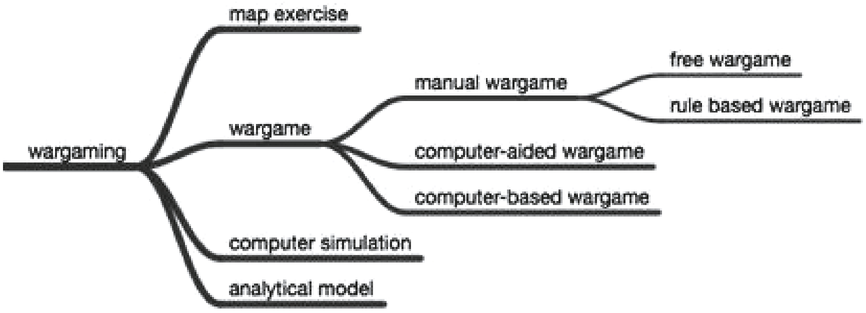


Figure 1. Military wargaming formats in Finland

The most accurate simulation, the analytical model, aims to analyze the fight mathematically [21]. From the wargaming point of view, the analytical model is designed to eliminate the human variable from the battle. In playing wargames, decisions made by man plays an important role and bring human factor into a battle. [8; 22]

The wargame format can be divided in three different categories depending on how they use computer technology [8]:

1) the manual wargame,
2) the computer-aided wargame and,
3) the computer-based wargame.

The manual wargame can be divided in two categories depending on how rules are used for determine the outcomes of events and battles: the free wargame and, the rule based wargame. In a free wargame the umpire define the battlefield events and the consequences of the events and the battles, on the basis of experience and professional skills. In the rule-based wargame the rules of the game determine the consequences of the events and the battles. [17; 19; 23]

The computer-aided wargames are more sophisticated versions of the manual wargames. They use information technology to help game managers or the umpire to manage the wargame. The computer assigns to determine the outcomes of the events and the battles. That is to allow the use of more complex rules than in a manual wargame. In a computer-aided wargame there can also be a partially computerized opponent. [8; 17]

The computer-based wargames are playable on the computer. There is the battlefield in the computer game and the needed troops and actors are modeled in the computer. The wargame software in the computer runs the events and the battles and solves the consequences by the programmed rules. The game managers do not usually have the opportunity to influence on the consequences of the events and the battles of the game, only the wargame players activity influences. [8]

The computer simulations are simulating a battlefield as accurately as possible. The computer simulation has often opponents modeled in artificial intelligence. In most of the cases, the computer simulation is used to simulate individually every soldiers or small military forces activities. [21] The most commonly used military simulators in Finland are flight simulators and Virtual Battlespace 2 (VBS2).

The discovery by wargaming starts by setting a research question to determine what is being studied. The research question is analysed in order to determine the criteria for wargaming. The criteria will determine the place (the battlefield) and the time where the wargaming scenario takes place and what kinds of forces are used and what is the initial situation. This forms the base of the wargaming scenario, which may have a number of options to play. In addition, the analysis of the research question determines resolution of the wargaming to the wargame model and to player’s necessary instructions to play the wargame. [17; 19; 20]

The players of the wargame are playing one or more wargames to get an insight of the research question. By the activities of the players in wargame events, accumulates material to be analysed in two ways: subjective observations and mathematical analysis. The players and the observers of the wargame make subjective observations on the events and the battles in the wargame. The wargame model (in the computer-assisted, the computer-based, and the computer simulations) performs calculations and this data can be analysed by using mathematical analysis methods. [20; 24]

Situation at the end of the wargame / wargames, as well as the subjective findings of the events and the battles and the mathematical analyses can be used to make estimates of the effectiveness of different things and to give estimates considering the research question. The wargame / wargames are mostly unique and are usually not reproducible in the quantities needed for scientific certainty. [8; 20; 24]

The findings of the wargaming need to be examined more detailed by analytical methods and by simulations of the component parts, as well as by literature review to achieve scientifically sound conclusions. The main findings of the wargaming seem to be subjective findings of the wargame events and battles. [20]

The biggest challenge in design the wargame is to find the right balance of detail and smoothness of the game progress. One example is an unprecedentedly detailed military simulation game of the North Africa Campaign of World War II, The Campaign for North Africa. According to game manufacturer (Simulations Publications, Inc) a complete game can run over 1500 hours. The rules cover logistic in extreme detail. [25]

2.3 Cyberwar and cyber defence in wargaming

Cyberwar means the use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems [15]. Cyberwar is digital means to conduct espionage, damage information systems, make financial damage, and manipulate national critical infrastructures. Cyberwar is used in conflicts between governments, between citizens, and between government and civilian society. [26]

From wargaming point of view cyberwar is not a separate way to influence, it is related to real-world real objectives. To understand the impact of intermodulation of real-word and cyberwar is the key to bring cyberwar into military wargaming as a way to impact. The most important thing is to find out how the cyberspace related issues affect real-world functions and how the functions of the real-world impact in cyberspace. The cyberwar is either the cyberwar as a weapon in wargaming or wargame is focusing only on cyberwar methods in cyberspace. [26; 27]

Cyber defence is the military aspect to cyber security. Some sources define cyber defence as defensive function and the protection of information system, but in Finland the term cyber defence is referred to a way that includes all military actions taken to protect, attack, or exploit our own or adversaries information and computer systems. [28]

Cyber defence as part of the wargaming can be looked from two different points of views, a defence and a threat perspective. [1; 5; 26; 29; 30]

Looking from the defence point of view the cyber defence is divisible into two parts, a technical and a method of operation. The technical cyber defence capabilities include, for example, access control to information networks, antivirus software, firewalls and encryption applications. For example, these technical features can give the goodness values that can be used to evaluate the influence of attacks during the wargaming. The methods of operation cyber defence capabilities includes, for example, how people are trained, how they have been practicing and how disciplined they are to follow protocols. During the creation of a wargame scenario, these capabilities can be estimated, for example, how the attacks affect the operation or how quickly after the attack can the defender recover. [1; 5; 26; 29; 30]

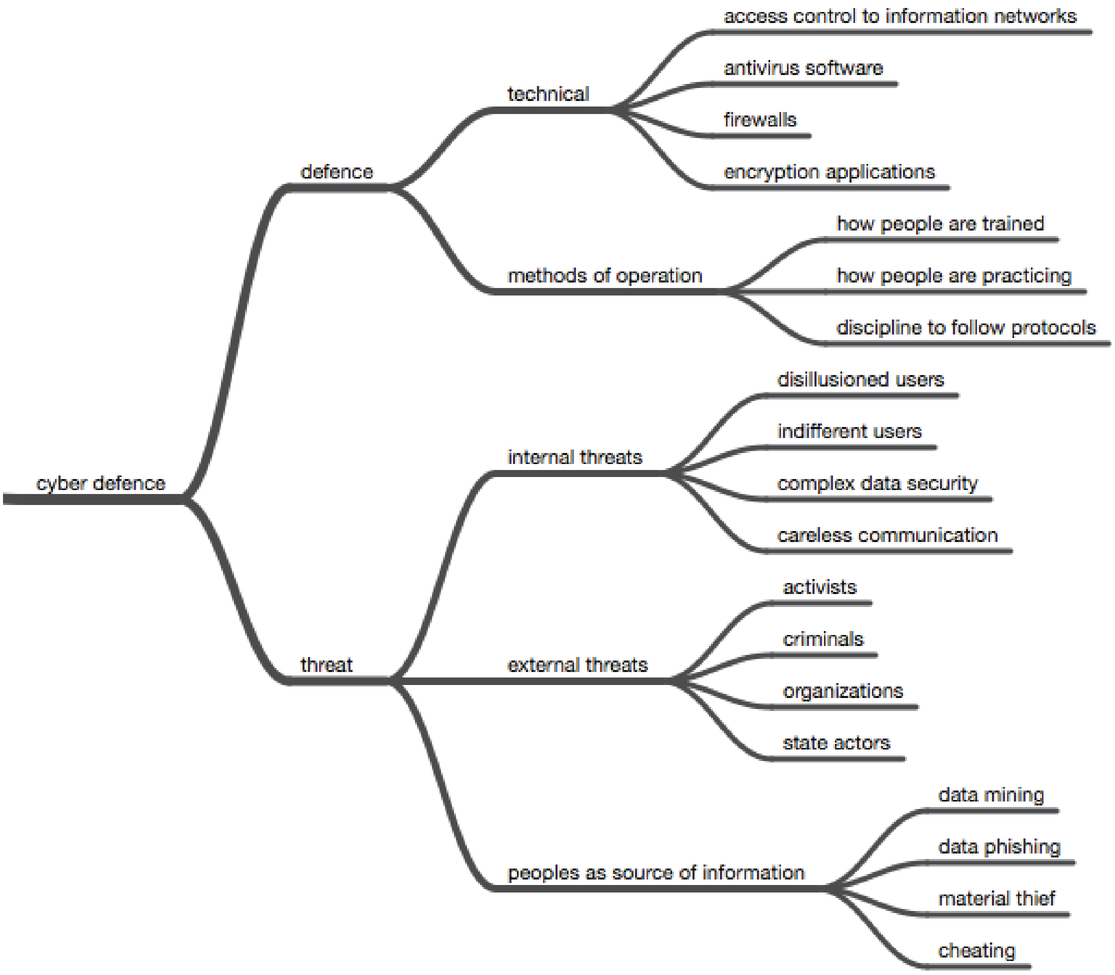


Figure 2. Cyber defence perspectives from wargaming point of view

Looking from the threat point of view the cyber defence is divisible into three areas, internal threats, external threats and people as sources of information. The internal threats are, for example, disillusioned users, indifferent users, the complex data security and the careless communication. Most of the internal treats form for the attacker a way to get information, which can be used to carry out attacks against systems. To wargaming there should be established as accurate, truthful and realistic picture of internal threats, without a cover-up. The external threat includes, for example, activists, criminals and organizations as well as state actors. To wargaming cyber defence, the external threats represent a potential attacker. People as sources of information, includes, for example, data mining, data phishing, material theft and cheating. [1; 5; 26; 29; 30]

The wargaming can be used in cyber defence for three main purposes, training, planning, and discovery. [1; 5; 26; 29; 30]

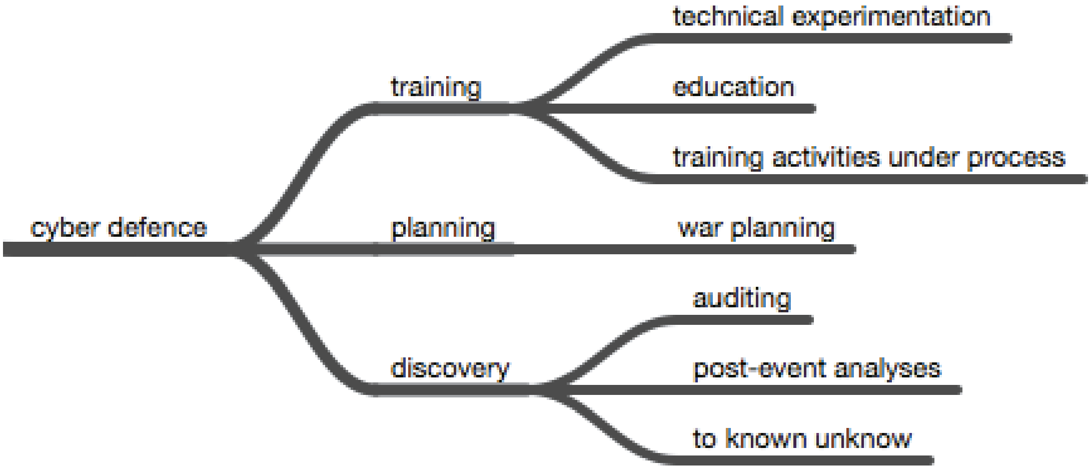


Figure 3. Cyber defence purpose from wargaming point of view

The training includes, for example, a technical experimentation, education and training activities under process. The planning includes a war planning. In the war planning a wargaming is regularly used in part of a planning process, mostly to develop, compare, and improve courses of action. [17]

The discovery includes, for example, an auditing, post-event analysis, and to be able to know the unknown. The audit may wargaming to assess the functionality of a system or a process in relation to the threats, in order to create a complete picture of the activities, including people, systems and guidelines. By wargaming the event there can be made an estimate on those parts of the event that have been left to the shadows. The estimate can consider the possible background to the event, how the event should be resolved, how the responsibilities should be divided into resolving the event, and how to prevent in advance the event from happening again. By using a wargame with cyberwar elements it is maybe possible to find out something what is not know about, to known the unknown. [1; 5; 26; 29; 30]

2.4 Differences to traditional wargaming

Cyberwar as a part of wargaming brings a slightly different functional component to wargaming. The time of the effect is extremely faster related to traditional wargaming components. Attacking and defensive measures can be seconds or even faster.

The actors in cyberwar are more varied. The target can't be sure who or which organization is behind the attack, or activities. The most common types of operator categories are cyber crime, activists, government and agencies, terrorists and individual people. In addition, the motives of the action or the objectives of the action are also very challenging to figure out. Operation of the source and motives can be, and usually are, masked so that is not possible to directly prove who did what. [26; 7] In a traditional wargaming out very clearly indicate who was attacker.

The cyberwar battlefield can be global. Information networks are globally linked in some way to each other, so the operators do not necessarily work in the same battlefield as the traditional wargaming components. [27] In a traditional wargaming on the map are described in unit's locations, where they physically are. Information systems networks and devices can be placed on the same map as the units. In the addition to the physical location of the networks they form a logical networks that are required to describe their own maps.

In cyberwar the intelligence (surveillance, reconnaissance, etc.) is more meaningful compared to conventional warfare. Intelligence must be more detailed and must influence the chains of inquire fully to the end, so the effect can be obtained. Validity of intelligence information measured in time can be very short because of changes in systems and networks or systems have already to been inquired years in advance if any changes have not been done to the systems. [27] For example, if the attack is directed against the data, there maybe need to reconnaissance the network level, the host level, the application level, access controls at the application level, and encryption at the data level [10].

The legal status of the operator and the target axes will be considered challenging. The battlefield is global and the attacker is very challenging to comply with all relevant laws along the way. Compliance with the law can set actors in very unequal positions.

One impact of a successful attack may be substantially higher than the kinetic weapons carried. About the number of attack weapons is not possible to draw any conclusions on the effectiveness of the attack. On the other hand, attacker must wait to see real-world effects actually occur [26].

The performances of cyberwar weapons are more clandestine than the kinetic weapons systems. The possible existence and effects of cyberwar weapons can only be estimated. There may exist advanced operators with unforeseen weapons and systems, and the effects can be very imaginative.

2.5 Cyberwar as a means of effect in wargames

Cyberwar in wargames focuses on the attackers affect on the defenders systems. It can be viewed in either the attacker or defender point of view. In attacker point of view, there are two main questions: where to impact or how to impact. In defender point of view, the main question is what the target can do.

Looking at the objectives of the attacker cyberwar, there are seven main categories against what the attacker can attack [26; 32]:

1) defenders ability to carry out missions,
2) defender systems capacity,
3) defenders capability to reach their goals,
4) defenders capability to obtain information from phase of the their missions,
5) defenders capability to obtain information from the effects of their missions,
6) defenders capability to obtain information which forces are usable, and
7) defenders capability to obtain information how their forces are usable.

The attackers ways to affect the defender can be divided into six main categories [26; 30]:

1) degradation of defender’s systems,
2) interruption of defender’s systems,
3) modification of information inside of defender’s systems,
4) fabrication of false information to defender’s systems,
5) unauthorization use of defender’s systems and
6) interception of defender’s information.

The categories of impact can be subdivided to properties against which the attacker wants to impact [29; 31]:

1) Communications networks, for example attacks against network infrastructure or network services (denial of service).
2) Hardware systems. The attacker can imbues backdoor to hardware, attack against virtualization software or cloud services.
3) Weak or embedded systems, for example sensors, RFID, mobile devices and TVs.
4) Complex systems, against which the threat can be divided into, for example, unforeseen knock-on effect, system manageability and verification, hidden characters or the parallelization.

5) Data manipulations, for example, privacy and everyday life, the forged sensors data and threat to social networks.
6) The human factors, for example, user interfaces, an insider threats, targeted attacks, phishing communication, new ways and opportunities to influence people, and safety-critical systems security is more important than data security.
7) Processes. Insufficient safety requirements or practices in information security can be divided into, for example, information security that is added to the system after the system design, old systems security update, All-IP networks and use of COTS components (other system found in the exploration of this vulnerability in other systems using the same component).

Under the attack the defender has, as a general rule, four ways to react [32]:

1) to continue the activity and use the system under the attack,
2) to continue the activity and no use the system under the attack,
3) to wait and to continue the activity when the system is again usable, or
4) to stop the activity.

Wargame design should create numeric values for each of the different way to attack and to defend. It depends on the accuracy of modelling, for example, is every hacker, hacker group, or hacking performance have values. Due to the nature of the cyberwar there cannot be a single value to describe the attacking or defending power, but each assessment should be made of the matrix format, which assesses the ability to attack each target or defend against each attack. There need to define to the attacker's ability to attack and at least the attacker's ability to reconnoitre, to remain secret, and hide tracks. To the defender there must specify at least the ability to reconnoitre, to detect attacks, to investigate events, and to make counterattacks.

Attack values	Hacker A	Hacker B	Worm A	Criminal 1
Server A	3	9	1	8
Firewall A	7	1	0	2
Scada W	10	4	0	0
Webserver 1	2	9	13	12

Table 1. Example matrix from attacking values

In addition, there should be determine what kind of means of attacking and defending is possible to carry out. For example, the attack against SCADA system, the attacker must have known vulnerabilities, which make use of or access to the system. After successfully attack or defence operation there should be determined how is affected to target. There can use, for example, one or more earlier mentioned six ways to affect, degradation, interruption, modification, fabrication, unauthorization use, or interception.

The resolution of details must pay attention, that the wargame should be playable. If played in the system protect against attacks, there can go the precision of the individual vulnerabilities. Looking at the defence of critical infrastructures, the accuracy should not to go capabilities of every person or computer, if there is not computerized system to helping game managers to simulate events.

3 Conclusion

Wargaming can be obtained by the perceptions and experiences of network-centric warfare as part of the critical infrastructure defence. It facilitates planning and preparedness as well as allows participants of the wargame to experience accumulation of difficult characters on the network-centric warfare. In addition, the wargaming teaches the participants the importance of critical infrastructure.

Wargaming cyberwar concerning critical infrastructure defence forces the participants continually to checking the credibility and feasibility of their decisions and actions taken, and what information was needed to make the decisions. Wargames offer a safe, implicit reflection of some of the situational and decision dynamics associated with cyberwar. A proper opponent generates and action and reaction feedback loop that produces insights much more powerful than a single opinion, however well informed.

The cyberwar components in wargames, that dealing with the critical infrastructure in network-centric defence, can be used to create estimates on the impact of the cyberwar components in critical infrastructure defence. Wargaming can be used to threat analysis, as a training activity, and as a research and planning tool. A wargame can create an estimate of the functioning of the whole system, including people, equipment and instructions.

Threat analysis related to the wargaming can be used to identify weaknesses in the systems and to evaluate what is the probability of potential attacks. Threats can be detected through the analysis of the effectiveness of an attack and what counter-measures can be used. After the analyses there can be made assessment on what protective measures are reasonable to do.

Training activities include, from the cyberwar point of view, technical training, security training, and leadership and management training. By wargaming there can be practiced, for example, the acts of various authorities and other actors in a conjunction with each other. When the critical infrastructure challenges are identified training can improve the performance of the operators. Wargaming can illustrate their scope and effectiveness, clarify management, find out the information sharing needs, to identify critical systems, their technologies weaknesses, identify the interdependences and identify the critical infrastructure as a part of asymmetric warfare.

By wargaming cyberwar there can be done research about the necessary legislation issues, as well as to assess the nature of the legal consequences of different actors. Cyberwar is a relatively new case from a legal perspective. Wargaming can provide an opportunity to illustrate what kind of cyberwar is, and to raise the necessary legal issues.

In the context of the war planning and resource allocation, wargaming can produce estimates how various cyberwar assets can impact to an estimated outcome. Estimates can make use of when making a decision with limited resource, how to protect the systems best or how to affect to the enemy systems. Cyberwar development is rapid compared to the conventional weapons technology. Therefore, the war planning context, comes into warpaly plans more frequently than in the past.

Leaders in strategic level must take necessary steps to prevent a surprise military attack, also in cyberspace. The big challenge in cyberwar is to get to know are you under an attack and how is the real attacker. Leaders must understand this issue because the risk of being deceived is much higher than in traditional warfare.

The defence of critical infrastructure cannot be practiced in reality. Critical infrastructure system cannot be turned off. Playing a wargame in which the events are simulated can practice how to operate critical infrastructure when part of it is disabled.

4 Discussion

”It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.”
Sun Tzu, ”The Art of War”

In accordance with the preceding quote from Su Tzu comes to know yourself and your enemy can give you forehand. Wargaming allows for this. In providing the ability to create understanding of a complex issue, it can also create the illusion of knowing things. Therefore wargaming end results will be to examine critically. All activities, in which the person is involved, cannot be established definitely in models.

Wargaming also has decided weaknesses. Preparation is laborious and players have to be well qualified for their assigned roles. Wargames conducted by inexperienced players may have large educational pay-off, but the significance of results is always suspected.

In the wargame design there must maintain a balance between detailed modelling and playability between. This relationship must be considered when designing the wargame to set the research issues. If the wargame is designed to look at the different authorities' responsibilities, it is not appropriate to model the things individual component accuracy.

Wargaming is used to explore and to discover what we do not know. Wargames places the participants to situations, where they must make decisions, which are not based on clear and complete understanding of the situation and its facts. The real challenge is to make wargame that can help to get the reflections on the matters that are not known. Admiral Chester Nimitz said that in Naval War College they have re-enacted war with Japan in the game rooms so many different ways, that nothing that happened during the war was a surprise. Absolutely nothing except the kamikaze tactics.

A wargame is an effective way in building a united view of the important key factors to the participants. It gives the participants new insights of cyber warfare in network-centric critical infrastructure defence. By wargaming, problems may be investigated in wide perspective. This is important when connections are weakly understood and critical features cannot be isolated. Conventional methods of analysis become then difficult if now impossible.

References

[1] Lewis, T. *Critical Infrastructure Protection in Homeland Security*. Hoboken: John Wiley & Sons, 2006. 474 p. ISBN 978-0-471-78628-3.

[2] Hagelstam, A. CIP – kriittisen infrastruktuurin turvaaminen [verkkojulkaisu]. Huoltovarmuuskeskus, Julkaisuja 1/2005. [cited 29.9.2014]. Available: http://www.huoltovarmuus.fi/static/pdf/243.pdf

[3] Kyberturvallisuusstrategian toimeenpano-ohjelma, FI.PLM.2014-1503. Helsinki: Turvallisuuskomitea, Puolustusministeriö, 12.3.2014.

[4] Cyberspace Operations Concept Capability Plan 2016-2028, TRADOC PAM 525-7-8. The United States Army, 2010. Available: http://fas.org/irp/doddir/army/pam525-7-8.pdf

[5] Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment, STO-MP-MSG-111. NATO Modelling and Simulation Group Annual Conference, 13.12.2013. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-4258

[6] Wihl, L., Varshney, M., & Kong, J. Introducing a Cyber Warfare Communications Effect Model to Synthetic Environments [paper]. The

Interservice/Industry Training. [cited 29.9.2014] Available: http://www.scalable-networks.com/wp-content/uploads/2011/04/Introducing-a-Cyber-Warfare-Communications-Effect-Model-to-Synthetic-Environments-2010.pdf

[7] The Implementation of Network-Centric Warfare. Washington, DC: Department of Defense. 5.1.2005. Available: http://www.carlisle.army.mil/DIME/documents/oft_implementation_ncw%5B1%5D.pdf

[8] Perla, P. *The Art of Wargaming*. Annapolis: Naval Institute Press, 1990. 365 p. ISBN 0-87021-050-5.

[9] Downes-Martin, S. *Adjudiction: The Diabolus in Machina of War Gaming*. Naval War College Review, 2013, Summer, Vol. 66, No. 3, p. 67-80. ISSN 0028-1484.

[10] Andress, J. & Winterfeld, S. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham: Elsevier, 2011. 320 p. ISBN 978-1-59749-637-7.

[11] Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia. Helsinki: Valtioneuvosto, 27.11.2003. Available: http://www.nesa.fi/tied/Yhteiskunnan_elintarkeat_toiminnot_271103.pdf

[12] Valtioneuvoston päätös huoltovarmuuden tavoitteista. Helsinki: Valtioneuvosto, 8.5.2002 Available: http://www.nesa.fi/julk/huolto-varmuustavoitepfin2.htm

[13] AAP-06 Edition 2014. NATO Standardization Agency, 2014. [cited 16.7.2014]. Available: http://nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf

[14] Dictionary of Military and Associated Terms, Joint Publication 1-02. Washington DC: Department of Defence. [cited 16.7.2014]. Available: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[15] Oxford English Dictionary, Sixth Edition, Oxford University Press, 2007

[16] Koskinen, H. *Sotapeliohje*. Helsinki: Maanpuolustuskorkeakoulu, Taktiikan laitoksen julkaisusarja, Nro 4/2000.

[17] Boehlke, T. Wargaming. Hamburg: Bundeswehr Command and Staff College, 2006.

[18] Weiner, M. War gaming methodology, Santa Monica: Rand Corporation, 1959.

[19] Lantto, H. Sotapelaaminen saksalaisessa sotataidossa 1918-1940, Helsinki: Maanpuolustuskorkeakoulu, Esiupseerikurssin tutkielma, EUK65, 2013.

[20] Perla, P. & Barrett, R. Wargaming and Its Uses, Professional Papers 429. Annapolis: Center for Naval Analyses, 1984.

[21] Lappi, E. *Computation methods for tactical simulations*, Helsinki: Maanpuolustuskorkeakoulu, 2012. 272 p. ISBN 978-951-25-2317-7.

[22] Dunnigan, J. *Wargames Handbook*, *Third Edition*. San Jose: Writers Club Press, 2000. 417 p. ISBN 0-595-15546-4.

[23] Hoffman, R. War Games, Foreign Military Study # P-094. Europe: United States Army, 1952.

[24] Rhoads, R. & Gilman, S. *Wargaming and simulation as tools for CONOPS development*. Naval Postgraduate School, 2004.

[25] Sabin, P. *Simulating War: Studying Conflict through Simulation Games*, India: Continuum, 2012. 363 p. ISBN 978-1-4411-8558-7.

[26] Geers, K. *Strategic Cyber Security*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, June 2011. 169 p. ISBN 978-9949-9040-5-1.

[27] Shakarian, P. *The 2008 Russian Cyber Campaign Against Georgia*. Military Review, 2011, November-December. Vol. XCI, No. 6. p. 63-69. ISSN 1067-0653.

[28] Kärkkäinen, A. *The Origins and the Future of Cyber Security in the Finnish Defence Forces*, In: Rantapelkonen J. & Salminen, S. (eds.). The fog of cyber defence. Helsinki: Maanpuolustuskorkeakoulu, julkaisusarja 2, nro 10, 2013. p. 91-107. ISBN 978-951-25-2430-3

[29] Deliverable D3.1: White book: Emerging ICT threats. FORWARD Consortium, 2010. Available: http://www.ict-forward.eu/media/publications/forward-whitebook.pdf

[30] Curry, J. & Price, T. *Dark Guest: Training Games for Cyber Wargare*, Lulu.com, 2013. 97 p. ISBN 978-1-2916-6912-1.

[31] Stuart, H. *Towards an evolving theory of cyberpower*. In: Czosseck, C. & Geers, K. (eds.). Cryptology and Information Security Series 3. IOS Press, 2009. p. 18-52. ISBN 978-1-60750-060-5.

[32] Musman, S., Temin, A., Tanner, M., Fox, R. & Pridemore, B. *Evaluating the impact of cyber attacks on missions*. M&S Journal, 2003, Summer. p. 25-35.

Cyber-Target Categorization

Pasi Hakkarainen
JAMK University of Applied Sciences
pasi.hakkarainen@iki.fi

Abstract

Purpose and research method

The purpose of this article is to present a framework and a method for cyber-target categorization. The framework contains factors, which influence on cyber targeting process and the presented categorization method provides an example, how cyber-targets could be categorized to support targeting decision making.

The article is based on literature study. Research method was to build an analogy between conventional and cyber targeting.

Findings and originality

Cyber targeting does not seem to be studied widely, but the common approach to cyber security seems to be "threat-based". This article presents a new categorization criteria and method for cyber-target analyze, with a target-based approach.

Keywords
Cyber-target, targeting, cyber targeting

1 Introduction

Importance

Targeting is an important component of the effect-based warfare. According to AFDD (Air Force Doctrine Document) 3-60 targeting during conflict enables air and space power to be a decisive force in modern warfare [1]. In effect-based cyber warfare, targeting is as needed component as in conventional warfare. In cyber warfare, there is a clear difference between targeted operations and "pointless" use of malware.

Conventional targeting is the process for selecting and prioritizing targets and matching appropriate actions to those targets to create desired effects that achieve objectives, taking account of operational requirements and capabilities [1]. Structured target analysis can support targeting process to achieve commander's objectives. In this article, target analysis means basically target categorization for the targeting process. The objective of the target analysis is to identify both valuable and available targets.

Research method

The objective of this article was to create new criteria for categorizing cyber-targets. The research question was: How cyber-targets should be categorized to support targeting. The research method was to build an analogy between conventional and cyber targeting. Method considered comparison between conventional and cyber: targeting, infrastructure, weaponeering and target.

The main result of the research is a proposal about the criteria for cyber-target categorization. The results of the research can be used in cyber targeting process. Additionally the presented methodology can be used to improve cyber security.

Research framework

The research question was divided into sub questions as follows:

- What is the framework for cyber targeting?
- Which factors influence cyber targeting?
- Which are the essential features of the cyber-targets considering effect-based targeting process.

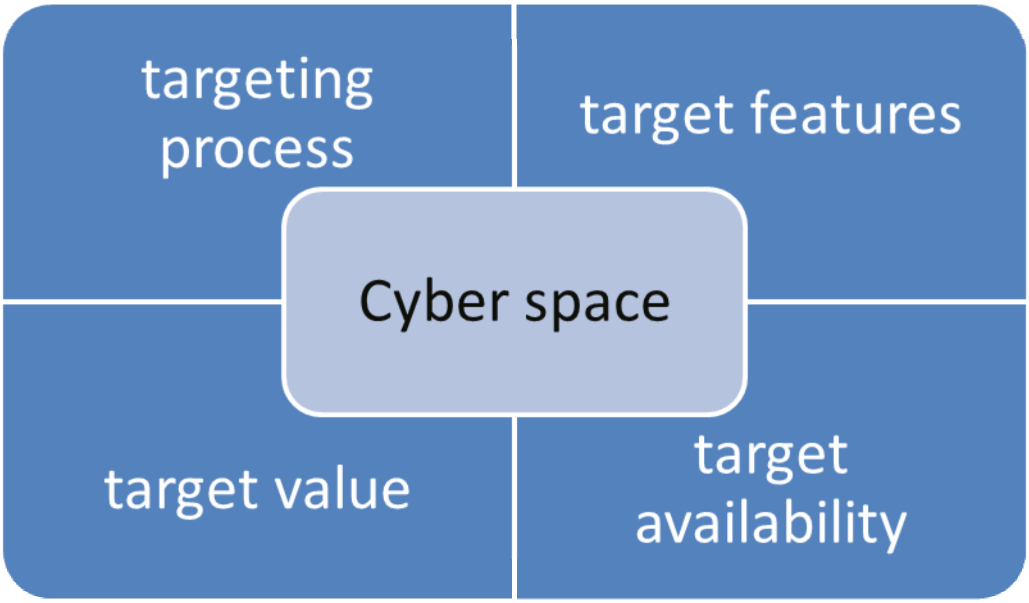


Figure 1. The approach to the literature study. The conventional targeting process is examined in cyberspace. Approach considers cyber-target features, cyber-target value and cyber-target availability.

In the article, the conventional targeting process was examined to provide the base for the analogy. Then the different approaches for evaluating target value and availability were examined. Previous research related exactly to cyber targeting was not available. However there were supporting research about, cyber security, cyber weapons and cyber warfare. The approach to the literature study is presented in Figure 1.

2 Targeting process and target

Background

Targeting is the key element of effect based warfare. If the commander wishes to produce the maximum effect with minimal effort, targets have to be chosen carefully. If the commander uses his/her power like in Verdun, for example, enormous resources can be used and lost without gaining any advance. Beside the desired effect, careful targeting facilitates avoiding collateral damage against civilian targets while executing military operations. Targeting process can to be used in both cyber warfare as in conventional war to pick up the most suitable targets.

According to AFDD 3-12, the cyber tasking order is analogous to an air tasking order [2]. In cyber warfare, the role of targeting is actually emphasized compared to conventional targeting, as the cyber weapons are more target sensitive than conventional weapons. For example, a mortar can cause damage both against armoured or unarmoured targets, but a Windows operating system exploit can be totally useless in Linux environment.

Targeting process

In this article, targeting process is examined with US Air Force Targeting Doctrine Document and FAS (Federation of American Scientists) JCS Joint Publications related to targeting.

Targeting process is systematic evaluation of potential target systems and their components to determine which elements of the target system(s) should, or could, be taken against to achieve the given objectives [3]. The end product of the target development process is an unconstrained prioritized list of potential targets. It reflects relative importance of targets to the enemy's ability to wage war. This list of targets is the basis for the weaponeering phase, where own capabilities are evaluated against the suitable targets [3].

Joint targeting cycle contains six different phases. In the first phase, the strategic level objectives are established. The second phase contains the target development, vetting, validation, nomination and prioritization phase. In this phase, the potential target systems are systematically examined. In the third phase, own capabilities against desired effects are evaluated. In the fourth phase, commander makes decision and approves the target list. In the fifth phase, missions are planned and the final phase considers assessment [1].

One important notice about the targeting cycle is that it is iterative and the following phase may have an influence on the previous one [1]. The cyber tasking cycle, which is based on the air tasking cycle, is also an iterative process [2].

Most of all, targeting process needs information about the possible targets. One absolute demand for any target is that the target has to be available for reconnaissance. If the target cannot be evaluated in advance, or the effect on the target cannot be observed, the target should not be nominated at all.

Target characteristics

Targets are evaluated and categorized with target characteristics. Every target has certain characteristics, which form the basis for the target detection, location, identification, and classification for future surveillance, analysis, strike, and assessment. In general, there are four categories of characteristics by which conventional targets can be defined: physical, environmental, functional, and cognitive. [1]

The physical features key characteristics of the target are: shape, appearance, number and nature of elements, reflectivity, structural composition, degree of hardening, electromagnetic radiation, location, size and dispersion. An example about environmental characteristics is terrain features. Cognitive features are, for example: how the target processes information, information that target requires to function, outputs to the processes the target performs, how much information the target can handle and how the target or system stores information. Functional features are, for example, what materials or resources the target requires to function. [1]

Converting physical and environmental characteristics into cyber space can be done by transforming them into virtual characteristics and IT infrastructure features. Physical characteristics would transform into cyber target's virtual characteristics, such as operating system, needed CPU efficiency, needed memory size and file or data formats. Cyber-target may also have an interface to physical space, which allows attacker to penetrate into cyber-target system through a physical connection. Environmental characteristics would consider network characteristics such as network protocols, layers, servers’ operating systems and databases – in other words the IT infrastructure characteristics.

Functional characteristics consider what the cyber target does. For example, these characteristics would be target's mobility, ability to defend and reconstitute it. These characteristics are quite similar between the cyber-target and conventional target. Cognitive features are, for example, how the target processes information, process input and output and how the target stores information. [1]

Overall physical and environmental characteristics have to be transformed into virtual characteristics and the functional and cognitive features are very similar in the physical or cyber space. The analogy between physical and cyber characteristics is illustrated in Figure 2.

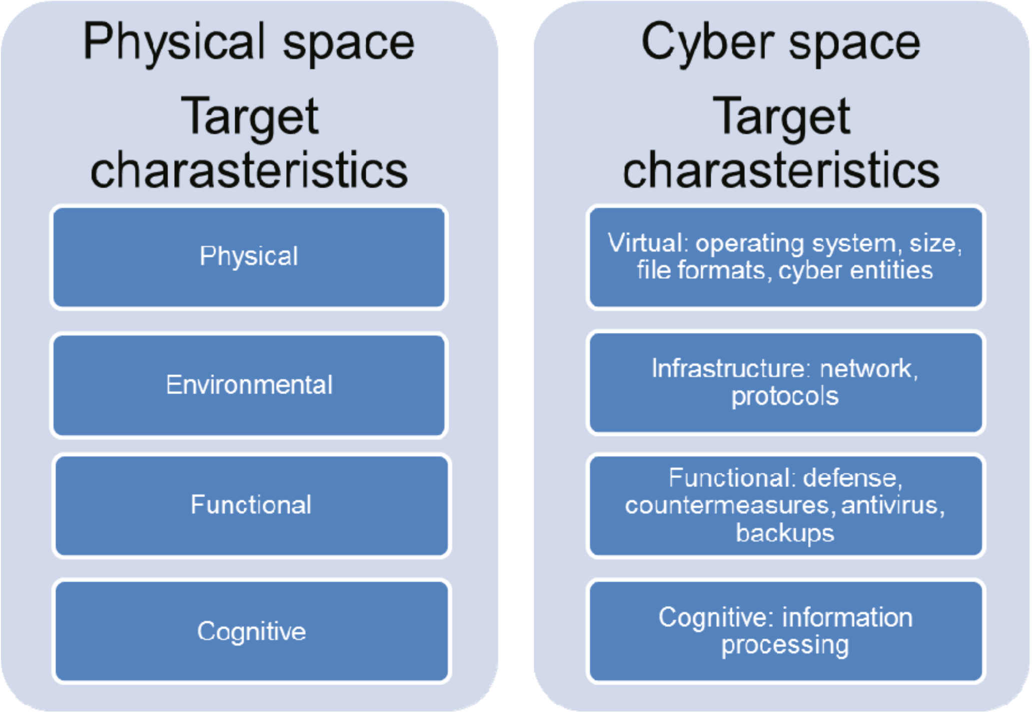

Physical space
Target charasteristics
Physical
Environmental
Functional
Cognitive
Cyber space
Target charasteristics
Virtual: operating system, size, file formats, cyber entities
Infrastructure: network, protocols
Functional: defense, countermeasures, antivirus, backups
Cognitive: information processing

Figure 2. Analogy between conventional and cyber-target characteristics

Weaponeering

Weaponeering means basically choosing the most effective and suitable weapon against the chosen target. Weaponeering can be seen as certain kind of optimisation. Some of the modern weapons are expensive and should be used after careful consideration. To be effective, targeting process must identify the best weapon for the intended target with appropriate timing to meet the objectives established by the commander. Weaponeering determines the quantity, type, and mix of lethal and nonlethal weapons required to achieve a specific level of target damage. [3]

Cyber-weaponeering itself is very target sensitive. Software exploits are useful only against certain vulnerabilities and totally useless against other cyber-targets. However, some cyber-attack methods, like denial of service attacks, can be used against several target systems.

Examples about cyber weapons and cyber-attacks against SCADA (Supervisory Control and Data Acquisition) systems are [4]:

Denial of service attacks to cause system shutdown.

- Deleting system files to cause system shutdown. Attack may not be avoided by reboot.
- Taking control of SCADA system. With this type of attack, an attacker may cause several kind of damage.
- Changing data in SCADA system.

3 Target Value

Concept

Target value means, how important the target is for the enemy's functionality. The reason for target value evaluation is that the attacker is able to choose those targets, which will cause the whole target system to collapse, after destroying the chosen targets. In conventional warfare, enemy commanding and communications functions are commonly seen as valuable targets. On nation level, critical infrastructures can also be seen as very high level targets. Protection of critical infrastructure such as water, power and energy is vital, because of the impact the destruction of the critical infrastructure would cause [5].

As the defender wants to protect the softest and critical targets, attacker wants to find and destroy the same targets. Because of this, both the attacker and defender can use similar analyse methods to find the critical points. The more critical the target is, the more valuable it is for targeting.

Network theory approach

In network theory approach, the critical infrastructure is modelled as a network to identify the critical nodes and links. Scale-free network theory establishes a basis for vulnerability analysis, because it reveals concentrations of assets that may be vulnerable for an attack. [5]

With the network theory approach, the most critical nodes or links can be identified in the critical infrastructure. If the attacker manages to effect on these critical points, the whole critical infrastructure may be paralyzed with minimal effort. Network theory approach is suitable also for the defender. As the attacker wishes to find and destroy the critical nodes, defender can try to protect, harden, duplicate etc. the critical nodes and links to increase the security.

Systems theory approach

Systems theory approach can be used after or beside the network analysis. Systems theory approach provides information on how complex systems interact with their environment, and this guidance can be applied to designing security. With systems theory approach, security designers are able to build layered defence on the target system [6]. The goal of the security is to ensure the critical functions. With systems theory approach, instead of identifying the threats in the system, losses are identified. The question is, what essential services and functions must be secured against disruptions and what are the unacceptable level of losses. [7]

With systems theory approach, the control, input, output and components in the target system are identified [6]. By totally destroying control or one of these functions, the whole system may be paralyzed with minimal effort. Besides the control, every function is essential for the output of the process. Process can be destroyed also by destroying a single function or by producing enough damage for every function.

Effect on the target network or system

When evaluating target value and the effect on the target system, target's importance for the target system or target network has to be studied, as the importance differs between critical components. In causality model, an initial component failure cascades through a set of other components [7]. Cascade failures are system-wide failures that begin with on single failure, but propagate throughout the entire system or network, ending in calamity [5]. With cascading effect, paralysing a single node, link of function, the whole target system or target infrastructure can be damaged. To avoid collateral damage and other unwanted effects, which cascading effect may cause, the meaning and functionality of the chosen cyber-target has to be known in advance.

Other target value characteristic may be target's capability to recover from the attack. For example, denial of service attack may not cause any permanent damage. Business systems may recover from an attack by simply rebooting the target system. But, for example, in industrial control systems reboot cannot be used as easily to solve problems as in enterprise environment [8]. Rebooting a SCADA system may cause the shutdown of the power plant of production facility, which cannot be done without preparations.

On the other hand, fault-tolerant networks continue to function even when some of the nodes or links do not operate [5]. An attack against a single critical component in the fault-tolerant system, can be totally useless for the attacker.

Levels of the cyber target

In cyber warfare research, cyber targets seem to be discussed only on very high level – as large infrastructure targets or whole information systems, or the concept of cyber target is not deeply analysed.

The chosen method to analyse a critical infrastructure or a target system influence on the targeting process. For example, a target system can be seen as a group of potential cyber-targets for the targeting process. According to Federation of American Scientists, military targets may be further classified as strategic, operational, and tactical [3]. While planning a cyber-attack, the target cannot be examined on system or network level, but the target system has to be divided into target and target entity levels. This is similar in conventional warfare as an anti-tank weapon can fire against a single tank, but not the whole tank division.

Cyber-target may be divided into different categories based on the level of the target. The highest level of the cyber-target concept would be cyber-target system, which is formed from the subsystems, and is the main objective of the attack. This could be, for example, SCADA or a flight control system. Cyber-targets would be single functions and subsystems, which are needed to make the whole system to function.

Cyber-target entity is a part of cyber-target which can be destroyed individually, but it is essential for the target system to operate. Cyber-target entity could be a single process, file, a sensor or a single function. Cyber-target entities are autonomous with simple behaviours and connect together and form a service. The levels of cyber-target are illustrated in Figure 3. For effect based warfare, it is essential to choose the correct target entity in the correct target system.

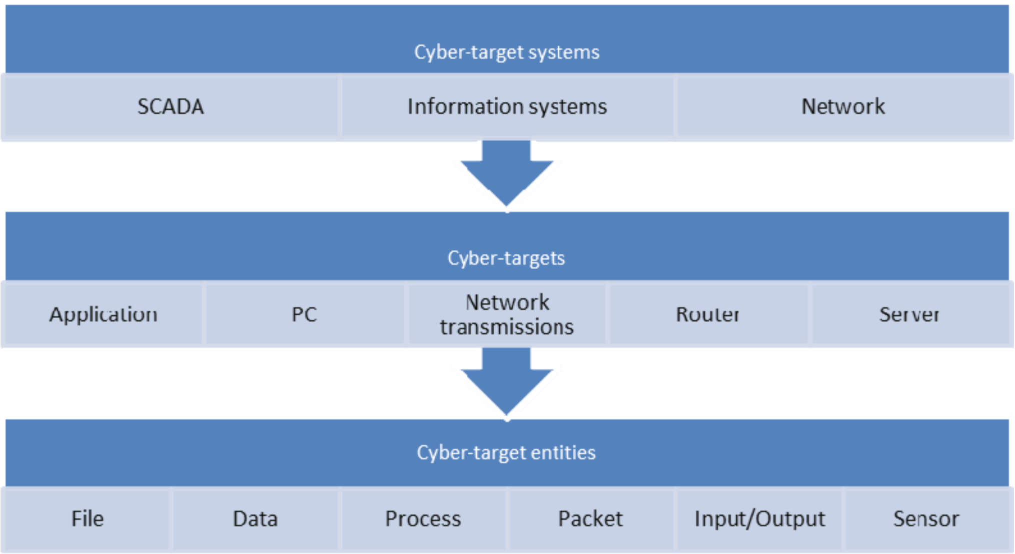


Figure 3. Levels of the cyber-target.

On cyber-target system level, possible systems could be SCADA or other information systems, network and network communications or organizations IT-infrastructure containing, for example, data storages, office software and identity handling systems. SCADA is a system to automate industrial control and monitoring [8]. SCADA systems are composed of computers, network communications, sensors, remote units and programmable logic controllers [5]. The complex and distributed structure of SCADA creates several attack vectors against it.

Cyber-target system can also be a hybrid, which exists in both in the cyber and the physical space. With a cyber-target system, an end user can also be influenced through the system, even when he/she does not exist in cyber space, or the target may be a physical device.

The ultimate objective of a cyber-attack may locate in the physical layer of the cyber space, or it may be the human actor above the application layer, or it may be inside the cyber space itself.

4 Target Availability

Concept

Target availability means how easy the target is to reconnoitre and destroy. The basic method for target availability analysis is to divide targets to “soft” and “hard” targets.

The actual target analysis can be carried out using several methods. Because the decision making process is constrained by time, costs, previous experiences, and perceptions of the participants, a great deal of decision making in the target development arena is based on qualitative rather than quantitative analysis. However, qualitative analysis is not a substitute for quantitative analysis. Both are useful techniques for structuring a problem to reach a rational conclusion. Both may be used to reduce uncertainty in decision making. [3]

The key elements of the target availability are: 1) target defence and 2) target vulnerability.

Cyber-target system defence contains [4; 6; 7; 8; 11]:

- Access control (firewall for example)
- Anti-malware
- Encryption

- Intrusion detection systems
- Backups and mitigation.
- System hardening
- Honeypot to distract the attacker

Cyber target vulnerability can be evaluated with CIA (information confidentiality, integrity and availability) approach. With this approach the information is seen as a target and the objective is to influence on the 1) information confidentiality by revealing secret information, 2) information integrity by removing or alternating information or 3) information availability by denying users to gain access to desired information.

Cyber weapon target analysis

In cyber weapon target analysis, the cost of achieving the target is evaluated with certain criteria. With cyber weapon systems, the cost of achievement analysis is conducted by considering the cyber weapon system functions and the components of the cyber-attack, to gain the overall understanding about the chosen cyber-target system. The evaluation should consider:

1) Possibility for the initial penetration into target’s cyberspace.
2) Possibility to operate in the cyber-target system containing:
    a) Searching
    b) Identifying
    c) Spreading
    d) Connecting to C2 servers
    e) Communications with peers
    f) Evaluating the situation
3) Possibility to influence the cyber-target and cyber-target entity.
4) Possibility to evaluate the caused effect on the cyber-target system.
5) Possibility to avoid cyber-target system's countermeasures.

For a successful attack, the cyber weapon system has to be able to perform all these actions. [9]

5 Target reconnaissance

Concept

Reconnaissance attacks allow an attacker to identify potential cyber-targets in advance [10]. To be able to gather all the information needed for the targeting process, the cyber-target has to be easy enough to reconnoiter. If the target system is a ”black box” and there is no information available about its functionality and features, the target can be seen as very hard target to influence.

Public information

Public information means information which is legally available for anyone. Some of the target system information may be online and available for anyone through the internet. Software and hardware manufactures usually provide documentation and other online information about their products. Information may contain, for example, default passwords and configuration. Inquiring public information is legal and can be done with home PC through internet.

Network devices can be seen as easier targets for reconnaissance, because the documentation is usually available in the internet. For example, information about SCADA systems, programmable logic controllers etc. can be found from online documentation available for anyone [4]. This makes them possible critical infrastructure targets, because control systems security is of prime importance for example for energy sector [8].

Public information may be easily inquired with, for example, search engines. If the device type and serial number are known, critical information about cyber-targets features and functionality can be found easily. Additionally the usage of common technologies, such as TCP/IP and common operating systems, makes the target systems easier to reconnoiter [4].

Hidden information

In this article, hidden information means information, which is not publically available. Revealing hidden information is usually illegal or revealing it requires illegal methods and tools. Usually the search of hidden information is done after all the public information is already gathered. Methods for searching hidden information can be technical or social engineering.

Usually the search of hidden information requires more sophisticated software tools and skills than the search of public information. Attacker has to be able to use tools like Netcat, Nessus and NMAP, and he/she has to be able to evaluate the results.

During reconnaissance attackers identify systems and then finger print the connected systems. Finger printing means finding out which ports are open and identifying version of the remote operating system [10; 11].

Social engineering means obtaining hidden information using human vulnerabilities. There are various techniques to commit social engineering. One of the effective features with social engineering is, that target may not even realize being under reconnaissance. [12]

6 Conclusion

Based on the approaches presented in the chapters 2, 3, 4 and 5, it is possible to build a categorization method for evaluation cyber-targets for cyber targeting process. The factors influencing on target categorization are presented in Figure 4 and the proposal for the cyber-target categorization is presented in Table 1.

First of all, targeter has to be able to reconnoitre the cyber-target. The easier it is to gain information about the target, the easier it is to analyse the target. One important notice is, that also the effect on the target has to be assessed. Cyber-targets using common commercial software and hardware and common protocols can be inquired more easily than "black box" or legacy systems, which have old and tailored software, which may not be well documented. Hiding information is not an inclusive solution, because there are methods for revealing hidden information technically or with social engineering.

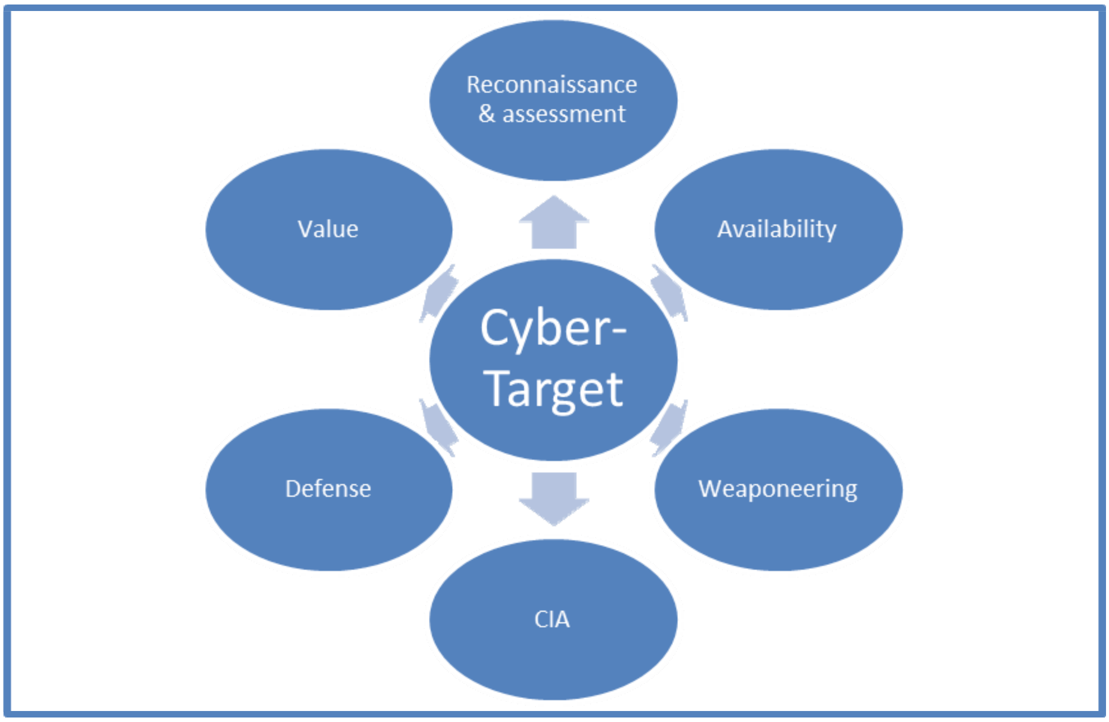


Figure 4. Target categorization criteria

With target analyse, there has to be a clear understanding about the levels of the target. Target value has to be examined based on the effect on the system or infrastructure level. After the cyber-target system is chosen, targeter has to identify the critical targets inside the target system. After identifying the targets, targeter can choose the correct cyber-target entities to be affected. Good features for the target are possible cascading effect and poor capability to recover.

Availability means that attacker is really able to affect the valuable target. Attacker has to be able to connect to target's cyber space. Internet access makes target systems easier to attack, when there is no need for physical connection. Remote connections enable attacks from the distance without entering to the target system area geographically.

Good target defence can prevent the attack in advance. If the target systems has reliable access control and intrusion detection system, it decreases attacker capability to operate in the target system. Encryption can hide critical information and possible use of honey pots create contingency for the operation.

Weaponeering is highlighted in cyber-attack. Cyber weapons are much more target sensitive than conventional weapons. Exploits are useful only against certain vulnerabilities. For the weaponeering, targeter has to gain a great deal technical information, such as operating systems, software versions, updates and configuration – in other words information about target's characteristics.

After all, the final objective is to influence a cyber-target entity. Target entity's information has to be affected and one or several tenets of target's CIA must be compromised. For this objective, target-entities' features must be known. Cyber-target entity has to be chosen carefully. Influencing right entity in the wrong system or vice versa, makes an attack ineffective. Information needed about cyber-entity contains the nature of the entity, environmental features such as operating system and protocols and hardware.

Cyber-target	
Reconnaissance	White box vs. Black box
Value	Critical vs. easy to replace
Availability	Available vs. unavailable
Target defence	Soft target vs. hard target
Weaponeering	Suitable weapons considering target characteristics
CIA	Cyber entity features

Table 1. Categorization method for cyber-targets

7 Discussion

The role of targeting seems to even increase in cyber warfare compared to conventional targeting. Cyber weapons can be totally useless in wrong kind of virtual environment and cyber-weaponeering is very target sensitive. There is a clear difference between targeted attack and “pointless” use of malware. Targeted cyber operations save resources, increase results and reduce collateral damage.

The conventional targeting process is a suitable approach also with cyber targeting and similar functions can be used with cyber-targets, but the importance and signification may differ. For example, available weapons influence a great deal on which target characteristics are important to reveal. On the other hand, cyber weapons can also be manufactured faster than conventional weapons and found opportunities may be more easily exploited.

There seems to be several methods for defender to turn his/her system as a “hard” target and avoid the attack in advance. These methods consider reducing single targets value and availability. The most useful defence method could be layered defence, where the first step would be hiding the systems existence, functionality and characteristics.

This article bases on literature study and presents only a proposal about cyber-target categorization. Presented criteria for cyber-target categorization should be evaluated in future research. Especially the weight of each presented categorization criteria, should be evaluated during an actual cyber-targeting process.

References

[1] Air Force Doctrine Document 3-60, Targeting, United States Air Force, 2006, 2011. Available: http://www.fas.org/irp/doddir/usaf/afdd3-60.pdf [cited 21.4.2014]

[2] Air Force Doctrine Document 3-12, Cyberspace Operations, United States Air Force, Cyberspace Operations, 2010, 2011. Available: http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf [cited 1.5.2014]

[3] Federation of American Scientists, JP 3-55, Reconnaissance, Surveillance, and Target Acq Sppt for Joint Op, 1993. Available: https://www.fas.org/irp/doddir/dod/jp3-55/3-55ch4.htm [cited 1.5.2014]

[4] Pollet, J. *Developing a Solid SCADA Security Strategy*. Published in Sensors for Industry Conference, 2nd ISA/IEEE, pp 148–156. 2002

[5] Lewis, T. *Critical infrastructure protection in homeland security*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2006

[6] Concling, A. & Dietrich, G. *Systems theory model for information security*. Published in Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, pp 265. 2008

[7] Young, W. & Leveson, N. G. *Inside Risks and Integrated approach to Safety and Security Based on Systems Theory*. Published in Communications of the ACM, Feb2014, Vol. 57 Issue 2, pp 31-35. 2014

[8] Mahboob, A. & Zubairi, J. *Intrusion Avoidance for SCADA Security in Industrial Plants*. Published in Collaborative Technologies and Systems (CTS), 2010 International Symposium, pp 447-452. 2010.

[9] Hakkarainen, P. *Cyber Weapon Target Analysis*. Book on Demand, 2014

[10] Morris, T. H., Shengyi, P. & Adhikari, U. Cyber security recommendations for wide area monitoring, protection, and control systems. Published in Power and Energy Society General Meeting, IEEE, pp 1-6. 2012

[11] Rowe, N. C. & Goh, H. C. *Thwarting Cyber-Attack Reconnaissance with Inconsistency and Deception*. Published in Information Assurance and Security Workshop, IAW '07, IEEE SMC, pp 20-22. 2007

[12] Mouton, F, Malan, M,M, & Venter, H,S. *Social Engineering from a Normative Ethics Perspective*. Published in Information Security for South Africa, pp 1-8. 2013

SCADA, Critical Infrastructure and Cyber Threat

Timo Vestama
Finnish National Defence University
timo.vestama@mil.fi

Abstract

Purpose

SCADA (Supervisory Control And Data Acquisition) is widely used type of different Industrial Control Systems (ICS). This article describes the system and how it is related to critical infrastructure and why cyber security of such systems should matter in the context of national security in Finland and other developed countries. SCADA systems today face similar cyber vulnerabilities than other information systems and measures are needed to make these industrial control systems more secure. However, SCADA systems are in many ways different from typical corporate networks and services and pose certain challenges that are non-existing on more traditional IT systems. This article should give a reader which is familiar with IT security in typical corporate or government environments some insight to SCADA systems and the challenges lying in Industrial Control Systems in general. On the other hand, industrial automation engineers, technicians and students in this field without the expertise on IT security itself may find some new insight on the cyber security properties of industrial control systems.

Design/methodology/approach

This article is based on a collection of literature, academic research papers, conference presentations and official documents mainly from United States and Finland. This article tries to find a compact overview on the problem without going too deep in technological details. As SCADA cyber security in the context of national security and critical infrastructure is not only technology, we also approach the subject through security studies and try to find a reason why SCADA cyber security should matter on national scale.

Findings

SCADA and industrial control system cyber security is a widely researched subject, especially in the United States. Challenges of SCADA cyber security are well understood, but implementation of effective information security and cyber defence measures is often difficult because of different technological limitations and also because of the expenses. In Finland, with the new emphasis on cyber security on national level, the cyber security of industrial control systems and critical infrastructure in general will hopefully see new development in the upcoming years.

Originality/value

As described, this article is based on published academic papers and other publically available documents and as such, it tries to give a compact enough overview for those who find themselves new or unfamiliar to the subject instead of approaching a certain problem that most of the academic papers do. There is also relatively little publications or even thesis works made of the subject in Finland and as such, those parts of the research concerning the current situation and future in Finland have original information. As this article tries to see the "big picture" of SCADA cyber security and not only focuses in engineering or technical aspects, there was a need to approach the problem through security studies and thus explain why SCADA is important for national security. This interdisciplinary approach is rarely used in more technical documents of the subject.

Keywords

SCADA, Industrial Control Systems, Critical Infrastructure, Cyber Security

Paper type

Research paper

1 Introduction

SCADA systems are widely used industrial control systems throughout the world. In the history they were largely fully proprietary systems, but through standardization and with general advancements in technology starting from the late 1980's, commercial-on-the-shelf (COTS) hardware and the use of Internet Protocol technologies are nowadays common in industrial control systems. Aspects such as interoperability requirements, system cost and expandability are playing ever larger role in the design which again has put pressure on the need to move away from proprietary systems. At the same time it has become possible to link industrial control systems to other networks and services. All this development during two or three decades has exposed SCADA systems to similar cyber threats that we see with other IT systems. What makes this situation worrying is the fact that SCADA systems are used in industries that are considered as critical in many countries.

There is substantial amount of research done in different research institutes, laboratories and academia throughout the world on the subject. Research gained momentum soon after 9/11 in the United States and has continued since throughout the world. Stuxnet incident in 2010 was another milestone, which caused rising interest in industrial control system cyber security in many countries. Although problems are quite well understood, there is still a lot work to do in the implementation of improvements both on the security processes and systems.

There are good research enhancement possibilities on the subject in Finland, as amount of publically available research here is still relatively low. After the release of national cyber strategy implementation plan in the spring of 2014, there is a need to gain more understanding on the current local situation of our critical industrial control systems and how it affects our national security.

2 SCADA system overview

To understand the nature and operation of SCADA, let’s first look at the main components of a typical Supervisory Control And Data Acquisition (SCADA) system. In short, SCADA systems are industrial automated process control systems which are used to monitor and control process equipment in many industries such as electric production and distribution, gas and oil refining and distribution as well as water and waste water delivery and purification systems. Definitions for SCADA systems tend to differ in detail somewhat depending on the source, but generally, it is represented as consisting of four main components:

1. There are one or more field devices on a *remote site* or *substation*, usually Remote Terminal Units (RTU), and/or Programmable Logic Controllers (PLC). These field devices are practically computers, which consist of communications unit and usually several digital and analogue inputs and outputs, which again interface the unit to the different sensors or Intelligent Electronic Devices (IED). IEDs can be for example motors, pumps or valve actuators equipped with a microprocessor or controller thus allowing the control of the device. PLCs or RTUs can be also connected to different relays or switchboxes which again can control “dumb” devices without microprocessor logic. [5; 8; 9; 19]

2. SCADA communications system can generally be divided to short and long distance communications. Short distance communications are on-site communications *within* the remote site, which connects the field devices to the IEDs, relays, switches or sensors. Long distance communications are used to transfer data between field devices and the computers in the SCADA central host. Short distance communications usually employ serial connections over twisted copper pair or LAN networks. Long range communications, on the other hand, can be almost anything that is best

suited and most cost effective option, which again depends mostly of the remote site location, available communication methods there and of the distance to the SCADA host. Long distance system can be radio, telephone, cable, satellite, etc., or any combination of these. Different remote sites in the SCADA system can be equipped with variety of aforementioned methods. [5; 8; 9; 19]

Communication protocols used in the system are specialized SCADA-protocols, which were developed the data models used in RTUs and PLCs in mind. Some protocols are suited specifically for the communication within the remote site, some are used for the long distance communication only and some suit for the both applications. Many of the most popular protocols are open protocols and maintained by foundations, international organizations or joint groups of manufacturers. Most of these widely used protocols date back in the late 1970's, 1980's or early 1990's and thus they were originally developed only for serial communications, but during the last 15-20 years, most of them were specified for packet data networks such as IP also. Protocols utilize in most cases polling, where a device upper in hierarchy (master) polls the information from the lower device (slave), although some of the protocols may utilize peer-to-peer operation in certain cases. Polling is necessary for serial communications, because there can be only one device at a time reserving the communications channel. For example, RTU or PLC would be a master and IED a slave and again SCADA host computer would be a master to these field devices. [5; 8; 9; 19]

Documentation for these popular open protocols is extensive and in many cases, available for free or for nominal fee. Along with supported field devices, there are several manufactures that produce networking devices that can route messages or perform protocol transformations. During the last few decades 150–200 SCADA protocols were developed [6]. Most of these protocols were rare and closed proprietary standards developed by variety of companies. Over the years, open protocols have become most common and amount of widely used protocols today is far smaller. Few of the most popular protocols used today include MODBUS, PROFIBUS, ICCP/TASE.2, DNP3, IEC 60870 and IEC 61850.

3. SCADA host, SCADA master or Master Terminal Unit (MTU) is a computer or a set of networked server computers which also provide a man-machine operator interface to the SCADA system. SCADA host computers process the information gathered from the remote sites and send control commands back. Amount of gathered data may be huge, as there may be thousands of different sensors and PLCs etc. in the system where data is constantly collected. Control room displays and control workstations or terminals and associated accessories are connected to the host via a LAN or WAN network. [5; 8; 9; 19]

Originally, SCADA hosts were largely fully proprietary mainframe computers, which meant that the hardware and software could be fully developed by a single manufacturer. This also meant that they were usually incompatible with devices from other manufacturers and expanding the system might prove to be expensive or a difficult task. Together with open protocols and with the use of common commercial-on-the-shelf (COTS) hardware and software, interoperability and maintenance has become a much easier and cost effective task. Nowadays, Linux, Unix or Windows server platforms are commonly used with regular or industrial server computers. [5; 8; 9; 19]

SCADA host also includes historian, which is a database of all the gathered values and parameters of the system. It is mainly used to validate the gathered data values, as data quality plays a big part in SCADA systems and long distance connections can be unreliable. [5; 8; 9; 19]

4. Man Machine Interface (MMI) or Human Machine Interface (HMI) is a part of the SCADA central host and includes all the control tools that the human operator uses for supervising and controlling the processes. It consists of software and hardware and the purpose of the MMI is to present the gathered data in the form that is understandable by humans. Nowadays information is usually presented using computer generated graphics through displays. Also, warning lights and sound effects can be used to enhance alert messages popping on the screen. Hardware wise, MMI may include normal computer accessories, such as mice and keyboards as well as customized dashboards with different set of controls. It is important to understand, that human operator doesn’t actively control the processes in the SCADA system as much of it is automated. Every remote site, or outstation, controls the process most of the time automatically by using its PLCs and RTUs with set parameters. Also, SCADA central host can give automated control commands to substation, if necessary. This independent operation of the system is important, because the long distance connections aren’t reliable and system needs to work a short time even if the connections between central host and the remote site are temporarily down or data corruption occurs. That is why operator’s main function is to *supervise* the process and human intervention is mainly required only when something unexpected happens. [5; 8; 9; 19]

Along with the main components of a SCADA system listed above, there can be several other networks or servers connected to the SCADA network and host. Originally SCADA systems where usually fully isolated without connections to outside world, but nowadays information is in many cases sent and received from a variety different information systems. For example, information from SCADA host can be used for billing purposes and for that, SCADA host has a gateway to the corporate network and associated systems there. Directory services and Enterprise Resource Planning (ERP) or Geographical Information Systems (GIS) may be also linked with the SCADA. [19]

Typically, SCADA systems also include engineering workstations, which are used for the programming and configuring of the PLCs and RTUs. Engineering workstations run a specialized software for this purpose. Updates to the PLCs and RTUs can be sent to remote sites via network or by a technician on site. In the network, with all the routers, switches and modems, front end computers can be used as a data gathering nodes. Also, large SCADA systems may consist of several control rooms and hosts, which are again connected together. [8; 10; 17]

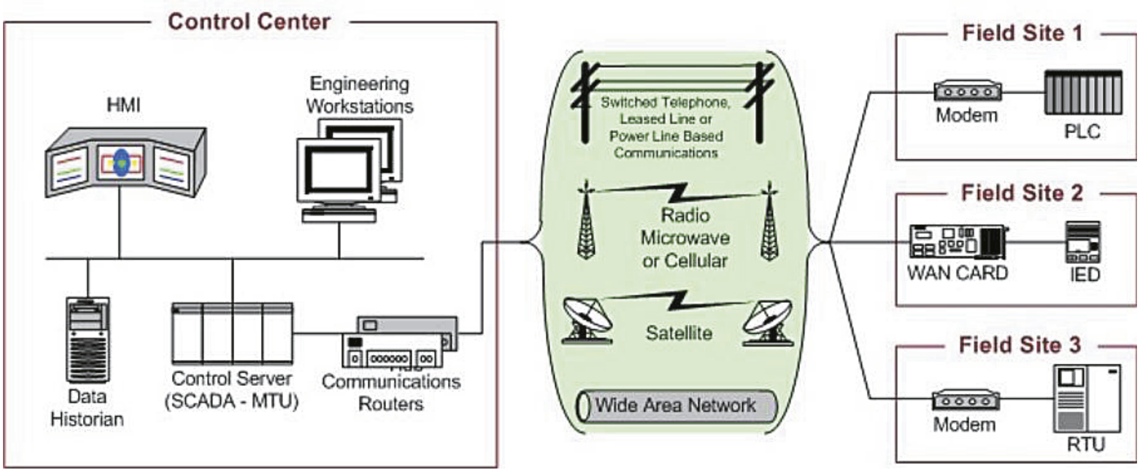


Figure 1. Basic SCADA layout [17]

SCADA systems are easily mixed with other industrial control system called Distributed Control System (DCS). DCS systems, although consisting of many same components such as PLCs, are very different in operation compared to SCADA. SCADA systems usually occupy a large geographical area as DCS systems are typically limited to one plant area. DCS systems are designed to control a complex process on the site usually by using a closed loop control scheme over fast and reliable connections thus making real time control of the process even more pronounced than it is for SCADA systems. On the other hand, because of the SCADA's wide area and somewhat unreliable long distance connections, remote sites has to be able to work independently and system's main function is towards data gathering. Because of the advances in communications and networking, these two type of systems have technically become more and more similar to each other, but the significant difference remains, where SCADA is an information oriented system, where control room is at its focal point, while the focus of the DCS systems is the process itself. [25]

2 SCADA, critical infrastructure and cyber threat

As described shortly in the beginning of chapter 1, SCADA systems are used in the industries, which in most countries are considered as critical infrastructure. Different areas of critical infrastructure are important for the survivability and wellbeing of the civilian population and for the operation of government itself in any developed state. Definitions for critical infrastructure can vary a bit depending on the country, but generally it consists of areas such as energy production and distribution, public safety, health care, banking and finance, transportation, communications and different manufacturing industries. For example, without electricity, it doesn't take long when modern society collapses as communication and information systems stop working and buildings cool down in the winter. In fact, without electricity, pretty much all the other aspects of the critical infrastructure are soon in peril. At the heart of electric distribution system are SCADA systems controlling the substations of the electric distribution grid. [4]

Cyber warfare and other cyber threats have gained a lot of momentum in the media during the last couple of years. Not only within the public and media, cyber threats and information security in general have risen also to the political debate and in many countries and cyber threats are considered as a potential new dimension in the threat maps of the states. It seems, that different nations still see the threat very differently. Why then these industrial control systems are or should at least be important to us when considering the cyber threat towards critical infrastructure in Finland?

Forrest Hare analysed in his paper *"The Cyber Threat to National Security: Why can't We Agree?"* why different nations among Nato coalition don't seem to find same view on the cyber threat thus making co-operation and finding consensus about the problem difficult, although at the same time, nearly every developed country sees the cyber threat as a potential problem. He approached the problem through the security studies using framework from the Barry Buzan's *"People, States and Fear: The National Security Problem in International Relations"* as a basis. Buzan presented a model in his work, where a combination of national power (or weakness) compared to neighbouring countries, and national cohesion are deciding factors for the vulnerabilities of the state. National power means military power, but a wider aspect, such as economic power can be taken into account also.

Hare applied Buzan's model for cyber security and presented a matrix in his work in the same way as Buzan did for the security of state. Hare's matrix is presented in Figure 2. [26]

Hare's model, as well as Buzan's, is very relativistic and measuring national power or cohesion by absolute numbers is very difficult, if not impossible, but comparisons between countries on an international system is still possible.

On the figure 1, we can see that cyber attacks on critical infrastructure are the defining vulnerability in states, which are relatively weak in power, but on the other hand have a strong cohesion. Vice versa, actions that are trying to destabilize the society politically are very unlikely to cause significant threat to the state in these countries. [26]

As said above, Hare’s table isn’t the absolute measure about the vulnerability of the state. It also presents how nations *perceive* the threat and why consensus is difficult to obtain.

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	De-stabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDOS and other major attacks on critical infrastructure*
	Strong	De-stabilizing political actions in cyberspace	Criminal activities in cyberspace

Figure 2. Cyber vulnerabilities and Types of States [26]

In the case of Finland, it is quite easy to classify it belonging to the weak powers. Although a developed nation, Finland has a small population, natural or other resources and military power is small when compared to the major powers and even some of the neighbouring countries. Finland’s economy is also quite specialized and focused on exports, which makes the economy more vulnerable to international crisis and economic down turns. At the same time, Finland is considered as a stable and socially equal state with high regard of civil rights and democracy. This places the vulnerability of critical infrastructure as the biggest threat towards the national security according to Hare’s model.

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	Highly vulnerable to most types of threats	Particularly vulnerable to military threats
	Strong	Particularly vulnerable to political threats	Relatively invulnerable to most types of threat (less inclined to characterize issues as military)

Figure 3. Vulnerabilites and Types of States from People, States and Fear (1991) [26]

What about the threat itself? Who are the actors causing possible harm to the critical infrastructure utilizing cyber space? Are they script kiddies, criminals or terrorists? Answer to this can be probably found easily by pure reasoning, but we can use Buzan’s original model here as a support. Buzan’s original matrix is presented in figure 3. [26]

Here we can see that Finland and other similar states are vulnerable to military threats most likely caused by other more powerful states. If we now place these two matrixes above each other, we can imagine a picture, where cyber threat towards the critical infrastructure is a part of a hostile military operation by a more powerful state or by an organization supported by the government with adequate resources, motivation and carefully defined objectives.

All this of course doesn’t negate the possibility of some other criminal activities in our cyber space with totally different goals and performed by completely different actors. It is of no question that a criminal or terrorist group couldn’t target our critical infrastructure in cyber space. However, crime or politically motivated actions are unlikely to cause a threat to the state itself *within* the state as seen in both matrixes, thus the threat is most likely foreign based. Also, as cyber operations are always tied to the real world at least through the motivations and objectives of the actors, it is very difficult to see what gain some foreign criminal group would achieve by intentionally launching a campaign against the information systems of Finland’s critical infrastructure. Extortion and monetary gain might of course be possible, but still probably much more unlikely, than a threat as a part of military operation.

Advanced Persistent Threat (APT) is a term that is used of the organizations that are well funded and systematically compromise government and commercial entities, and which also have the ability and resources to perform these sophisticated cyber attacks towards the critical infrastructure and SCADA. Typically, term refers to advanced adversaries that are focused on critical data and exploiting the information in covert manner. APTs have the resources to bypass most of the cyber security software and hardware and establish a long-term network presence in the target organization. Attacks are stealthy, carefully planned, targeted and data focused, which makes them very different from traditional computer viruses or worms. [3; 8]

All this means that APT attacks can last very long time. In the case of SCADA, it can start with the stealthy intrusion to the target organization’s corporate network from Internet and again from there pivoting through the gateways and firewalls all the way to the connected SCADA network and thus finally gaining access to the SCADA host, MMI and engineering workstations. After this, it can be quite simple task to gather data about the operation of the SCADA system as a whole and gain access to the RTUs and PLCs in the remote sites. Along with this method, it is also possible to perform man-in-the middle attack through the unprotected WAN connections. No matter how the attack is performed, all this time the target organization is unaware of the threat while attacker maintains its presence in the system without doing any harm at this point to the operation. After extensive data collection about the target system, attacker may have a complete picture and control of the control process and finally, it is possible to launch a harmful attack on the system at almost any time, for example, as a part of the larger operation during international crisis. [21; 27]

So, what can be the consequences of a cyber attack on SCADA and other industrial control systems? In short, successful attack can delay, block or alter the controlled process or the information related to the business operations revolving around the process, for example loss of the metrics obtained from the SCADA system used for billing purposes. In practice results may vary from financial impact of varying scale and minor disruptions in production to life-threatening incidents to plant workers and population by the release of hazardous materials to the environment after attacker caused a process to run off and disabled all fail safes. When we are talking about the critical infrastructure, which is essential for the wellbeing of the population and providing working services for the nation as a whole, most severe damages can thus pose a threat to the national security itself. [8; 16]

2 SCADA vulnerabilities

SCADA and other industrial control systems in use today were developed in the time, where modern networking, personal computers or Internet didn’t exist or weren’t used widely in business operations. SCADA systems were fully proprietary and physically isolated systems which used their own set of protocols throughout the system. From the late 1990’s internet technologies have become more and more common in SCADA system design. At the same time, the ability to link SCADA and with other services and networks became possible. This also meant that they became vulnerable to new cyber threats similar to other IT systems.

Air Gap is a term which has still lingered on with SCADA and other ICS systems. It is a term that refers to an isolated system and some still believe it is possible to maintain such system. But information exchange between ICS systems and other services is probably here to stay and even necessary. Even if it would be possible to run a certain SCADA system without any connections to other networks, patching software and reconfiguring the systems means at least that technicians and engineers need to attach USB sticks or other mass storage devices and perhaps even computers to the system. If nothing else, Stuxnet proved that no air gapped system practically exist anymore, not in SCADA or elsewhere. [2]

Originally SCADA protocols were designed for reliable operation over small bandwidth connections. This operation over existing networks was one of main deciding factors for the protocol design and network security wasn’t practically considered as a requirement at all. For example, one of the most popular protocols, MODBUS, has no encryption or authentication built in, only 16-bit or 2 characters CRC/LRC check to validate the payload integrity and with the MODBUS TCP/IP implementation, even that is removed [12; 13]. Using clear text communications makes reverse-engineering the protocol and system operation much easier and it also reveals usernames and passwords used for authentication in the system. It is also not uncommon to use shared passwords for SCADA operators to make operating procedures smoother. This not only makes intrusion easier for attacker, but also eliminates the authentication and accountability of the legitimate users in the system. However, using encryption or strong authentication in the SCADA system isn’t always practical, and we’ll come to that later in the chapter 3. [2; 5; 17]

SCADA systems have been and in many cases continue to be separated administratively from the business networks and other IT services of the companies operating these industrial control systems. Practically this means, that SCADA network is designed, operated, maintained and documented by industrial automation engineers, not by or even with the co-operation of the IT security experts dealing with the other business IT services. This practice also dates back to the history of the SCADA systems and to the times when they were proprietary and fully isolated systems.

Historically, automation engineers have very little formal training or expertise in IT risk management or in best security practices of the IT infrastructure. With that, and as industrial control systems are fundamentally very different in their operation compared to regular IT systems, automation engineer’s approach towards risks is usually very different from that of IT security expert: Where data confidentiality and integrity are usually most important for typical corporate networks and services, for SCADA, fault tolerance, human and environmental safety and the process availability are the topmost concerns for the operation. For SCADA and other industrial control systems, reliability and real-time performance requirements are usually much higher compared to typical corporate network requirements. Down time and temporary lack of availability are often tolerated in corporate networks and services, and for example rebooting of hardware is completely normal maintenance procedure and temporary outages are quite acceptable. For Industrial Control Systems, high levels of redundancy and fault tolerance are usually required and all outages must be planned days or weeks in advance not endangering the safe performance of the process. [10; 17]

This difference and clear separation between these two worlds pose a risk to the SCADA system as its security policies, training of the personnel, security architecture and both documented administrative and practical security procedures may all be inadequate for the control system concerning the cyber threat. Risk management and security policies suggested by the IT security personnel may even seem conflicting with the SCADA requirements and in some cases engineers operating the system may be unreceptive for IT staff recommendations. At the same time, IT personnel may not fully understand the peculiarities sand operation of the control system. This can lead to the situation, where SCADA system is not only exposed to attacks, but also the engineers and technicians operating the system are totally unprepared for the threat and unable to react properly to a cyber security breach. [5]

As SCADA systems consist of different hardware and software components, there is also always a possibility for flaws in those components. For example, from the beginning of the year 2014 till the end of July 2014, Open Source Vulnerability Database (OSVDB) has listed 94 publically exposed flaws in the SCADA equipment and related software [15]. In line with the problems described in the previous paragraph, platform vulnerabilities may also be caused by misconfigurations or poor maintenance of the SCADA applications, operating systems and other software. Also, SCADA system’s firewalls, intrusion detection systems, remote access practices, encryption, virus protection and password policies may be inadequate or misconfigured leaving the system exposed. [17]

Listed above are some simplified and general vulnerabilities discussed in short. Real life systems may have some or all of these deficiencies and true risk analysis of a certain system of course goes in much more detail. It is important to notice, that the problem is not solely in technical aspects ranging from the lack of proper encryption in protocols to the poorly configured or non-existing firewalls. It is also in the different culture stemming from the perceived risks, priorities and requirements in the world of industrial control systems and, at the same time, perhaps the lack of understanding of the requirements from those who are working on IT staff or IT security and operating organization’s other networks and services. It is actually likely that the roots of the inadequate cyber resilience of SCADA lie actually there, in the lack of proper co-operation between industrial automation engineers and IT security experts. In many cases, expertise from both sides isn’t properly combined and thus adequately secure industrial control system isn’t created or managed.

These differences in thinking may also be a challenge on a national scale. When governments are now rapidly creating resources and getting understanding of proper cyber defence measures, there may be a risk that SCADA and industrial control systems in general will have a similar fate here. It is true that Finland and many other developed nations have more or less defined critical infrastructure for themselves and cyber defence policies for critical industrial control systems should thus almost automatically apply here and cyber security of control systems will have attention that they deserve. What this would mean in practice, is government support in some form, like the use of expert red teams for evaluation, auditing and giving recommendations for critical ICS operators, but possibly even some form of regulation by the authorities. In Finland, quite an extensive regulation exists for telecommunications operators by Finnish Communications Regulatory Authority (FICORA), operating directly under Ministry of Transport and Communications. FICORA sets the requirements for public- and government networks and services concerning for example electric and physical protection, reliability, performance and security [1]. However, there is no such regulation for critical industrial networks or for organizations operating critical industrial control system networks [11].

3 Remediation and challenges

In September 2002, after the initial turmoil of 9/11 in the United States, President’s Critical Infrastructure Protection Board and the United States Department of Energy Issued a document entitled *“21 Steps to Improve Cyber Security of SCADA Networks”*. It is a simple brochure type document listing few rules in just eight pages, but it is nonetheless easily approachable check list which helps to describe remediation for many of the problems listed in chapter 2. It is not complete by any means, but the list is still valid today more than 10 years after its creation. There are several other similar and more in depth publications or literature which give recommendations for securing SCADA and ICS. One such example is *“Guide to Industrial Control Systems (ICS) Security”* from 2008 by National Institute of Standards and Technology (NIST), which is recommended reading for anyone seeking more in-depth view towards ICS security, but still likes to have the information presented in a quite compact and simple form.

Department of Energy’s document starts with the evaluation of all your connections, disabling unnecessary ones and using demilitarized zones (DMZ) to improve the security of data transfers between SCADA and other connected networks. After this, firewalls and Intrusion Detection Systems (IDS) should be implemented for different point of entries to the SCADA network. [28]

As with the physical connections to other networks, all unnecessary or unused services or features, such as Internet access, email, remote meter reading, billing etc., should be turned off, especially when SCADA system is interconnected with other networks. Those services that are deemed necessary, should be allowed only after careful risk assessment and evaluation weighing benefits and risks. If some services are allowed to or from the outside the SCADA, such as vendor connections to some parts of the system, strong access control methods should be enforced. Here, co-operation with SCADA vendors is important to identify proper secure configurations. [28]

Many SCADA devices also include built in security features, which should be used and system designers should never rely on proprietary protocols offering security. As said, Intrusion Detection Systems should be implemented, but for them to be effective, a 24-hour-a-day incident monitoring and response has to be established. As a part of monitoring, logging should be enabled where possible and a daily review of logs should be performed to find possible suspicious activity as early as possible. Technical audits for the network and devices will help in locating vulnerabilities and “paths of least resistance” in the system that an attacker could exploit. [28]

All aspects suggested in the paper are not fully technical and related to the SCADA system itself. Physical security, especially with remote sites, is also important. Areas like clearly defined requirements, policies and responsibilities, architecture documentation, configuration management processes, risk assessments and recovery plans are equally important for building and maintaining a secure SCADA system. “Red Teams”, which are groups of experts with understanding of the SCADA system and IT security, should be established to evaluate attack scenarios towards the system. [28]

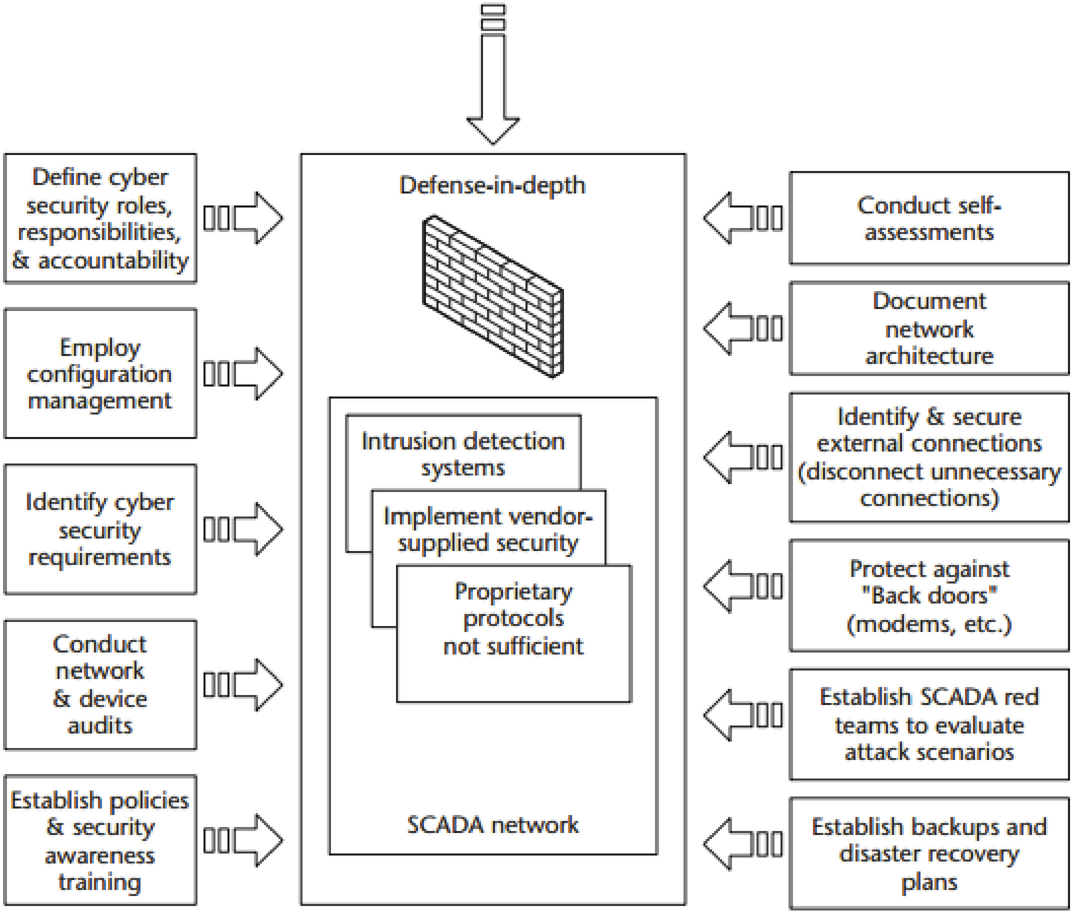

Define cyber security roles, responsibilities, & accountability
Employ configuration management
Identify cyber security requirements
Conduct network & device audits
Establish policies & security awareness training
Defense-in-depth
Intrusion detection systems
Implement vendor-supplied security
Proprietary protocols not sufficient
SCADA network
Conduct self-assessments
Document network architecture
Identify & secure external connections (disconnect unnecessary connections)
Protect against "Back doors" (modems, etc.)
Establish SCADA red teams to evaluate attack scenarios
Establish backups and disaster recovery plans

Figure 4. Graphical summary of 21 steps of SCADA cybersecurity. [9]

As we can see, Department of Energy recommendations for SCADA are very similar compared to pretty much any other information system, and in that sense SCADA and other industrial control systems are very similar. However, especially from technical perspective, building a secure SCADA system with aforementioned recommendations, can easily get quite complicated and problematic.

Encrypted connections such as Virtual Private Networks (VPN) are one of those widely used techniques for creating reliable connections through untrusted networks and as such, they are a possibility for long distance communications with SCADA systems too. Specifications and hardware for different encryption solutions has been developed, but problem is that many widely used public or private key methods would cause too much latency for SCADA operation. Using SCADA protocols over IP adds as much as 30% overhead itself, so added encryption may be just too much. Also, field devices have limits of their own as they are designed to be low-power and reliable, but at the same time they lack the processing power to handle complex encryption or authentication schemes [10]. In addition to that, industrial automation systems tend to have very long working life, for example 10-15 years. Therefore much of the existing equipment might not have any support for encryption and upgrading hundreds or thousands of devices to newer prematurely might prove very expensive. Remote sites use still lots of serial connections within the site and implementing IP-based VPN's there isn't possible at all, so building fully encrypted connections throughout the system is often very difficult. Furthermore, encrypted data traffic becomes essentially opaque to network monitoring and intrusion detection systems. Although encryption can eliminate some vulnerabilities, it should be implemented only after a careful evaluation of operational constraints and network monitoring policies. [30]

We find similar problems easily with other security features. Firewalls, IDS systems and access control functions can also add to the latency of connections and configuring firewalls with large amount of connections and altering them according to a changing threat environment or system architecture can be a big task [9; 17]. Authentication poses another unique challenge for SCADA systems, as user's ability to recall and enter a password may be impacted by the stress of the moment in an emergency situation. Some other methods such as dongles or other similar tokens provide other problems, as there is a possibility to lose the item. Again, authentication schemes may also add to the latency issues in the network requiring processing power and adding length to the messages. Protocols themselves may pose another challenge for authentication: while it would be possible to build proper authentication for operators and technicians, many of the widely used industrial protocols send passwords in clear text format and they don't support any sort of device authentication [10; 17]. All these restrictions should be noted and different authentication methods should be carefully considered in the way that authentication is feasible, but usability of the system from operator stand point of view has to be maintained and the safety or availability of the process isn't endangered in any situation.

4 Situation in Finland and the future

Although description in the end of chapter 2 may give bleak picture about the cyber security situation of industrial control system, it is not the whole truth and in Finland there has been a lot of effort from both industry and government on SCADA and industrial control systems cyber security. The focus of FICORA's cyber security services, mainly that of National Cyber Security Centre Finland, is in the security and reliability of public communication networks and services, which of course more or less indirectly improves also the cyber security of SCADA networks. However, FICORA also has an agreement with National Emergency Supply Agency, which tasks include the maintaining the security of supply stockpiles, guiding the national economy in emergency situations, promoting the readiness planning of companies and ensuring the functioning of the national technical infrastructures [20; 23].

One example of the agreement's results and joint effort is HAVARO system, which is effectively an intrusion detection system offered for supply critical companies in Finland. HAVARO has few shortcomings, such as it only supervises traffic on the edge of Internet and adjoining corporate network. This means practically that everything inside the corporate network is out of HAVARO's reach and networked systems such as SCADA with perhaps of hundreds of connections are not well suited for HAVARO. It is still a step towards right direction and because of National Cyber Security Centre's co-operation with other CERT representatives throughout the world, HAVARO can utilize more current and larger database for threat detection than publically available commercial products. [18]

Security Committee, a permanent and broad-based co-operation body for proactive preparedness working within Defense Ministry, accepted National Cyber Strategy Implementation Guide in 11.3.2014. It lists a total of 74 concrete proceedings to improve cyber security on national level. One of them is the use of HUOVI web portal, which will be developed towards a secure cyber information and situational awareness channel for supply critical companies and government. In the future, platform may be available for all businesses. [7]

On the agenda are also the development of training, research and exercise programmes between the years 2014-2018. To support this, Finnish Information Security Cluster (FISC) aims to establish a national cyber laboratory. There is no timetable for FISC-laboratory in the implementation plan, but its functions include the empowering of the co-operation between cluster companies and different research institutions and, of course, the research of cyber security of different products and services. If and when this laboratory is established, it needs to have the capabilities to test SCADA and other industrial control systems too. As an example from abroad, Idaho National Laboratory in the United States runs National SCADA Test Bed Program. Program was founded by Department of Energy to ensure a secure, reliable and efficient distribution of electric power. Practically it means that the program evaluates selected control systems and control system components to identify cyber vulnerabilities, provides training in workshops and works in collaboration with industry and standardizing organizations. All testing is planned and conducted in collaboration with the interested industry partner and may be performed in the laboratory environment or at the partner’s site. Scale of operation in Finland will be of course smaller, but similar approach is probably required. Research should be also made in collaboration with different academia in Finland, who already have expertise in cyber security and/or industrial control systems, something that has generally been practiced widely in Finland in many fields of research. Close co-operation and information exchange with foreign laboratories, like the one in Idaho, is essential to have the most current information on the subject. National and international co-operation and research programmes are also on the agenda of implementation guide. [7; 14]

Industry has also worked on the industrial cyber and information security. The Finnish Energy Industries (Energiateollisuus Ry) is a sector organisation for the industrial and labour market policy of the energy sector. It represents companies that produce, acquire, transmit and sell electricity, district heat and district cooling and offer related services. One emphasis for the year 2013 were networked control systems, communications systems and cyber security and to promote the theme, a study concerning the cyber security of our networked control systems in the energy sector was made. Study included a web questionnaire for sector companies and specific interviews with different actors on the field, from device manufacturers to telecommunications operators and information security companies. All together 27 companies and government agencies took part in the study. Results were both positive and negative and many challenges cited in this paper are present in the control systems of our electric distribution and production systems. In summary, the total information security levels in the companies generally varied from satisfactory to good according to the study, but the variance in results was large. Because of the public availability of the study, precise analysis about the technical details or recommendations based on findings wasn’t possible, but problems existed in both legacy and more modern IP-based control systems. According to the study, very little 3rd party auditions and evaluation of systems is preformed throughout the industry. Also, non-technical aspects, such as proper background checking when hiring new employees, leaves room for improvement. [22]

As a major recommendation in the study, energy and electric distribution companies should define a broad security policies with one specific area that concentrates on cyber and information security. It is natural to do this as a part with normal continuity planning and risk management so that cyber and information security is properly integrated with management, processes and reporting. Availability of the systems and recovery from the crisis situations should be in the focus, which is very similar to NIST recommendations. With some of the distribution companies, work was done quite well in this aspect, but there is still room for improvement with all the participants. [17; 22]

References

[1] 54 A/2012M. Määräys Viestintäverkkojen ja palveluiden varmistamisesta.

[2] Byres, E. *The air gap: SCADA's enduring security Myth.* Communications Of The ACM, 2013. Vol. 56, No. 8. p. 29-31. ISSN 0001-0782.

[3] Cole, E. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Waltham: Syngress, 2012. 290 p. ISBN 978-1-59749-949-1.

[4] Hagelstam, A. *CIP – kriittisen infrastruktuurin turvaaminen - Käsiteanalyysi ja kansainvälinen vertailu*. Helsinki: National Emergency Supply Agency, 2005. 78 p. ISBN 952-5608-00-X. Available: http://www.huoltovarmuus.fi/static/pdf/243.pdf

[5] Hildick-Smith, A. *Security for Critical Infrastructure SCADA Systems.* SANS Institute. Created 23.2.2005. [Referenced 11.8.2014]. Available: http://www.sans.org/reading-room/whitepapers/warfare/security-critical-infrastructure-scada-systems-1644

[6] Igure, V., Laughter, S., & Williams, R. *Security issues in SCADA networks*. Computers & Security, 2006. Vol. 25, p. 498-506. ISSN 0167-4048.

[7] *Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma.* Security Committee, 2014. [Referenced 25.8.2014]. Available: http://www.turvallisuuskomitea.fi/index.php/fi/component/dropfiles/?task=frontfile.download&id=21

[8] Knapp, E. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.* Waltham: Syngress, 2011. 341 p. ISBN 978-1-59749-645-2.

[9] Krutz, R. *Securing SCADA Systems.* Indianapolis: Wiley Publishing Inc., 2005. 218 p. ISBN 978-0-7645-9787-9.

[10] Larkin, R., Lopez Jr., J., Butts, J. & Grimaila, M. *Evaluation of Security Solutions in the SCADA Environment.* Advances in Information Systems, 2014. Vol. 45, No. 1, p. 28-53. ISSN 1532-0936.

[11] *List of regulations addressed by FICORA* [web page]. Finnish Communications Regulatory Authority. [Referenced 11.8.2014]. Available: https://www.viestintavirasto.fi/en/steeringandsupervision/legislation/regulations.html

[12] *MODBUS Messaging on TCP/IP Implementation Guide V1.0b.* Modbus Organization, 2006. [Referenced: 5.8.2014]. Available: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[13] *MODBUS over Serial Line Specification and Implementation Guide V1.02*. Modbus Organization, 2006. [Referenced: 5.8.2014]. Available: http://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

[14] *National SCADA Test Bed Program* [web page]. Idaho National Laboratory. [Referenced 25.8.2014]. Available: http://www.inl.gov/scada/index.shtml

[15] *OSVDB Vulnerability data base* [data base]. Open Sourced Vulnerability Database (OSVDB). [Referenced 9.8.2014]. Available: http://osvdb.org/search/search?search[vuln_title]=SCADA&search[text_type]=alltext&search[s_date]=Jan%201,2014&search[e_date]=August%2029,%202014&search[refid]=&search[referencetypes]=&search[vendors]=&search[cvss_score_from]=&search[cvss_score_to]=&search[cvss_av]=*&search[cvss_ac]=*&search[cvss_a]=*&search[cvss_ci]=*&search[cvss_ii]=*&search[cvss_ai]=*&kthx=search

[16] Robles, R. & Choi, M-k. *Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems*. International Journal of Grid and Distributed Computing, 2009. Vol. 2, No. 2, p. 27-34. ISSN 2005-4262.

[17] Stouffer, K. & Falco, J. & Scarfone, K. *Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology. 2008. Special Publication 800-82. [Referenced: 3.8.2014]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

[18] Sulankivi, T. *IDS:n käyttöönotto herättää todellisuuteen* [web blog]. KPMG Finland. Hacking Through Complexity. Created 25.4.2013 [Referenced 25.8.2014]. Available: http://www.hackingthroughcomplexity.fi/2013/04/idsn-kayttoonotto-herattaa.html

[19] *Supervisory Control and Data Acquisition (SCADA) Systems*. National Communications System. 2004. Technical Information Bulletin 04-1. [Referenced: 3.8.2014]. Available: http://scadahacker.com/library/Documents/ICS_Basics/SCADA%20Basics%20-%20NCS%20TIB%2004-1.pdf.

[20] *Tasks of National Emergency Supply Agency* [web page]. Emergency Supply Agency. [Referenced 25.8.2014]. Available: http://www.nesa.fi/organisation/national-emergency-supply-agency/tasks/

[21] Tracy, A. & Van, T. *Back Door Attacks: How to protect Serial Communications* [presentation] SEQUI, Inc, 2011. [Referenced 11.8.2014]. Available: https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/F2011/D1-09-0200pm_Track2_Amaio-Van_rr_Title-IEEE1711-2010SecforLegSCADAProt.pdf

[22] *Verkostoautomaatiojärjestelmien tietoturva 2013*. The Finnish Energy Industries, 2013. [Referenced 25.8.2013]. Available. http://energia.fi/sites/default/files/verkostoautomaatiojarjestelmien_tietoturva__2013-09-27.pdf

[23] *Viestintäviraston tietoturvapalvelut* [web page]. Finnish Communications Regulatory Authority [Referenced 25.8.2014]. Available: https://www.viestintavirasto.fi/tietoturva/viestintavirastontietoturvapalvelut.html

[24] Yardley, T. *SCADA: issues, vulnerabilities, and future directions*; LOGIN:, 2008. Vol. 33, No. 6, p. 1-7. ISSN 1044-6397.

[25] Galloway, B. & Hancke, G. *Introduction to Industrial Control Networks* [preprint document]. IEEE Communications Surveys and Tutorials, 2012. [Referenced 11.8.2014]. Available: http://www.rfidblog.org.uk/Preprint-GallowayHancke-IndustrialControlSurvey.pdf.

[26] Hare, F. *The Cyber Threat to National Security: Why Can't We Agree?* [document]. Conference on Cyber Conflict Proceedings, 2010. [Referenced 3.8.2014]. Available: http://www.ccdcoe.org/publications/2010proceedings/ Hare%20%20The%20Cyber%20Threat%20to%20National%20Security%20 Why%20Cant%20We%20Agree.pdf

[27] Meixell, B. & Forner, E. *Out of Control: Demonstrating SCADA Exploitation* [presentation]. Cimation Inc. Black Hat 2013. 2013. [Referenced 14.8.2014]. Available: https://media.blackhat.com/us-13/US-13-Forner-Out-of-Control-Demonstrating-SCADA-Slides.pdf

[28] *21 Steps to Improve Cyber Security of SCADA Networks* [document]. U.S. Department of Energy, 2002. [Referenced 18.8.2014]. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

[29] Coates, G. & Hopkinson, K. & Graham, S., & Kurkowski, S. *A Trust System Architecture for SCADA Network Security.* IEEE Transactions On Power Delivery, 2010. Vol 25, No.1. p. 158-169. ISSN 0885-8977.

[30] Fink, R. & Spencer, D. & Wells, R. *Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems* [document]. U.S. Department of Energy, 2006. [Referenced 18.8.2014]. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/1-NSTB_Control_Systems_Security_Standards_Accomplishments_and_Impacts.pdf

Electric Power as Critical Infrastructure

Kimmo Heinäaro
Finnish Defence Research Agency
kimmo.heinaaro@mil.fi

Abstract

Purpose

Modern society is increasingly dependent on electric power. Without power, almost all functions of the society halt in a time frame from seconds to days. The aim of this research is to describe technical structure of the Finnish power grid and find vulnerabilities either for natural phenomenon or deliberate damaging of the system. Potential targets for physical or cyber attacks are recognized.

This study is based on public sources available on literature or the Internet. Based on the study, it seems that the importance of the power grid is widely recognized even in the media. Power companies are minimizing risks, but there is still a lot to be done.

1 Introduction

Modern power system consists of power plants producing the electric power, nationwide power grid delivering the electricity and consumers using the power.
Historically, producers and consumers of power were at first located close to each other, the power grid didn't exist. Local power plants produced electricity to a city or factory nearby. [29] History of the Finnish power grid goes back almost a hundred years. Construction of the first modern high voltage line Rautarouva (Iron Lady) between Turku, Helsinki and Viipuri was started in 1925. Nationwide power grid is a basic infrastructure and a very long term investment. This becomes obvious with the fact that the Rautarouva line powered up in 1929 is still partly operational (Figure 1). [22] Very few technical systems can reach a life cycle that long (except railways or Roman aqueducts).

Electric power is a basic necessity for a modern society. Without power almost all other services and infrastructure cease to operate. Power failure causes an immediate stop of [17]:

- most of public transportation (trains, metro, trams)
- commerce (most shops, banks, ATM's, petrol stations)
- infrastructure (water, heating)

Some services might have capability to survive some hours or even some days [17]:

- Vehicles will operate until fuel runs out
- Food stocks will last some days without fridges and freezers
- Communications (cell phones, Internet, IT) will partly be operational even some days on backup power
- Emergency infrastructure (hospitals, emergency centres) will run on backup power until fuel runs out.
- In winter, buildings without a backup heating system will be frozen in a matter of days

As those figures above state, power is among the most critical infrastructures in our world today. Lack of power stops the whole society and has big and fast economic impacts. In 2003, a large blackout in north eastern USA and Canada affected 50 million people lasting two days. Estimated cost of the blackout was between 7 and 10 billion USD. [11]

In chapter 2 of this paper, the technical structure of the Finnish power grid is described. Understanding the technical principles of the system is important to be able to evaluate possible vulnerabilities. Basic structure of the power system has been the same for almost a hundred years. In the near future we will see largest changes in the history of the grid because of renewable energy and globalisation. Future of the power system is described in Chapter 3. Due to the long history of power systems, operators are quite well aware of dangers related to natural phenomenon. Still, even nowadays, storms, tsunamis, flooding etc. can cause a lot of damage to the power system. On the other hand, deliberate attacks to power systems are a new threat. Natural and man made threats are studied in Chapter 4 of this paper for both present and future power systems.

Figure 1. Rautarouva, 110 kV line in Riihimäki. Photograph: Heinäaro, Kimmo

2 Finnish Power System

2.1 Technical Background

Modern power system in any country can be divided into three main parts:

- Power plants producing the electrical power. These can be far away from consumers.
- Network connecting producers with consumers. This network consists of several layers serving different areas and distances.
- Consumers of electricity. These could be anything from ordinary households to large manufacturing plants.

Power can be produced from lots of different sources that are not described here. Main focus in this chapter is to describe the structure of the network between producers and consumers. Understanding the technical principles of the network is important when considering possible vulnerabilities.

The fundamental starting point of developing a power system is Ohm's law:

$$I = V/R,$$

where I=Current, V=Voltage, R=Resistance

Another important thing to remember is the electric power equation:

$$P = UI,$$

where P=Power, U=Voltage, I=Current

All materials used in the wiring of a power network have resistance (except superconductors) that causes energy losses according to Ohm's law and the power equation. Part of the energy transferred will warm up the wire. When transferring lots of power from a power plant over long distances to consumers, these thermal losses are significant. In addition to costs, too much thermal loss will eventually melt the wire. To reduce losses, high voltages and thick wiring (less resistance) are used for long distances. High voltage means long safety distances, for example higher pylons supporting the wires. Thick wiring means more material costs for wiring. End result when planning a transmission line is always a compromise between losses and costs. [9] Superconductors don't have resistance and hence no thermal losses, but the core of the cable must be cooled down near absolute zero temperature with e.g. liquid nitrogen. Superconductors can transfer higher power levels than a copper wire equal size, but some of the power is lost for cooling the cable (Figure 2). [10]

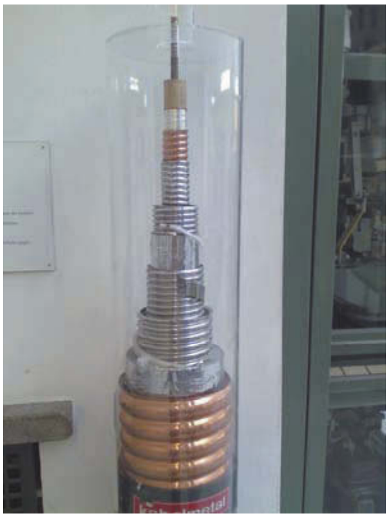


Figure 2. Superconducting power line (60 kV, 1000 A) in Deutches Museum. Photograph: Heinäaro, Kimmo

For the technical reasons described above, power network is hierarchical (Figure 3). For long distances high voltage lines are used. High voltage is transformed to a smaller voltage in a power substation serving a certain area. This is further reduced in several stages when approaching the consumer and finally the household voltage of 400 / 230 V in Europe. [4]

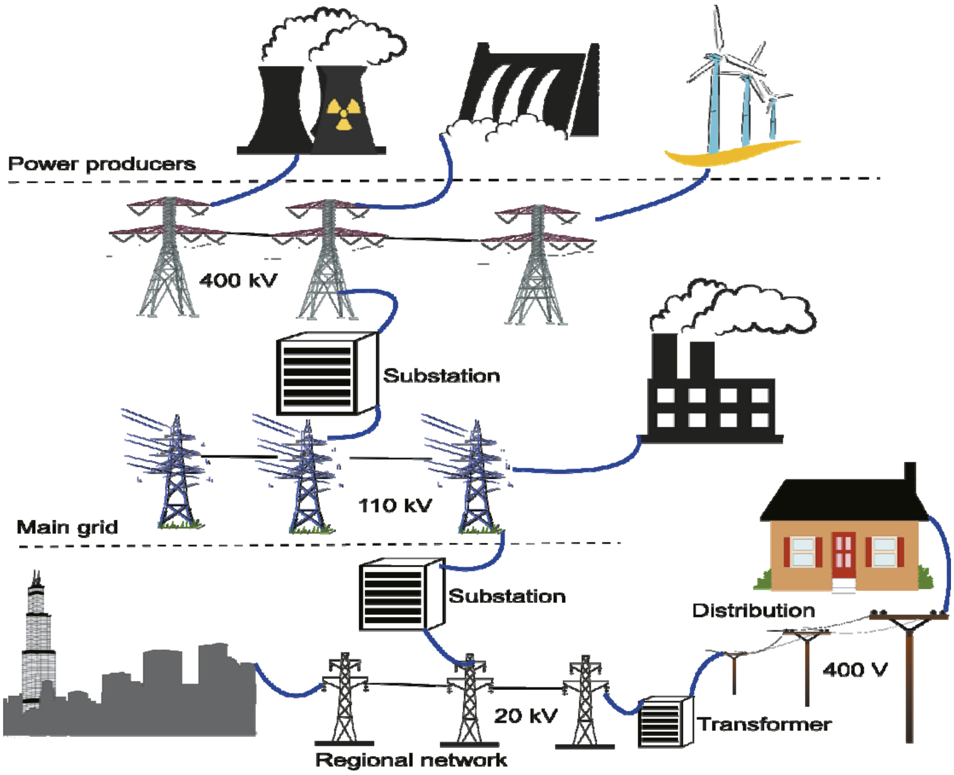


Figure 3. Principle of Finnish Power System

For easy voltage conversion through all the voltage levels of the transmission network, AC (Alternating Current) is used. DC (Direct Current) is used mainly for extra long distances or international transfer of power. AC requires synchronizing all producers of electricity to the frequency and phase of the network (50 Hz in Europe, 60 Hz in USA). There is no storage of power in the network (except kinetic energy stored in generators); production and consumption must be in balance at all times. If production is larger than consumption, the frequency of the network will start rising (generators in power plants will rotate faster). If consumption is larger than production, frequency will fall. Production and transmission of power requires constant monitoring and tuning to keep it in balance. Some types of power plants can be adjusted rapidly (e.g. hydroelectric power). Some are slower to adjust (e.g. nuclear power plants). For instant adjustment of power produced there are spinning reserves (running, but on partial production power) in the network. For peak load situations there are standing reserve units ready to be started. There are also predefined consumer loads that can be disconnected if necessary. Maintaining reserve units is expensive and the fuel they use is more costly (e.g. diesel). Electricity produced with reserve units is more expensive compared to other means. For this reason, power companies will try to minimize the need for standing reserve units and their use. [1]

For adjusting the power production, there must be controlling station(s) in the network. Controlling station is constantly aware of consumption and forecast of consumption days ahead. It controls production, import, export and routing of power in the transmission lines. To achieve this, real time information of all parts of the network and remote control of devices and plants is needed. Management station uses industrial control systems to monitor and control the network (SCADA, Supervisory Control and Data Acquisition). [6]

Power systems nowadays are no longer national only. Electric power is constantly crossing borders of countries. All national operators will buy the power needed at any moment from the most economical source, either domestic or foreign produced. This must of course happen within limits of power line transmission capacity. Transmission of power across borders can be DC to separate networks of neighbouring countries or it can be AC when networks are synchronized together. 24 countries in continental Europe are connected together to form the largest synchronous grid in the world (Continental Synchronous Area). [4]

2.2 Finnish Power System in Practice

Main sources of electricity in Finland are nuclear power (27%), hydroelectric power (15%) and biomass (13%) according to 2013 statistics. Import of power was 19 % of total consumption in 2013. Finnish specialty in production of energy is Combined Heat and Power (CHP). In cold Finnish climate it is economically reasonable to combine production of both heat and electric power from the same fuel in the same plant. Waste heat from production of electricity is used for district heating. Accommodation of almost half the population is heated by district heating and about 80% of production of district heating is combined with generation of electricity. CHP production is economical and emissions are lower compared to separate production of heat and power. This is achieved with the high efficiency of CHP plants, which might be up to 90% compared to 45 % of ordinary power plants. Load following hydroelectric power plants are the main spinning reserve in Finland to adjust for variations in the consumption of power. Other means for spinning reserves are import of power and CHP plants. [5] Fast standing reserve units include diesel and gas turbine plants. Slow reserves include plants powered by coal, oil or peat. There are also contracts with heavy industry (wood, chemical, metal) to disconnect some loads in case of need to stabilize the network. [4]

The Finnish power network consists of the main grid, regional networks and local distribution networks. Main grid is operated by Fingrid Oyj, established in 1996. Main shareholder of Fingrid is Republic of Finland (55% of votes). Fingrid is responsible not only for the national main grid, but also international connections. Finnish main grid is part of the synchronized inter-Nordic network of Northern Europe (eastern Denmark, Finland, Norway and Sweden). Additionally, there are DC connections to Estonia, Sweden and Russia. Finnish main grid is not part of the European Continental Synchronous Area, but there are DC links between inter-Nordic network and the continental network (Figure 4). [4]

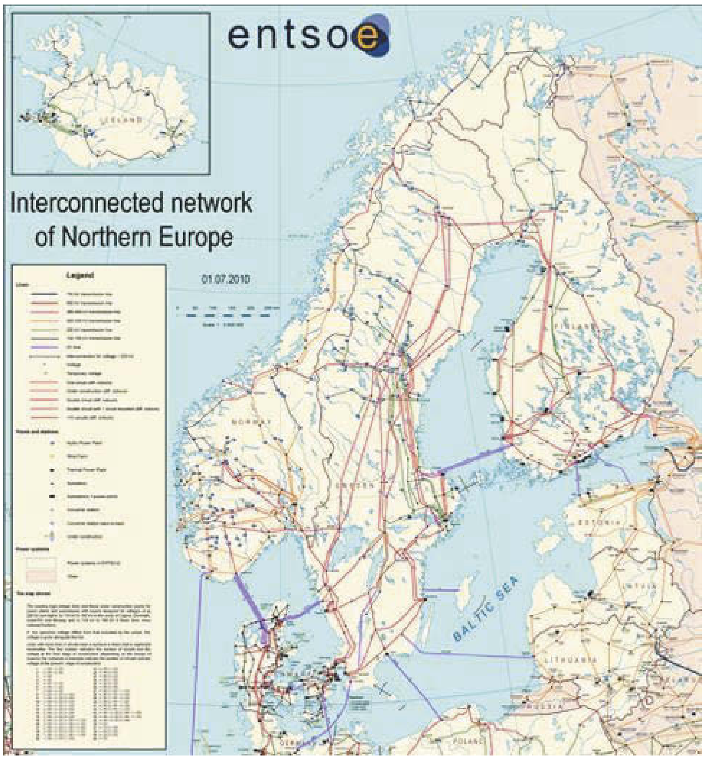


Figure 4. Inter-Nordic transmission grid [4]

The main grid in Finland consists (Figure 5) of [4]:

- 4500 km of 400 kV lines
- 2300 km of 220 kV lines
- 7500 km of 110 kV lines
- 113 electric substations.

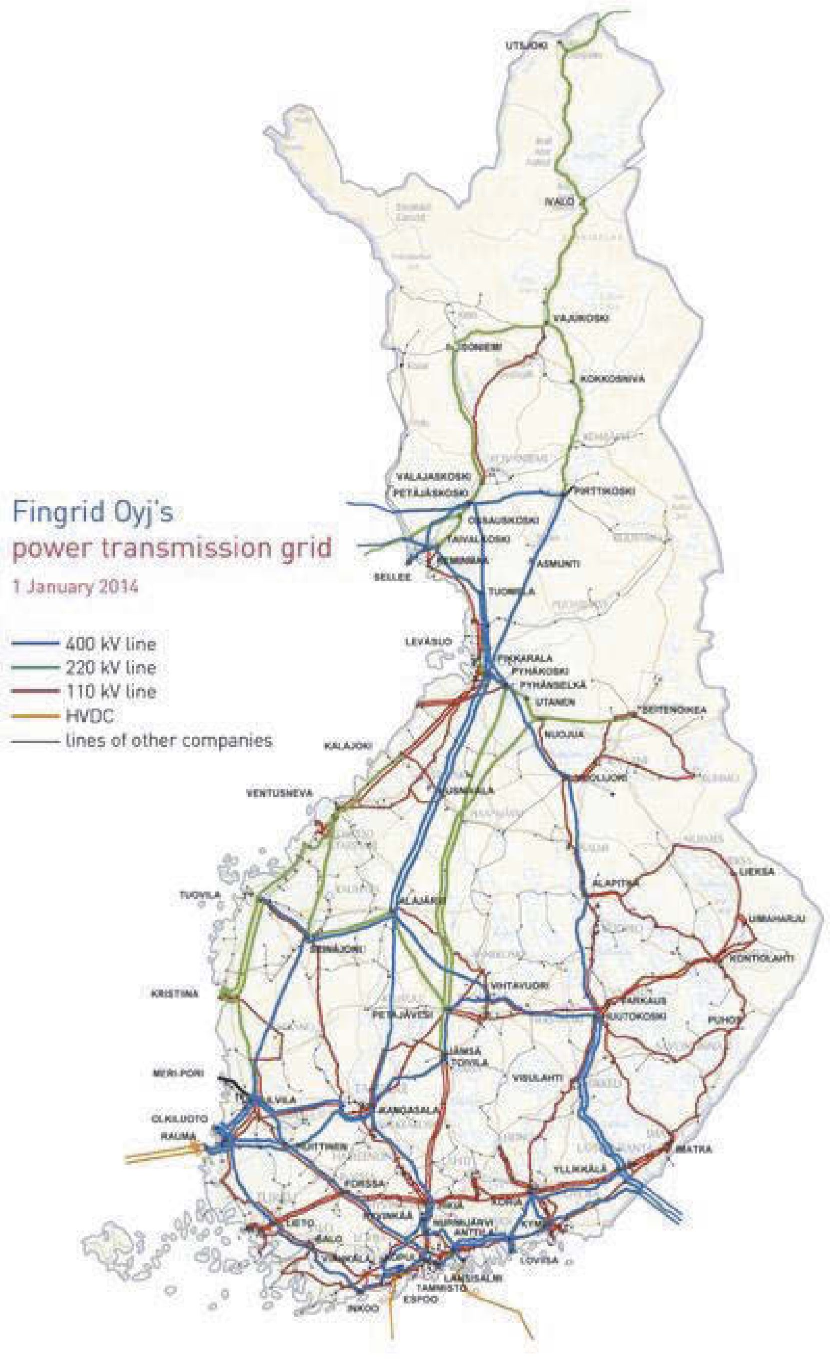


Figure 5. Finnish Main Power Grid operated by Fingrid [4]

The Finnish (and Nordic) power system is planned using the N-1 security criteria. This criteria means that any single fault, like disconnecting any producing unit (even the largest 1200 MW nuclear power plant) or any transmission line from the grid shall not produce any large impact in the network. Only local disturbances are allowed. After 15 minutes, the grid shall withstand another N-1 fault. In Finland, largest single fault would be 865 MW (power of one unit in Olkiluoto nuclear power plant). This will increase significantly after powering up the third unit in Olkiluoto (1600 MW). [1] The main grid in Finland is a looped (mesh) network to achieve backup routes. Loops exist also in regional networks, but backup routes are only connected when necessary. Also distribution networks are looped in towns, but in rural areas networks are normally radial, there are no backup routes, for economic reasons. [9]

Frequency of the network should remain within 49.9 - 50.1 Hz (Nordic Grid Code). This is normally achieved with frequency controlled spinning reserves. When frequency of the network falls below 49.9 Hz, fast reserves are automatically deployed. Slow reserves are manually started in 15 minutes to release fast reserves for the next use. Goal is to keep frequency over 49.5 Hz even when a large power plant is suddenly disconnected from the grid. [12]

3 Future of Electric Power Systems

Technical structure of power systems has remained static for almost a hundred years. In the near future, however, there will be major modifications in the whole infrastructure. Of course, Ohm’s law and Euros spent will still dictate the framework to work within. These are some new trends that will affect the power infrastructure:

- Smart grid
- Renewable energy
- Globalisation of power systems
- Distributed generation of power
- Electric vehicles.

3.1 Smart Grid

Smart grid is a modern version of the power grid. Exactly the same wires for transporting energy can be used in a smart grid than in a traditional grid. The “smart” grid is created with the aid of Information and Communications Technology. Old manually operated and mechanical components (kWh meters, switches, circuit breakers etc.) of the grid are changed to remote readable and controllable units. Key issue in a smart grid is two way communications between components. Another important element is the “smart meter”. Old on-site readable meters are replaced by smart meters that can communicate with the network manager (Figure 6). A smart grid also has sensors to measure voltage, phase, stability etc. in multiple locations of the network. These sensors can for example provide real time information to network management, reduce effects of faults, automatically isolate faulty circuits and make more efficient use of the network. [5]

Smart meters can enable variable pricing of power. Goal is to cut peak consumption that is produced in reserve power plants with costly fuel. Disconnecting secondary loads could even be done automatically through the smart meter. It is also possible to use smart meters two ways: to buy power from the grid or to sell power to the grid. It is possible to collect e.g. solar power locally and feed surplus to the national grid. [5]

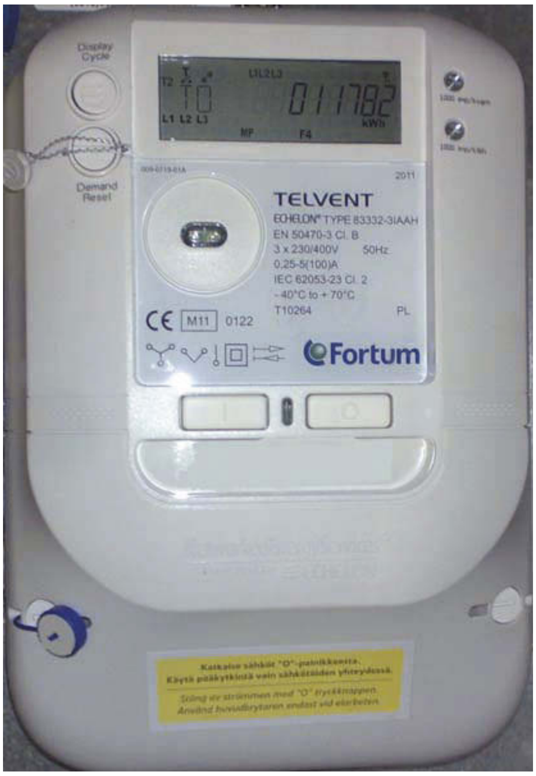


Figure 6. Smart meter, Photograph: Heinäaro, Kimmo

3.2 Renewable Energy

In order to reduce emissions from fossil fuel and reduce dependence on foreign energy, EU has a target to produce 20 % of energy from renewable sources by 2020 [3]. Another boost to renewable energy in Europe is decision of German government to close all nuclear power plants by 2022 [28].

Renewable energy has been used in power production for a long time. Traditional renewable sources of energy are hydroelectric power and biomass. New growing areas for emission free power are solar and wind energy. These are typically produced in large farms connected to the power grid. These energy forms however have one major drawback: the production is not continuous. Sun isn’t always shining or the wind may calm down. Connection to the power grid must be made according to the peak power of the farm, although the average power is far from it. To compensate variations in production, there must be enough power reserves available in the grid.

3.3 Power System Globalization

There is a trend to further interconnect national grids together both physically and economically. In EU goal is to achieve European market for power by the end of 2014. European market aims to lower costs, increase reliability and reduce need for expensive reserve power. [4]

A very large grid can compensate differences in renewable energy production: it is probably always windy somewhere in Europe. When stretched over several time zones, the peak consumption hours in one zone can be covered by excess power from another. There are some projects that aim to produce large quantities of solar power in Sahara and export it to Europe with high voltage DC connections or even superconductors [2; 16; 23].

In USA, the national power grid is divided to four separate synchronous areas: Eastern Interconnect, Western Interconnect, Texas Interconnect and Quebec Interconnect. [11] Project Tres Amigas plans to connect three of these grids together in New Mexico. The superstation planned will use superconducting cables and high voltage DC between areas. [10]

3.4 Distributed Generation of Power

Distributed Energy Resource (DER) means producing power locally in small scale. This could mean a few photovoltaic cells in a household, or larger farms. These systems can be used for local use only or they could be connected to the national power grid (Feed-in Tariff, FIT) [18]. Distributed production has potential to become the biggest change in power system infrastructure in its hundred years of history. In several countries cost of solar power (calculated over the full lifetime of the equipment) compared to retail cost of power has reached equality. This point of equal costs is called ‘grid parity’. Below grid parity, consumers will get cost reductions by installing their own power production. This could eventually lead to massive distributed production of power. Distributed energy production is even compared to replacing wired phones with mobile phones. Power companies might become producers of backup power only, for night time and cloudy days. Net flow of power to a large number of consumers would be zero or even negative. [13]

3.5 Electric Vehicles

Number of electric cars will undoubtedly increase fast in the near future. Charging of electric cars will require a whole new infrastructure based on power grids, not tank trucks. Electric cars can be charged slowly over several hours from an ordinary wall socket. This is however not always possible, also fast charging stations are needed. Fast charging means high voltage DC of 50 kW's or more. With this amount of power, it is possible to load the battery for additional 100 km in less than 30 minutes. A charging station with several charging sockets will need a lot of power during peak hours of the day. [15]

According to calculations done, even large numbers of electric cars should have no affect on the main power grid, but local delivery networks might get congested. Smart grids should be deployed to reduce peak power, not to charge large number of electric cars at exactly the same time after working hours. [14]

4 Threats and Risk Mitigation in a Power System

Natural phenomenon or deliberate damaging can affect any part of a power system. Possible threats to power producing plants, power transmission network and the network management system are described in this chapter. Threats to consumers of power are not studied in detail. Consumers should however be aware and prepare for a possible blackout in the power grid. For Finnish households there exists a guidebook from the Finnish Ministry of Defence giving advice how to survive a long lasting blackout [17]. Companies should also make calculations of risks and costs involved. Backup power is easily available as UPS devices or generator systems. In all preparations for producers, network operators or consumers, it is necessary to calculate costs of problems and costs of preparations. It is economically impossible to prepare for everything, but it might be economically wise to invest for some level of backup in the most critical components. For example, a household might have just enough backup power for the pump of central heating system to keep the house warm burning logs. For companies, data or a web shop might be the most valuable asset to keep intact using geographical decentralization.

4.1 Threats to Power Plants

Power plants are of course critical components in a power system. Disconnecting a single power plant (even the largest nuclear plant) from the grid, however, shouldn't even be visible to consumers. There are power reserves available, both domestic and imported. Threats to power plants include natural phenomenon: storms, tsunamis, flooding, earthquakes, volcanoes etc. and human actions: user error, terrorism, cyber attacks.

Large plants are fairly easy to protect cost effectively against all imaginable threats. Problem is that all possible threats cannot be imagined. In Fukushima, the nuclear plant survived an earthquake and loss of connection to the grid, but failed when a tsunami wave destroyed the backup generators. Combination of three simultaneous problems was not predicted. [20] In Chernobyl, a user bypassing security systems added with severe design faults in the plant caused the accident [7].

Large plants are heavily guarded making them hard targets for terrorists. In Finland, nuclear power plants are protected with for example vehicle barriers, electric fences and armed guards [31]. On the other hand, small plants might be unmanned, but their importance to the grid is negligible.

Cyber attacks are a new threat to power plants as well as other networked systems. Aurora Generator Test done in 2007 at Idaho National Labs demonstrated that it is possible to actually physically destroy a big diesel generator by a cyber attack. Attack was used to control a circuit breaker between the generator and the power grid. By opening and closing a circuit breaker without synchronizing the generator to the grid, caused mechanical overload and destruction of the generator. [24] Protecting a power plant from cyber threats is similar to protecting any other industrial facility. Cyber threats to power infrastructure are further studied in chapter 4.3 of this paper.

4.2 Threats to Power Grid

According to chapter 2.2, there are 14000 kilometres of high voltage lines in the Finnish main grid. In addition to the main grid, there are lots of regional and distribution lines. It is obviously impossible to guard every pylon of these lines. Deliberate attacks against the wiring however aren’t very effective. The main grid is a mesh network: damaging one line doesn’t affect delivery of power. Even if some local delivery networks aren’t looped, damaging them only causes local problems and can be quite quickly repaired.

Main threats to the wiring of the grid are caused by natural phenomenon. The main grid in Finland should be protected from trees falling by maintaining a treeless corridor around the lines. Still, sometimes trees are falling even on the main grid [4] Lower voltage lines are not so well protected. They can be affected by falling trees, storms, heavy snow or lightning. Accidental man made threats include excavators cutting underground cables or loggers cutting trees over power lines. Storms can cause large scale destruction and blackouts that can take several days to repair. A new law was passed in Finland in 2001, after two storms caused blackouts (lasting up to a week) for 800000 customers. It mandates power companies to compensate customers in blackouts lasting more than 12 hours. The goal is to make power companies invest in faster recovery times. [27]

Best way to prepare for both natural and man made threats for wiring is to use underground cables instead of overhead wires. Storms, falling trees, lightning or snow won't affect cables hidden underground. Underground cables cost more, but are a useful alternative when replacing old distribution or even regional networks. Using cables for main grid however is challenging because of much higher costs and electrical qualities of cables (higher reactive power compared to overhead wires). [4]

Critical points for man made damage in a power system are the junction points of the network: power substations. They convert voltage levels and / or route power between transmission lines. Substation typically contains large transformers and a switchyard (Figure 8). It is normally unmanned and remote controlled. Transformers used in the substations are big, heavy and expensive. Delivery time for replacing such transformers could be months and power companies are reluctant to invest in spare units. [11] Natural phenomenon threatening substations are for example storms, flooding and lightning. Man made threats include user errors, terrorist attacks and cyber attacks. In California it was reported that a group of snipers using AK-47 assault rifles destroyed 17 large transformers in Metcalf power station causing damage worth millions of dollars. Attack took only 19 minutes and snipers disappeared before the police arrived. [19]

Substations are very easy to locate, they are large and quite visible. It is also easy to find them from online services. In Figures 7-9, the address of a random substation was checked from Fingrid online map service. Based on the address, photograph and satellite image of the station were fetched from Google Maps. It is difficult to protect the substations from deliberate physical attacks; it would be very costly to guard them all the time. At the moment there is no obligation for power companies to stock spare transformers either. [30] When calculating risks and costs involved in key components of the network, power companies and government have somewhat different equations. For example, keeping spare transformers in stock is a big investment for a power company, spares are probably never needed and biggest financial threat is compensation to customers. For a society, cost of a transformer is negligible compared to costs of a large long term blackout.

4.3 Threats to Network Management

A power system needs constant adjustment of production level and routing in the grid. This requires a Network Management system using industrial control (SCADA) to monitor and control all parts of the network. Also, all trends of future power systems described in chapter 3 have one thing in common: more communications and smart remotely controlled components are required. Communications is ever increasing in power systems, but these SCADA systems are vulnerable to several threats. Natural phenomenon like storm and lightning can cut communications or destroy remote devices. Man made threats include user errors, terrorist and cyber attacks.

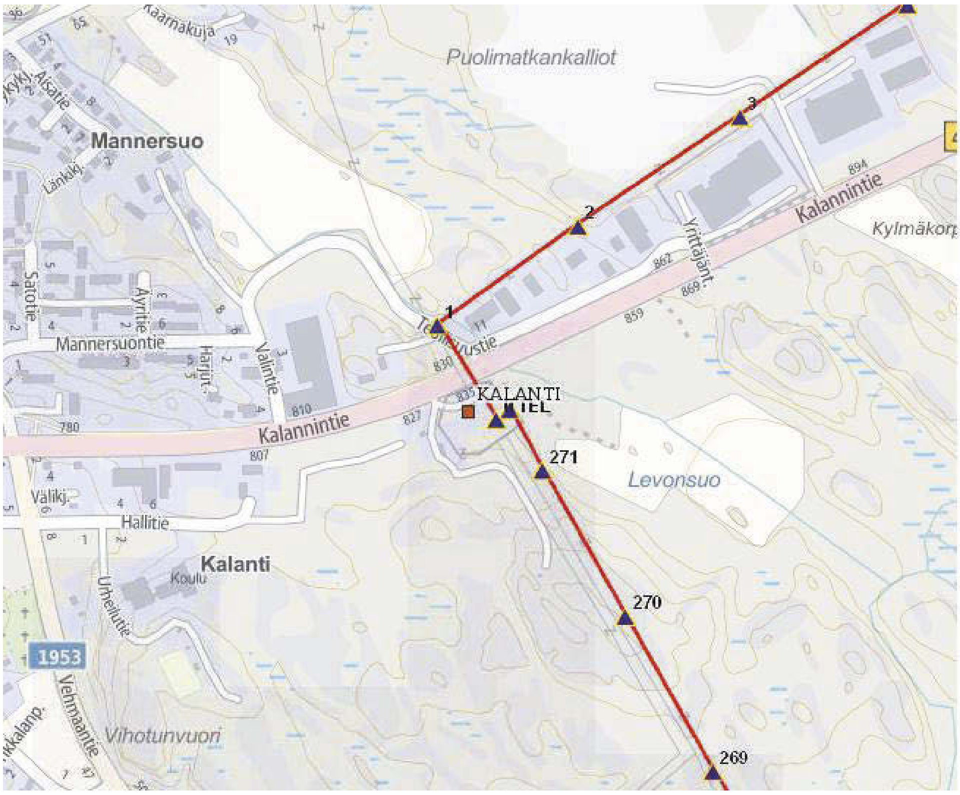


Figure 7. Map location of a power substation. Screenshot: Fingrid Map Service

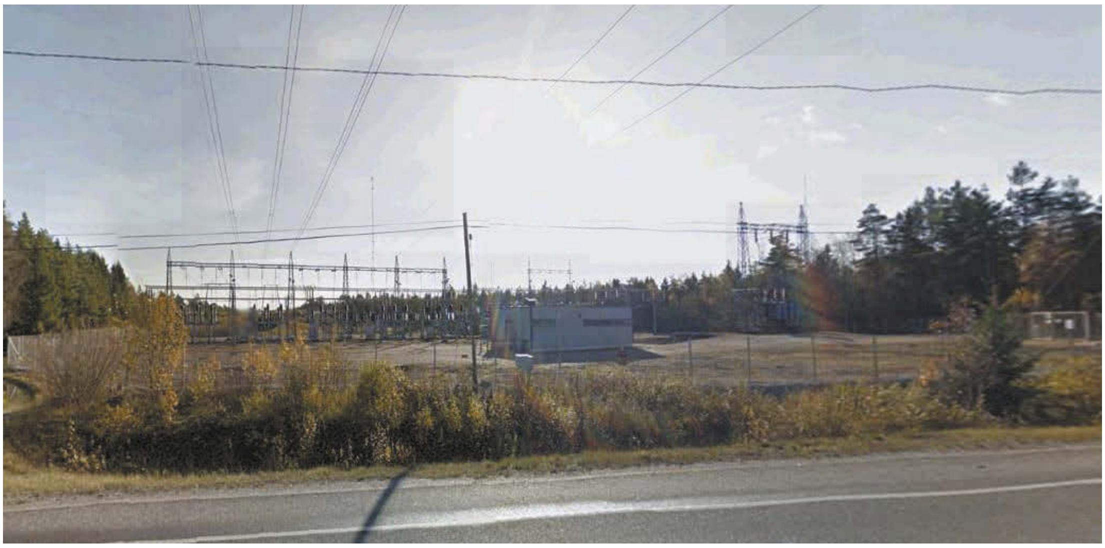


Figure 8. Photograph of a power substation. Screenshot: Google Streetview

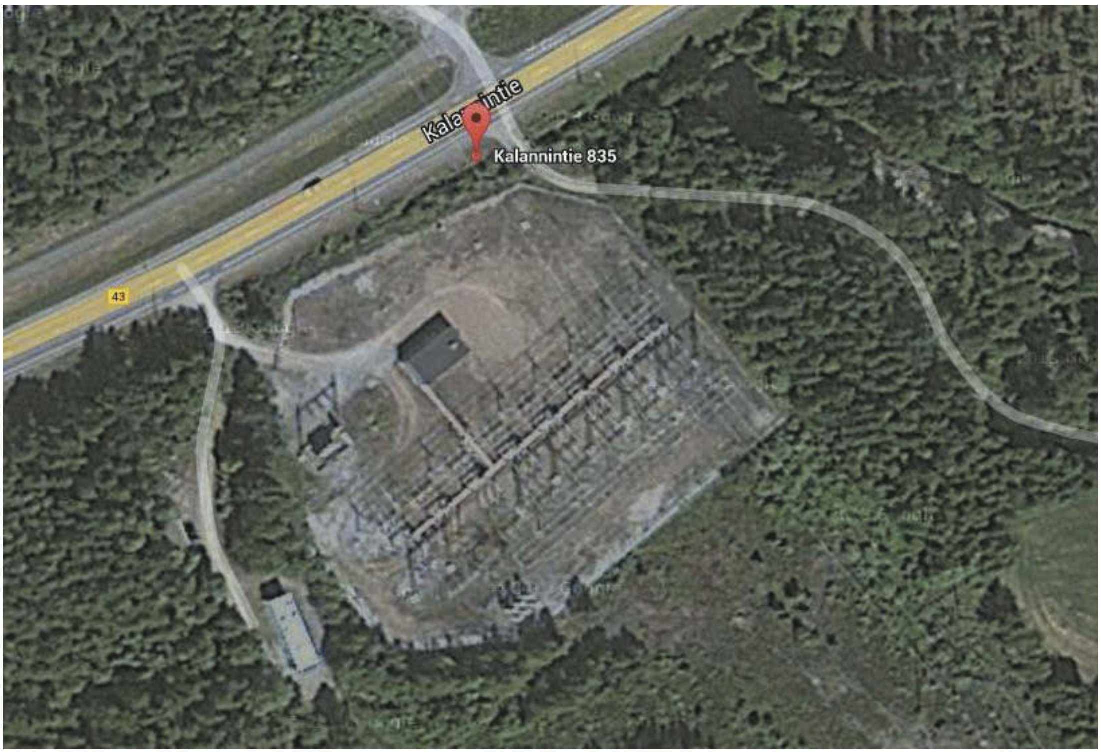


Figure 9. Satellite view of a power substation. Screenshot: Google Maps

Large power plants are in theory relatively easy to protect against cyber attacks, because they are manned and contained in a single geographical area. Possibly the whole industrial network of the plant is inside a secure area. Normal precautions apply: air gapped (physically isolated) production network, defence in depth, firewalls, IDS and IPS systems and good security policy. Despite all the precautions above, these systems aren't totally safe. Malware called Stuxnet successfully targeted an air gapped industrial control system in Iran through an infected usb memory in 2010. Such tailored attacks with detailed inside knowledge of the plant cannot be prevented with ordinary measures. [25]

Opposite to power plants, components of the power grid are geographically distributed all over the country. All remotely controlled sub stations and other devices need some communication channel. Lots of these components are located in unguarded locations in possibly far away sites. According to a survey among Finnish power companies in 2013, there are currently several possible vulnerabilities in the SCADA power networks. About 60% of companies surveyed allow remote connections to power control systems from a vendor network or even home computers of employees. 60% of companies interviewed don't use encryption when communicating with remote controlled stations. On the other hand, 75% of companies are planning to improve their SCADA systems in near future. [21] In 2014, over thousand energy companies in 84 countries were found to be infected by malware called Dragonfly or Energetic Bear. Software was designed to spy target systems and had capability to grant control of the SCADA system to the attacker. The malware was delivered with updates to SCADA software. [26]

SCADA of power systems is problematic regarding cyber attacks because the systems are very heterogeneous: there are devices from a long time period, there are lots of protocols used, geographical distribution is at least nationwide and lots of companies are involved. Smart grid brings a new set of challenges by combining all these together. Making them interoperable is a challenge on its own and adding cyber security to the whole system is costly. To protect systems from advanced attacks, security must be considered at all levels, there is no single device or box that keeps the attackers outside. [8]

Some countermeasures to protect power systems from cyber attacks are (in addition to traditional firewalls and virus scanners) [8]:

- Defence in depth. Multiple layers of security should be used. This might be challenging in the extremely heterogeneous power grids.
- All communications should be encrypted. This can be a challenge with embedded remote controlled devices demanding low latency communications and with limited processing power. At least whitelisting (checking running processes to be legitimate) should be used.
- Situational awareness. Abnormal actions in the network should be detected through advanced network monitoring. This can be achieved automatically by checking logs and events.
- The whole supply chain of both hardware and software should be checked. It is possible to get embedded malware or backdoor directly from a vendor. The vendor could be compromised or even malicious itself.
- Smart grid standards for security should be followed; in USA: NISTIR 7628 Guidelines for Smart Grid Cyber Security, in Europe: M/490 Smart Grid Mandate

5 Conclusion

Electric power is widely recognized as a critical infrastructure of a modern society. During the whole history of power systems, there have been attempts to protect the infrastructure from natural elements. But even recently, nature has shown its power. Natural disasters like storms or tsunamis can destroy our power infrastructure in large scale. Man made attacks, both physical terrorist and virtual cyber attacks are a relatively new phenomenon. Protecting the vast power grid from physical attacks it was never designed for, is a challenge both technically and economically. At least key components of the network should be recognized, protected and precautions should be made in case of their destruction. Cyber attacks in a very complex and rapidly developing industrial network of power systems are another challenge. Security should be considered at all levels from hardware components to applications. On the other hand, in a power consumer perspective, distributed generation seems a promising way to reduce risks of power failures and eventually even reduce costs of energy.

References

[1] Ahonen, Lauri. *Häiriöreservit*. Project report. Tampere, 2007. Tampere University of Technology, Faculty of Electrical Engineering

[2] Desertec. *The Desertec Concept*. In: http://www.desertec.org/consept cited August 27th 2014

[3] European Commission. *Energy: What do we want to achieve?*. In: http://ec.europa.eu/energy/renewables/index_en.htm [cited August 14th, 2014]

[4] Fingrid Oyj. *Fingrid - Home*. In: http://www.fingrid.fi [cited August 27th 2014]

[5] Finnish Energy Industries. *Energiateollisuus*. In: http://energia.fi [cited august 27th, 2014]

[6] Holmgren, Mikko. *Power regulation resources required by wind power in Finland and regulation characteristics of power plants*. Master's Thesis. Espoo, 2008. Helsinki University of Technology, Faculty of Electronics, Communications and Automation

[7] International Atomic Energy Agency. *INSAG-7 The Chernobyl Accident: Updating of INSAG-1*. Vienna: 1992.

[8] Knapp, Eric D. & Samani, Raj. *Applied Cyber Security and the Smart Grid*. Syngress, 2013.

[9] Korpinen, Leena. *Sähkövoimatekniikkaopus*. Tampere: TTKK, 2008

[10] Korteila, Maria. *Toimii ilman teoriaakin*. Tiede, 2011. Vol. 4, p. 32-35.

[11] Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security*. USA: John Wiley & Sons Inc., 2006

[12] Luukkonen, Juho-Tuomas. *The Impact of Storms on Wind Power Production in Finland*. Master's Thesis, Espoo, 2012. Aalto University, School of Electrical Engineering

[13] Martin, Richard. *Distributed Generation Poses Existential Threat to Utilities*. Forbes, 2013. August 26th

[14] Masoum, Amir S. & Moses, Paul S. *Impacts of Battery Charging Rates of Plug-in Electric Vehicles on Smart Grid Distribution Systems*. In: Innovative Smart Grid Technologies Conference Europe, Gothenburg, 11-13 October 2010

[15] Mauri, Giuseppe & Valsecchi, Antonio. *The Role of Fast charging Stations for electric Vehicles in the Integration and Optimization of Distribution Grid*

with Renewable Energy Sources. In: Integration of Renewables into the Distribution Grid, CIRED 2012 Workshop, Lisbon, 29-30 May 2012

[16] Medgrid. *Medgrid Project.* In: http://www.medgrid-psm.com/en/project cited August 27th 2014

[17] Ministry of Defence. *Pahasti poikki.* Puolustusministeriö, 2008

[18] Ministry of Employment and the Economy. *Feed-in tariff of renewable energy*. In: https://www.tem.fi/en/energy/renewable_energy_sources/feed-in_tariff_of_renewable_energy [cited August 27th 2014]

[19] Mufson, Steven. *Why an AK-47 may be a bigger threat to the electricity grid than a cyberattack.*. The Washington Post, 2014. February 7th. In: http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/07/why-ana-ak-47-may-be-a-bigger-threat-to-the-electricity-grid-than-a-cyberattack/ [cited August 27th 2014]

[20] Nielsen. Rolf Haugaard. *Fukushima*. Tieteen kuvalehti, 2011.Vol 15

[21] Reneco. *Verkostoautomaatiojärjestelmien tietoturva 2013.* In: http://energia.fi/sites/default/files/verkostoautomaatiojarjestelmien_tietoturva_2013-09-27.pdf [cited August 27th 2014]

[22] Riihimäki. *Rautarouva-johtolinja.* In: http://www.riihimaki.fi/Riihimaki/Tekninen-keskus/Kaavoitusyksikko/rautarouva-johtolinja [cited August 14th 2014]

[23] Sahara Solar Breeder Foundation. *Sahara Solar Breeder Foundation Official Website*. In: http://www.ssb-foundation.com [cited August 27th 2014]

[24] Salmon, Doug et al. *Mitigating the Aurora Vulnerability With Existing Technology*. Schweitzer Engineering Laboratories Inc, 2009

[25] STUK. *Stuxnet loi kyberturvallisuudelle uudet vaatimukset.* In: http://www.stuk.fi/ajankohtaista/artikkelit/fi_FI/artikkeli-stuxnet-loi-kyberturvallisuudelle-uudet-vaatimukset/_print/ [cited August 27th 2014]

[26] Symantec Security Response. *Dragonfly: Cyberespionage Attacks Against Energy Suppliers.* Symantec, 2014

[27] Valtiontalouden tarkastusviraston toiminnantarkastuskertomus 176/2008, *Valot päällä Pohjolassa.* Helsinki: Edita Prima Oy, 2008

[28] Wikipedia. *Nuclear power phase-out*. In: http://en.wikipedia.org/wiki/Nuclear_power_phase-out cited August 15th 2014

[29] Wikipedia. *Suomen sähköverkko*. In: http://fi.wikipedia.org [cited August 14th 2014]

[30] Yle. *MOT - Suomi polvilleen 15 minuutissa.* March 11th 2013, In: http://yle.fi/aihe/artikkeli/2013/03/08/suomi-polvilleen-15-minuutissa-kasikirjoitus [cited August 15th 2014]

[31] Yle uutiset. *Ydinvoimaloita suojataan järein asein.* In: http://yle.fi/uutiset/ydinvoimaloita_suojataan_jarein_asein/5548520 cited August 15th 2014

Improving Situational Awareness of Critical Infrastructure with Common Cyber Picture

Jussi Timonen
Finnish National Defence University
Jussi.timonen@mil.fi

Abstract

Cyber operations are developing rapidly among the armies. The need of consistent and comprehensive Common Operational Picture (COP) is a fundamental need in performing the operations, but the implementation such is not straightforward. Situational Awareness of cyber environment proposes multiple challenges to the automation as well as the personnel using the information. The challenges lie in possibilities of gaining the needed information from physical systems as well as from the network itself. From the critical infrastructure point of view the challenges exists in the entire society. The actor making decision, based on national cyber situation awareness, needs the information from multiple sources, including industry entities, in an easily understandable form.

The concept of Common Cyber Picture (CCP) is created by combining several information sources using information integration and fusion. The environment is multisensory; the information can be e.g. from information networks, industrial automation systems, physical sensors as well as from electric systems. CCP includes only high level information because it is a tool for high level observation and decision making. If the need for accessing the detailed raw data exists, it will be collected using on demand service provides by the sources. In another words, the system needs to be scalable. The displayed information is to be arranged into a layers which can be filtered based on geographical locations, logical system views and according to industry branch (e.g. all the water supplier companies). In the advanced applications the CCP system is capable to support threat analysis and visualize the results.

The desirable result of the integration and visualization of the CCP answers at least to the questions; “What is happening in critical infrastructure” and “what is the state of our capabilities”. Based on the derived information it is possible to make decisions and expand the scope from situational awareness into a decision making system.

This research presents the Situational Awareness of Critical infrastructure and Networks (SACIN) framework for gathering the information from the entities, means for information fusion of such information, and finally presents the initial version of user interface.

Keywords

Cyber, Situational Awareness, Decision making, Cyber Common Operational Picture

1 Introduction

Understanding the status of the network and connected devices is not an easy task, especially if the need for national or global situational awareness is taken into consideration. The concept of critical infrastructure broadens the scope by introducing the end product deliverables, such as electricity or water, into to the theatre. The traditional way of understanding the cyber usually focuses on networking devices and tools. This approach is not wide enough from the perspective of national common cyber picture, which aims to provide an up-to-date picture of critical infrastructures which are heavily bounded to networks.

The perspective of different entities changes the approach to Situational Awareness (SA) applications and especially command systems. The military, government and industry have different approaches to situational awareness of systems. One thing that is common to all, is the need for secure their own processes; in industry level this means unstopped business, but in government level it is the continuous operation of society. The Common Operational Picture (COP) alone does not present a durable solution for the society’s needs. Command and Control (C2) is needed in order to effect to the situation. When C2 and COP are combined in cyber environment the system becomes a tool for decision making which is the desired endpoint.

Definition of Common Operational Picture

A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called COP. [1]

Definition of Command and Control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. [2]

Critical infrastructure

is a term used by governments todescribe assets that are essential for the function ing of a society and economy. [3]

The research questions for the research are:

- Is it possible to create a combined national cyber Common Operational Picture?
  - With what kind of high level architecture can be created to support national CCP?
  - Is it possible to present Common Cyber Picture in a feasible manner?

This study mainly focuses on the first sub question and presents one solution based on multiple layers of services which are able to create and share the information. Moreover, the focus is in planning architecture, which is able to support dynamic adjustment of data amount. The idea is not to use so called Big Data solutions, but to limit the information to status information and create an on-request link for the components for more accurate information. The fundamental component of Situational Awareness of Critical infrastructure and Networks (SACIN) is built on top of services and it is in fact the service itself. Even the approach has influences from Service Oriented Architecture (SOA), it is not bound to SOA ideology. The SACIN system is planned as a reusable component for different levels. Different instances are able to access and discover the services provided by others and increase the abstraction level. In many cases the systems are created as an endpoint for all information. That is not the case in SACIN; the idea is to expand the information gathered to the services in the next levels.

The planned system focuses on answering the question “What is happening in critical infrastructure?” The answer could have the perspective of a specific industry branch, similar systems (components), national infrastructure, etc.

The limitations for this study include the risk of attack towards the created system and user access management of the created services. It is recognized that solutions for improving the reliability exists such as in [4], but it is not the key area of research. The study focuses on investigating a concept, not to deliver a product.

2 Overall description

The information levels used be the system varies from data to information. The SACIN presents a framework, which is able to transfer the simplified information from sensor to the integration service. The framework supports information from multiple different sensors and also presents the user interface for operation center as well as simplified interface for browser users. The framework implements Joint Directories of Laboratories (JDL) model from levels 0 to 2 and also creates a platform for 4 and 5. The implementation of JDL model to cyberspace has been studied in [5; 6]. Complex event processing (CEP) framework is able to provide improvement capabilities to JDL model and improve accuracy [7]. Figure 1 below presents the JDL model adopted with the CEP component.

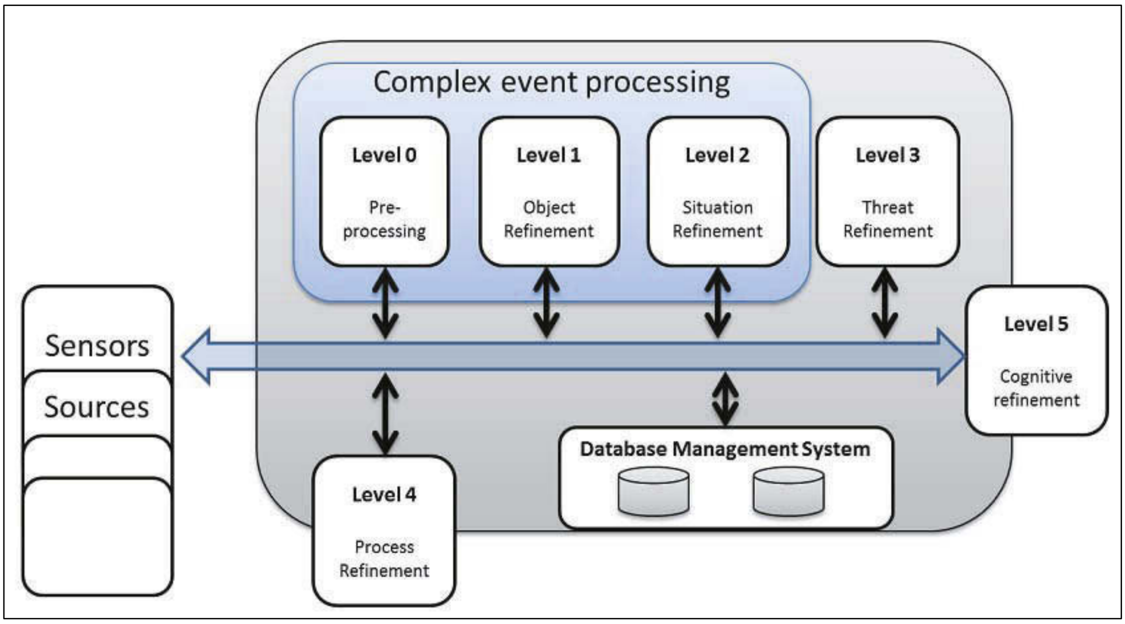


Figure 1. – JDL and CEP adapted from [7-9]

The framework uses client-server connections from the sensor entities to the SACIN services. The SACIN includes multiple services which the passive services are able to discover and start sharing. The active services can be for example an external database containing the information which is accessed through web service. In the figure 2 the overall description is presented.

The process of information delivery is based on service discovery from which the connecting services are able to find the services provided by the SACIN. Moreover, the entities using the services (Operation center & Mobile application) are able to detect the information source. The framework hosts two different types of information in terms of gathering method; active or passive. Active methods include operations from the SACIN framework, such as invoking a service which will deliver service availability information. These active services will publish a description to the service discovery component from which it is possible to automatically start using new services. Passive methods from the SACIN point of view includes services such as intrusion detection systems (IDS), which will provide the information when something happens or it is needed. This is enabled by providing a service which the individual components can discover and start sharing.

The framework is built to support the combinations of multiple SACIN instances for sharing the information. One possible use case would be to build and independent SACIN for water delivery and independent SACIN for electricity systems. These two components contain the sources for their own needs and then publish the result as a service using service discovery. When the national wide component is starting to combine the information it will use the provided services and create a higher level presentation of the situation. This framework is presented in figure 3. Any SACIN system can consist of multiple lower level implementations where operators are focusing on specific problems (such as IDS detections) and then contribute to the next level of abstraction.

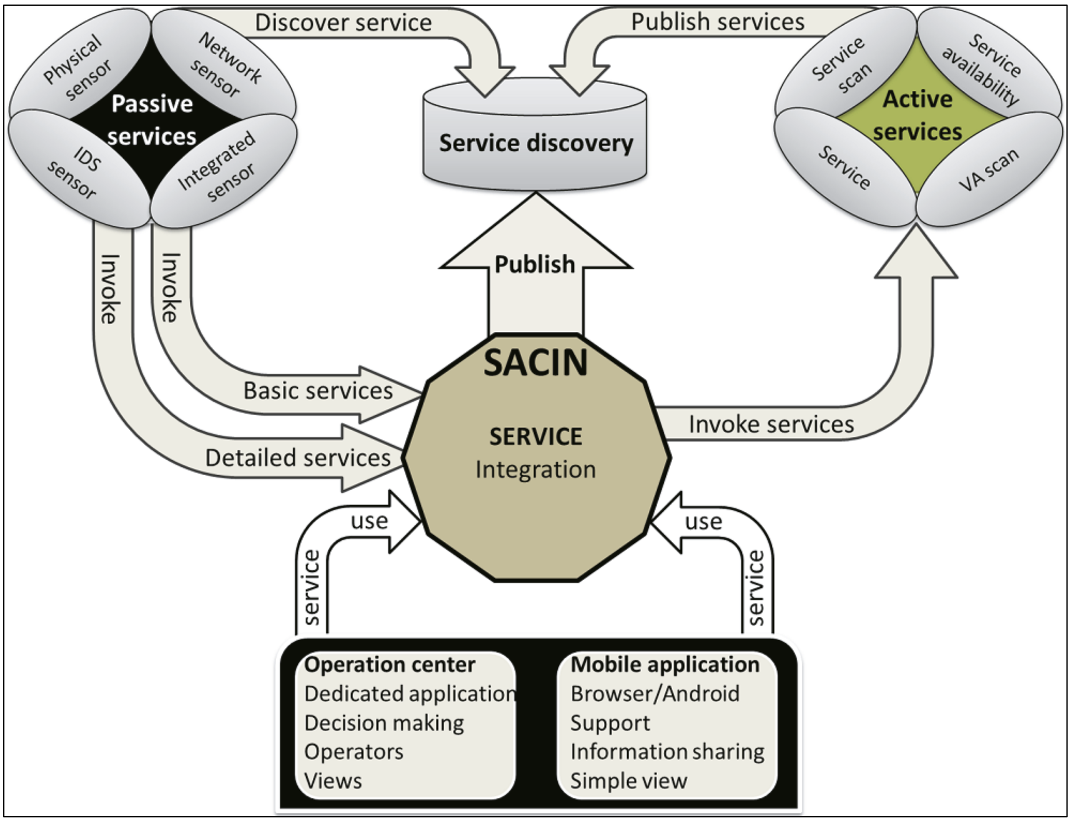


Figure 2. Overall system

3 Information sources

A precondition for system supporting situational awareness is the accessibility of source information. In this case there are two types of information in terms of collection method; active or passive. The fundamental difference is that active entities use on-demand services when passive systems enable push type of operation (see figure 2).

2.1 Active methods

Active methods are services provided by an independent entity, which is able to publish the services and perform specific tasks which require larger amount of CPU power when compared to passive services. These services can be tailored solutions inside corporate network or external services open to everyone. In figure 4 the basic architecture is presented. In fact, the SACIN can be an active service itself as described in earlier paragraphs.

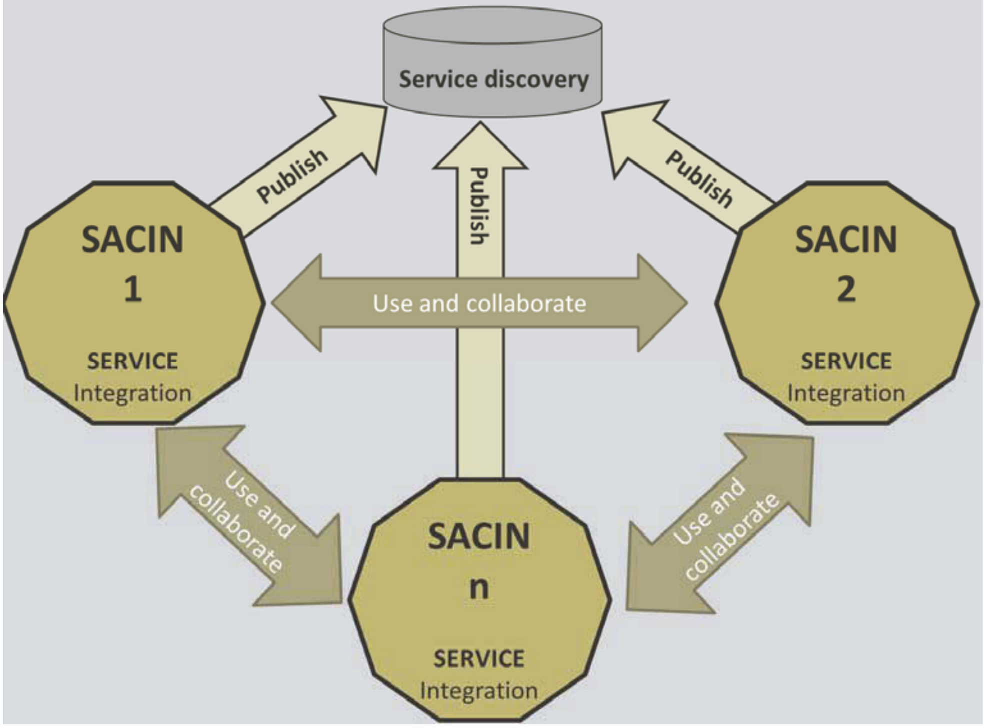


Figure 3. Relations

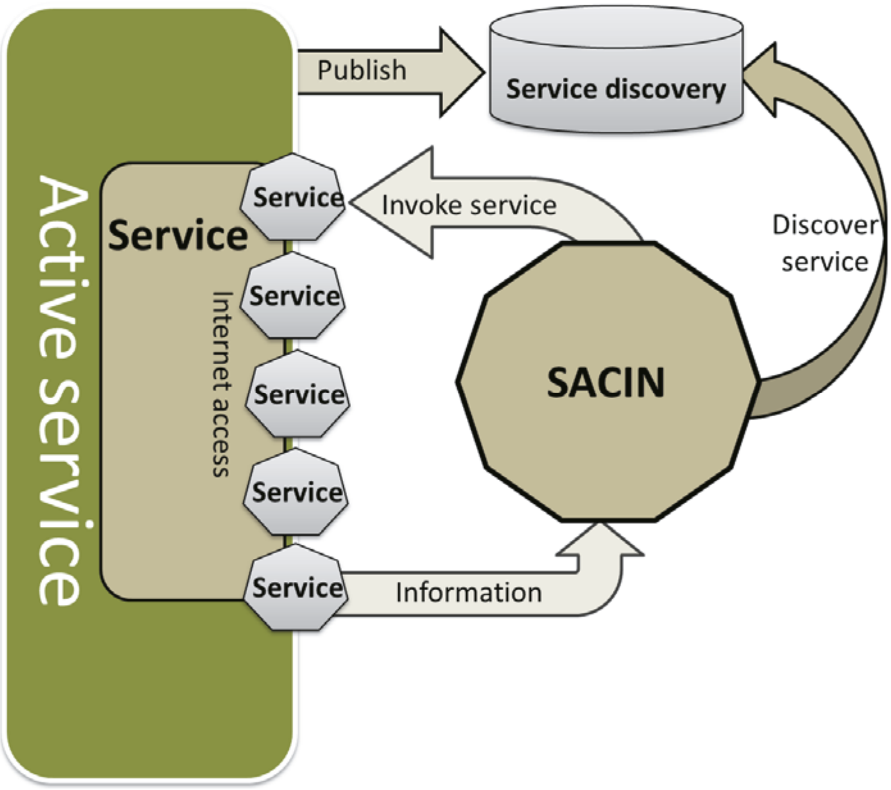


Figure 4. Active services

An example of an external system requiring relatively lots of power would be an environmet tailored to scan industrial automation systems vulnerabilities constanly. This component can publish the results of the constant scan when it is requested by SACIN. A component for this purpouse is partially presented in [10]. Recognized active services are presented in table 1 below.

Active services		
Service	**Purpouse**	**Estimated update frequency**
Service availability	Detect if a selected service is running and accessible	1 minute – 60 minutes
Route discovery	Detect if multiple important routes are in use	1 minute – 60 minutes
Open source Systems	Honeybot detection, incidents, virus detections	Less than minute
Vulnerability scan	Detect vulnerable systems in public networks	1 minute – 60 minutes
Vulnerability Analysis	Estimate risk of a specifi event	30-300 minutes

Table 1. Active methods

2.2 Passive methods

Passive methods create the backbone of the SACIN by producing the largest part of the information. The amount of these sensor can be large (e.g. 10 000 and more) depending the entity being tracked. Passive services deliver the information when an incident has happened. The figure 5 presents the architecture of the services. The main difference between the active services is the way of publishing. The SACIN publishes the services, which can be used by the passive services (see also figure 2). This enables the use of extremely light weight solutions without any server running in the passive device. At the same time all the clients are able to reconfigure automatically if SACIN changes the way or place where it publishes services. The passive service also has means to deliver more accurate information to SACIN on request. The information can be for example log files from specific time frame or service functionality history information.

A central component in passive services is the stand alone component, called the agent, created to fit in the needs of industrial automation management system or just for on-off type of sensor. This component can be installed to a generic framework and it will use interface to receive information from the system. The most simplified information which is delivered is the red-green-blue presentation of the state of the system. The agent also implements the gateway and dictionary for transferring log files. The agent can also store the history information in several ways for later use. The final solution could take advantage on peer-to-peer (P2P) solution, which enables the probes to connect to each other and deliver the information using a network of agents.

As presented in the figure 5 the SACIN consist of services which can be published throught the service discovery to all the entities. Table 2 presents the possbile components providing the information.

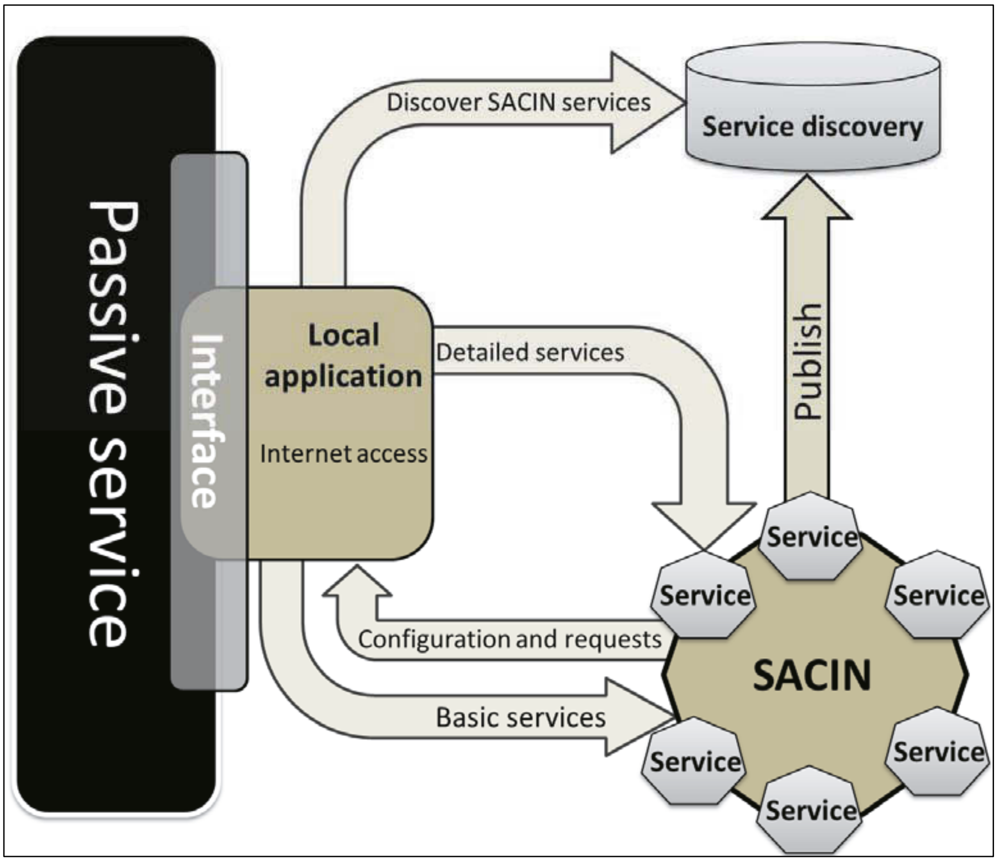


Figure 5. Passive services

Passive services		
Service	**Purpouse**	**Estimated update frequency**
Intrusion Detection System (IDS)	Detect harmfull traffic from network traffic and inform	On incident
Intrusion Protection System (IPS)	Detect harmfull traffic from network traffic and inform and also react on detected traffic	On incident
Firewall	Report intrusion or scan attempts	On incident
Honeypot	Report detected malicious activity inside honeybot	On incident
Agent	Attach to the component or system being supervised and report status and provide on-request data	On incident

Table 2. Passive methods

3 Agent

The purpose for the agent is to provide the needed information for SACIN. The point where the agent will be deployed is a management component in an industrial automation system or similar. The agent is not designed to be deployed in a low level device, such as IDS, but to the component controlling a group of devices.

The figure 6 describes the agent attachment to the target system. All the black boxes are entities where SACIN does not have visibility or control. As can be seen from the picture an important part is the plugin component, which in fact provides information from the target system. This component will be built by a domain expert and it will take care of gaining and calculating system status (e.g. Red-Green-Yellow) and providing log files based on dictionary created by the domain expert, which is bound to the specific generic dictionary advertised by SACIN. The only information which is delivered automatically is the status information. Log files are available only on request and maintained in the agent database for later use.

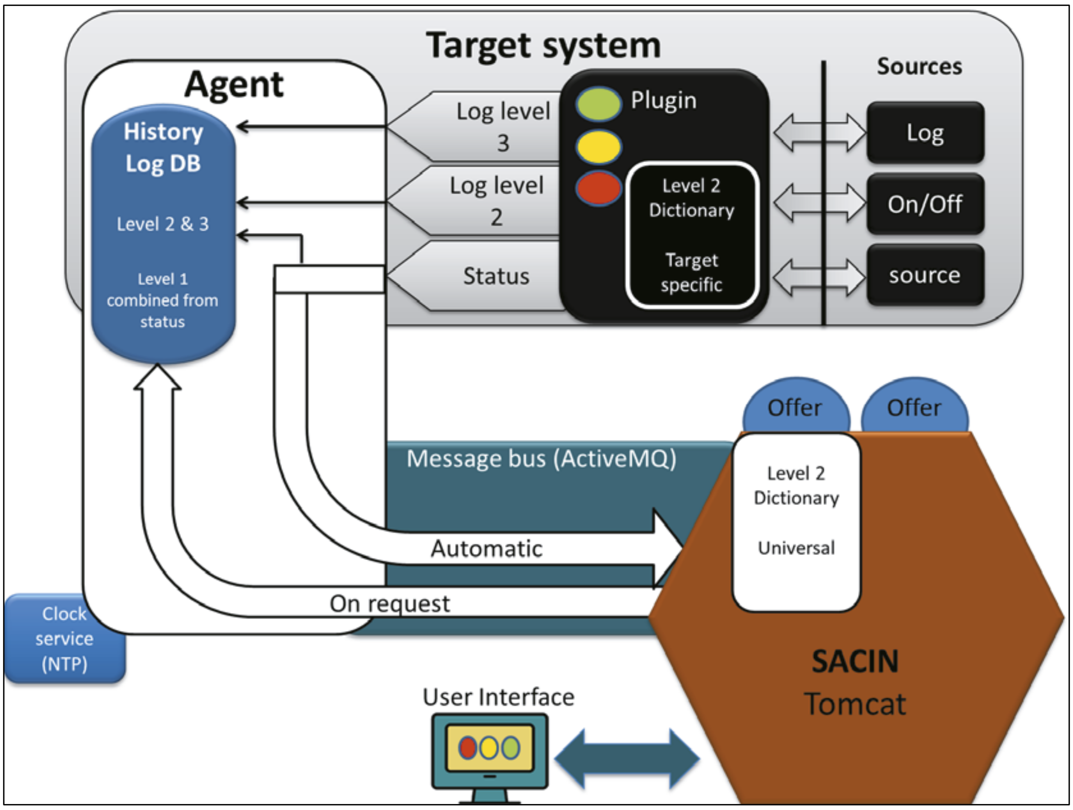
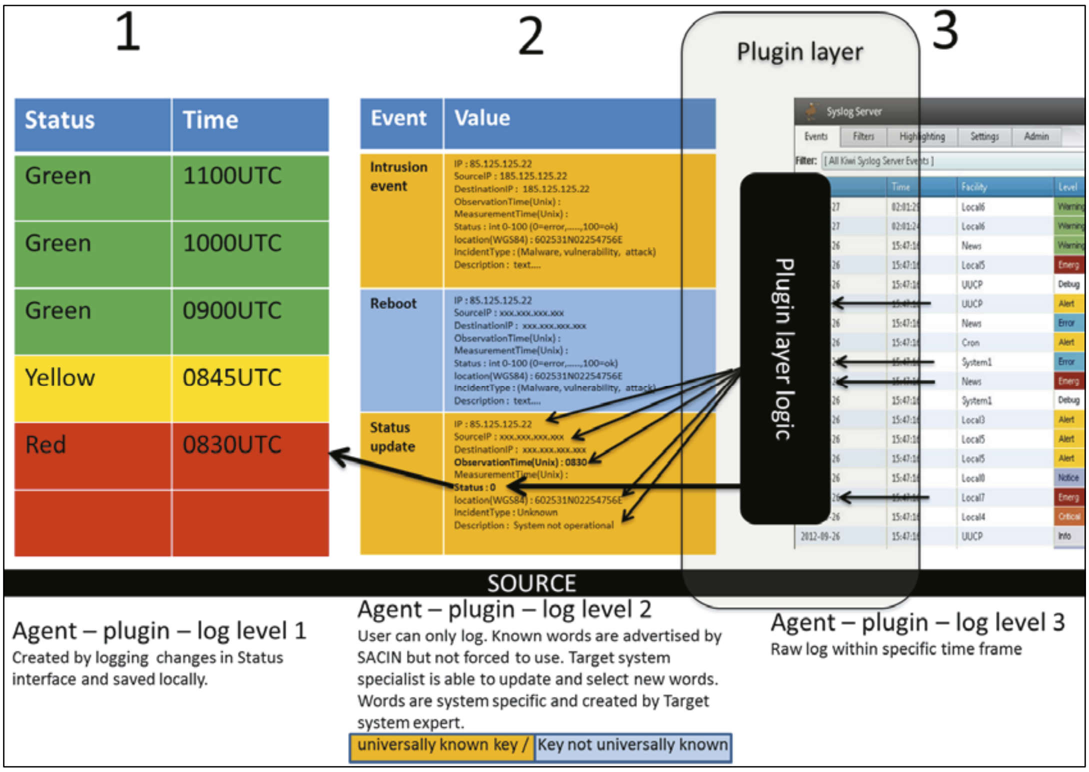


Figure 6. Agent

The agent is capable to deliver four types of information to the SACIN; status information (red, yellow, green), log information from status, log information based on known dictionary and raw log data from the system. The time used in the delivered log files can contain the original time stamp, but it is also bound to a time synchronized from a Network Time Protocol (NTP) server. The log sources are divided to three different classes as presented in figure 7.



Status	Time
Green	1100UTC
Green	1000UTC
Green	0900UTC
Yellow	0845UTC
Red	0830UTC

Event	Value
Intrusion event	IP : 85.125.125.22 SourceIP : 185.125.125.22 DestinationIP : 185.125.125.22 ObservationTime(Unix) : MeasurementTime(Unix) : Status : int 0-100 (0=error,.....,100=ok) location(WGS84) : 602531N02254756E IncidentType : (Malware, vulnerability, attack) Description : text....
Reboot	IP : 85.125.125.22 SourceIP : xxx.xxx.xxx.xxx DestinationIP : xxx.xxx.xxx.xxx ObservationTime(Unix) : MeasurementTime(Unix) : Status : int 0-100 (0=error,.....,100=ok) location(WGS84) : 602531N02254756E IncidentType : (Malware, vulnerability, attack) Description : text....
Status update	IP : 85.125.125.22 SourceIP : xxx.xxx.xxx.xxx DestinationIP : xxx.xxx.xxx.xxx **ObservationTime(Unix) : 0830** MeasurementTime(Unix) : **Status : 0** location(WGS84) : 602531N02254756E IncidentType : Unknown Description : System not operational

Agent – plugin – log level 1
Created by logging changes in Status interface and saved locally.

Agent – plugin – log level 2
User can only log. Known words are advertised by SACIN but not forced to use. Target system specialist is able to update and select new words. Words are system specific and created by Target system expert.
universally known key / Key not universally known

Agent – plugin – log level 3
Raw log within specific time frame

Figure 7. Log classification

3.1 View

The first level of information used by the system is presented in three states; operational (green), disturbance detected (yellow) and not operational (red). The relations between different entities can be taken into account by presenting a relation link with colour using similar codes as presented earlier. This relation can be saved in the definition of service and presented to the user using filter for the purpose. The simplified symbols are presented in figure 8.

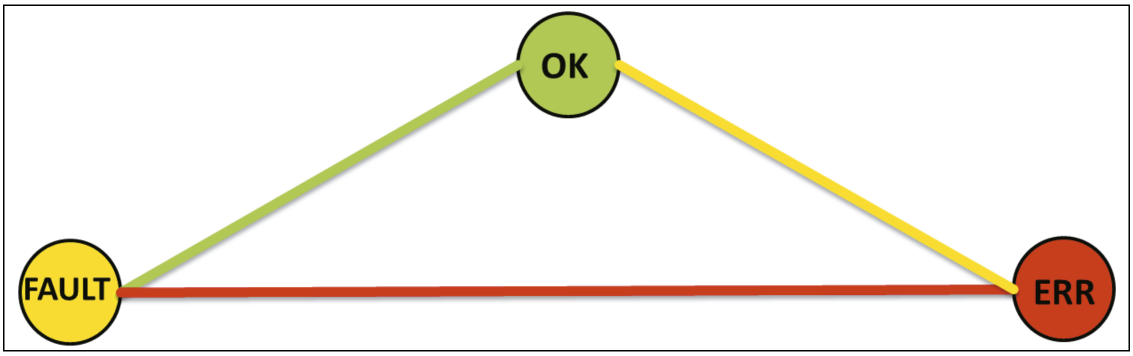
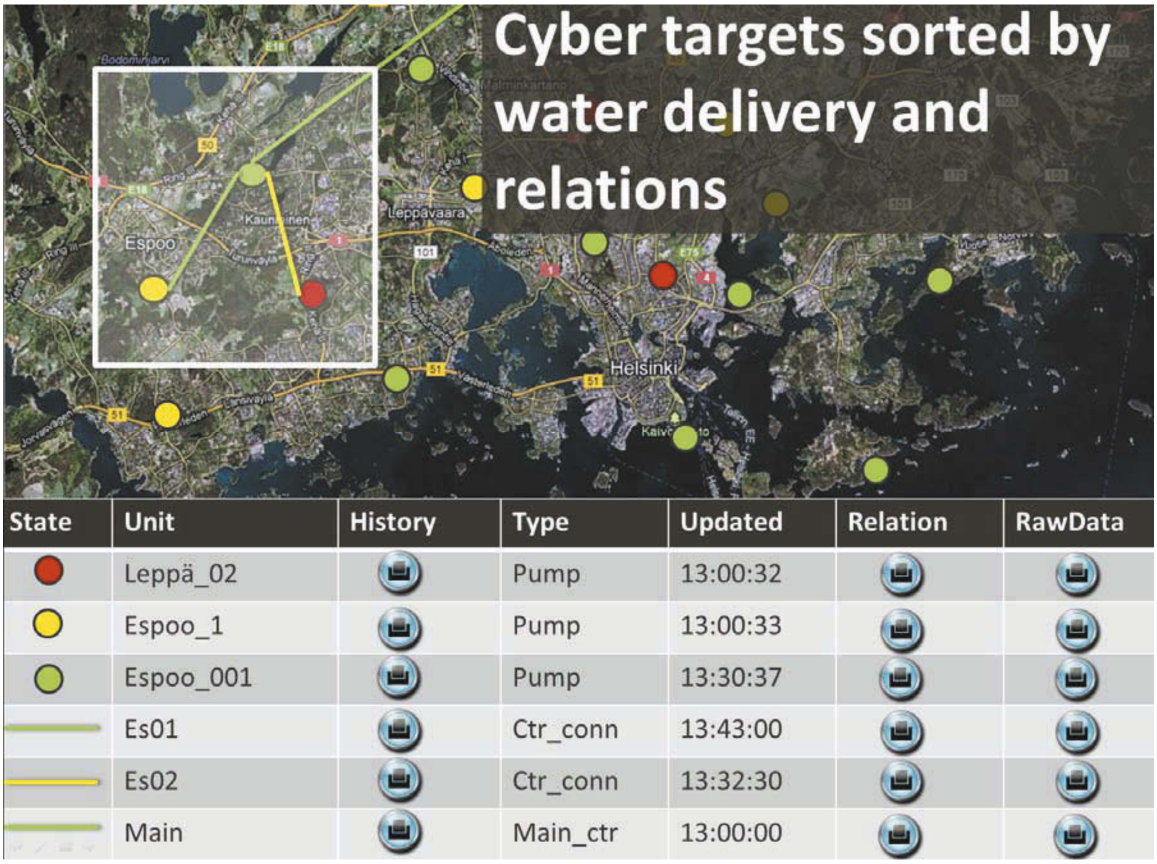


Figure 8. Status symbols

Based on these extremely simple symbols it is possible to create the first level presentation using filtering of the objects. These custom views are created by a human operator. When an analysis is applied it can be shared for the use of the new abstraction level. In the figure 9 the targets in water delivery are filtered and presented in a logical view from a specific area. The selected area presents at least the unit name, provides level 1 history (status history), type and update time.


Cyber targets sorted by water delivery and relations

State	Unit	History	Type	Updated	Relation	RawData
🔴	Leppä_02	◉	Pump	13:00:32	◉	◉
🟡	Espoo_1	◉	Pump	13:00:33	◉	◉
🟢	Espoo_001	◉	Pump	13:30:37	◉	◉
━	Es01	◉	Ctr_conn	13:43:00	◉	◉
━	Es02	◉	Ctr_conn	13:32:30	◉	◉
━	Main	◉	Main_ctr	13:00:00	◉	◉

Figure 9. View

The field of visualization of cyber targets is in constant change and it has a great need of further research. The concept of multimodal user interface [11] could offer improved capabilities also in cyberspace operations. Wei et al. [12] present a visualization technique based on discrete wavelet transform (DWT), which could offer an usable non-traditional way of interpreting cyber events. The user interface should be able to provide a simple and easy view for human, but this is all but trivial task to the designer. Blasch [13] lists the main challenges in human perception as follows.

> **Limitations of human attention** which the automation designer must keep in mind include:
>
> - **Perceptual Processing Limitations** – Increased perceived difficulty attending to more things at one time.
> - **Focus of Attention -** Impact of the situation on the user in directing the attention and keeping it focused.
> - **Central Processing Limitations** – Cognitive processes may be limited in number which can occur at a time.
> - **Memory** – Long, Working, Short - relationship between attention, working memory, search, short-term retention.
> - **Modes of Attention -** Top-down or Bottom-up [13]

Often the systems for cyberspace are focused on incident detection and handling. In terms of critical infrastructure visualization, it can be considered also in terms of situation visualization, which contains incidents, but also the capabilities operating normally. The proposed agent infrastructure is built for the latter purpose.

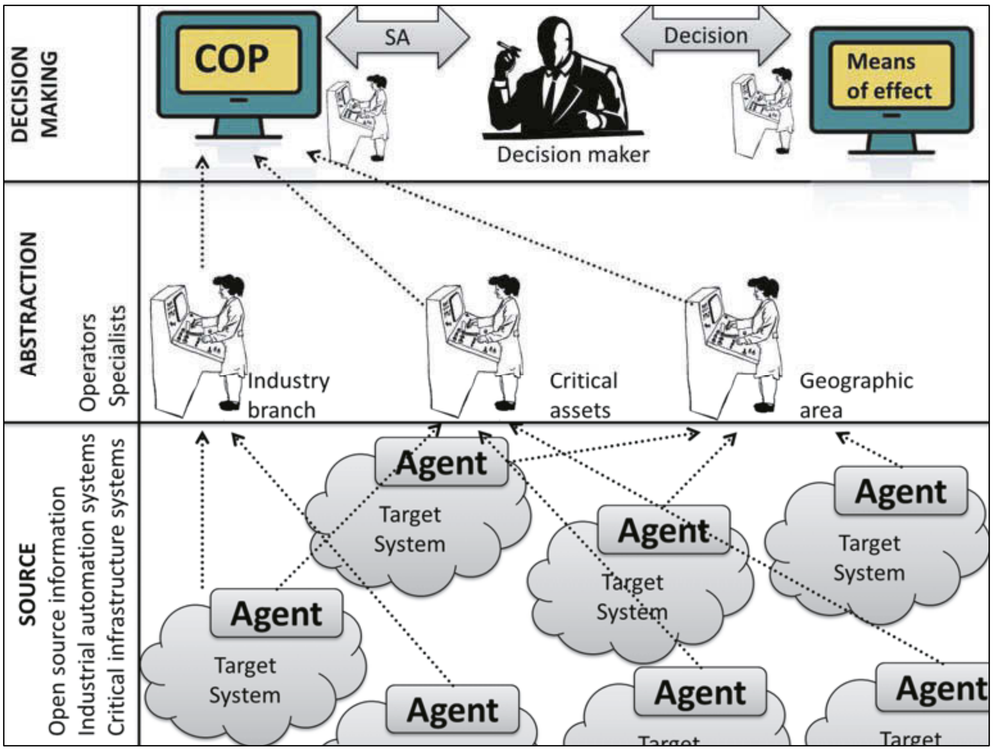


Figure 10. Decision making architechture

4 Decision making

Why would a system offering a common operational picture would be created? As alone it does not offer any more than an improved situational awareness to the user. In order the system to be usable it needs to operate as an aid to the decision maker. This is accomplished by using multiple abstraction levels maintained by operators and analysts, who are experts in their field. From these levels the created information is shared upwards and presented as a decision making view, also operated by a specialist. The figure 10 presents the levels from agent to decision making.

The SACIN system does not include a component, which would be the actual system for effect. In the field of critical infrastructure it is not straightforward to create a generic gateway for effect. All the systems are different so the effect will most likely be gained by contacting the domain expert of the target system. This will force the effect system to be heterogeneous and based on multiple experts in their field also in the target systems.

5 Conclusions and future research

The technology exists for multiple challenges in the field of critical infrastructure situational awareness. The proposed system presents an architecture and concept for creating information from the society. The solutions in terms of service discovery, information delivery and storing are trivial from the perspective of technology, but the challenges lie in what is gathered and how it is gathered. At the same time the laws must be evaluated. What kind of information it is possible to collect and is it possible to demand this information from the companies and society based on laws?

An extremely important area is the sharing. Any system in this area should not be planned as the endpoint of information. The best solution would be to use known formats for sharing the information the different actors in the field. At the same time the newly built system need to have gateways implemented for importing information.

References

[1] "Kansallinen Kyberturvallisuusstrategia," TURVALLISUUS- JA PUOLUSTUSASIAIN KOMITEAN SIHTEERISTÖ (TPAK) 7.5.2012 2012.

[2] "Definition of C2," in *DOD Dictionary of Military and Associated Terms* vol. 2013, ed: United States Department of Defense.

[3] http://www.reference.com/, "Definition of Critical infrastructure," vol. 2013, ed, 2013.

[4] Y. Xinfeng and S. Singh, "A SOA Approach to Counter DDoS Attacks," in *Web Services, 2007. ICWS 2007. IEEE International Conference on*, 2007, pp. 567-574.

[5] S. Schreiber-Ehle and W. Koch, "The JDL model of data fusion applied to cyber-defence " in *Sensor Data Fusion: Trends, Solutions, Applications (SDF), 2012 Workshop on*, 2012, pp. 116-119.

[6] G. P. Tadda, "Measuring performance of Cyber situation awareness systems," in *Information Fusion, 2008 11th International Conference on*, 2008, pp. 1-8.

[7] L. Perrochon, J. Eunhei, S. Kasriel, and D. C. Luckham, "Enlisting event patterns for cyber battlefield awareness," in *DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings*, 2000, pp. 411-422 vol.2.

[8] N. A. Giacobe, "Application of the JDL data fusion process model for cyber security," in *Proc. SPIE*, 2010, p. 77100R.

[9] A. N. Steinberg, C. L. Bowman, and F. E. White, "Revisions to the JDL data fusion model," *Proc. SPIE 3719, Sensor Fusion: Architectures, Algorithms, and Applications III*, vol. 3719, pp. 430-441, March 12, 1999.

[10] S. Tiilikainen and J. Manner, "Suomen automaatioverkkojen haavoittuvuus," Aalto yliopisto, Sähkötekniikan korkeakoulu 2012.

[11] "Ajan tasalla - Tilannetietoisuutta tukevat käyttöliittymät vaativissa toimintaympäristöissä," Aalto-yliopiston teknillinen korkeakoulu, Espoo 2010.

[12] W. Yu, S. Wei, D. Shen, M. Blowers, E. P. Blasch, K. D. Pham*, et al.*, "On detection and visualization techniques for cyber security situation awareness," in *SPIE Defense, Security, and Sensing*, 2013.

[13] E. P. Blasch and S. Plano, "JDL Level 5 fusion model: user refinement issues and applications in group tracking," in *AeroSense 2002*, 2002, pp. 270-279.

Trust Based Situation Awareness in High Security Cloud Environment

Klaus Zaerens
Finnish National Defence University
klaus.zaerens@iki.fi

Abstract

Trust management has been a topic of keen interest in recent years. There has been a lot of discussion as to what new opportunities it can bring to concepts like semantic web, social networking of collaboration methods. Most of the researches in the field of trust management are based on assumption where trust is relatively static quantity between two actors. If it changes, it changes over long period of time.

In this paper, we will discuss issues and problems to be considered when creating situation awareness in public authority environment. It is evident that joint operations between different authorities could benefit from common operative collaboration platform. We focus in more detail to a challenge where credibility of information sources might alter in very short period of time like during the operation. We present a formal challenge named durability of trust to address this event and propose methods as a solution to challenge. In addition to a challenge itself, methods provide new tools for improving the situation awareness. The discussion and views presented in this paper can be adopted in any organization with doubts concerning the sensitive and classified contents of current ICT systems in cloud computing.

Keywords

Trust management; Cloud computing; Security; Situation awareness; Public authority; Military

1 Introduction

Importance of trust management is increasing as the Internet is more open for access, different collaboration tools and social networking become more common. The relevance of trust management is gradually becoming more significant but the abstractive nature of the context has kept commercial activators and applications away. Trust management is a challenging context because the content varies on the frame of reference. The specific definition changes whether the aspect is social science, behaviour science, humanist science, business science, political science or computer science. Within computer science we can focus on security, safety or integrations features and limit observations to computative properties.

Concept of semantic web is also increasing noteworthiness. While the amount of sources producing data, information and knowledge is increasing and the possibility to identify individual actors, the question about the trustworthiness of source or data itself is becoming more significant. Information can be modified or coloured by opinions, views, interests or goals of the data producer. In semantic web the combination of different data fragments at best can produce more informative value than the arithmetic sum of the fragments. However at worse the information combined can be misnomer or attempt influence directly or indirectly to opinions or actions of recipients.

Altogether trust is an emotional issue. For example a new webshop: How can consumers and potential clients decide whether the shop is trustworthy and not a hoax? Probably the enterprise name and information is viewed and the most advanced users will use web search for more information but in the end most clients just feel that everything looks fine and the need for item bypasses all rational considerations. For this purpose different kind of ranking by manual methods and automatic listings are developed in web to advice the information seekers. For manual decisions properties such as authority, accuracy, objectivity, currency and coverage are encouraged to be considered [1]. Perhaps the most famous webpage listing is PageRank provided by Google [2]. Rank is based on the amount and quality of links to page.

Another kind of example on trust is a crisis area with information warfare produced by the both parties of the conflict. How can we determine what data is accurate information on the situation and what is propaganda attempting to affect public opinion?

Public authorities in security field have sought and developed numerous means to improve cooperation by ICT solutions. Different kind of collaboration tools and environments has been deployed and integrations between systems and data storages have developed. It is obvious that concepts like semantic web and social networking gain authority cooperation. However these concepts cause also new challenges. Openness is can be hard to manage in highly secured environment. Also threat of centralizing physically or logically critical knowledge of the society in single location is enough to increase hostile interest on system. This can trigger malicious activity.

In authority cooperation trust within own organization is usually unreserved. This trust is based on mutual experience, common procedures and professional community. A lot harder is to trust another authority and different organization. Yet on matters of professional expertise, trust is important element in operations and in core specialties of the organization easy to accept in the field of public authorities.

The main goal is to have enough sufficient information to form awareness of a situation. The collaboration methods improve the accuracy of the awareness and delegate awareness to all actors within operation. This enables better communications, safe procedures and more effective actions in operations throughout participating authority organizations.

In this paper, we will discuss issues and problems to be considered when creating situation awareness in high security authority environment in which the need for computational capacity is high and the reliability of information is always critical. We focus in more detail to a challenge where a possibility for malicious intervention is present and a credibility of information sources might alter over time. We call the feature of maintaining trust in the aspect of situation awareness as a durability of trust. As a solution to problems with the durability of trust in high security public authority environments, we propose for methods applied simultaneously. These methods are propagation of trust metrics within network, dynamic maintenance of subjective trust map, current data flow analysis according to past data flow and elimination of abnormal information.

The paper proceeds as follows. First, we will examine the essence of trust management by defining its relevant terminology, characteristics and principles, as well as the benefits of the technology within the scope of a public authority situation awareness context. Next, we address the some problems or challenges that exist in high security cloud collaboration platform in public authority context. Lastly, we focus our discussion to a trust management and propose possible solutions or indicate future work to be done to overcome the obstacles described. We will conclude with key findings and a description of the future of trust management in the public authority context.

2 About Trust Management in Public Authority Context

There has been also a lot of discussion on accurate definition of trust computing. The definitions presented vary more or less according to the organizational, business or operational environment or interests. In this paper we adopt the definition of trust presented by Grandison and Sloman because of the simplicity yet complete enough. Trust is “a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context” [3].

Features of the trust management vary as the definition itself. In this paper we limit our observation on computative trust management. Widely accepted features on computative trust management include subjectivity, the expected probability and relevance. These features can be quantified and implemented as part of a computer system. Because of subjectivity, the evaluation of trust is made by service requestor, client or end-user. The evaluated system or the target has little possibilities to affect directly to the evaluation process but indirectly it must present itself and its behavior as trustworthy in given context. The probability or the likelihood of trust indicates how strong the trust relation is. The probability is quantified metric of certainty of belief of the requestor and not absolute trustworthiness of the object. Relevance fine tunes the probability and limits the observation only to act or functionality essential to requestor [4].

Examining trust management characteristics in more detail can be accomplished by examining the trust itself. According to relevance, trust is limited to domain and to specific action or class of actions [4]. Trust can be seen as an aspect of things for specific content. Trust is rarely or never absolute. There is always room for interpretation or uncertainty. That is why it is usually quantified as probability or likelihood. The belief of trustworthiness of target does not indicate anything about the target itself. Target may not be competent in matter, anyway motivated towards the requestor or target need not to be generally reliable. Moreover the relation of trust is asymmetric by nature. If the requestor trusts the target it might not apply vice versa. We argue that the trust is rarely same with between two participants except if there is no trust at all to each other (i.e. P=zero). Even if trust is quantified as same numeric probability, the subjectivity prevents the realization as same kind of trust.

Authorization methods and certificates identify the participants of communication but not symmetry of trust, because identification itself might be irrelevant in relation to trustworthiness of the processed content. It is also noteworthy that trust can be bound to role where the participant represents some organization while authorization always tries to identify the actor.

In public authority context participants are bound to role. Participant represents some unit within organization. Similarly data providers such as sensors can be modeled by an ownership of an organizational unit. Unit has a task and a goal and special expertise specified by the organization. It is important to understand that when two actors from different units interact, one trusts the represented role not the actor itself. Yet the trustworthiness between two roles can be fixed on process level, the individual actor might have specific preferences, interests or experience which affects to quantitative trust.

In public authority context we can set the initial credibility on process level for each unit according to expertise and ability to react or interpret situation around unit. The credibility is not static, because it changes according to situation and environment. Changes in goals, interests or resources differentiate credibility between organizations. How the credibility could be modeled between authorities for example in crisis situation needs more research. In this paper we limit our observation on analyzing the possible need for changing the trust value of given target.

3 Situation Awareness and Trust Management

Improving situation awareness has become more critical in public authority operations and especially in military context. The possibilities and utilizations of situation awareness have increased together with technical evolution. Sensors and mobile devices increase the effectivity of collecting data from locations that traditionally have been difficult to access. More data can be collected and stored than previously which enables view on situation to be more truthful, accurate and comprehensive.

The most severe challenges on improving situation awareness are related to refinement of significant information from huge amount of data, unstable data transfer connections and especially in field operations limited data capacities. Also data correctness, reliability, redundancy and timeliness have been research issues or discussed in several publications. Less interest has been addressed to trust evaluation of data based on source.

This special characteristic on ensuring correctness becomes more important when considering a threat where some malicious actor inserts false information to operative decision making process. The aim of perpetrator is to have influence the decision itself and the environment around it. Impact to different sources of information will affect corresponding decision making processes. On disrupting single sensor, receiver of data can easily to detect failure on data feed. Detection is much harder if the sensor starts sending infrequently abnormal values, metrics or information. Yet more challenging is to detect almost correct data when similar results are provided from large amount of sensors. This situation can happen if several sensors are occupied by hostile actor. This kind of scenario might have very large effects. For example modification of temperature values from a region can have impact on decision of limiting the use of some technical equipment. On military operations this can give a significant advantage to opposite. Similarly most technical equipment is vulnerable on extreme weather conditions.

Another example is public authority systems which use geographical positioning system (GPS). Modifying the GPS signal can compromise the safety of troops on target area. Especially on military operations this can lead to a situation where troops are endangered to friendly-fire. At peace time rescue service can be guided to a false location or police might create incorrect understanding on isolated area and possible fringe areas.

Message or data transfer techniques are designed for ensuring the consistent data transfer between two nodes [5; 6]. The usual assumption is that the data itself is correct and the end nodes recognize each other by different authenticate methods such as PKI (Public Key Infrastructure) solutions [7]. Trust management brings a new dimension to secure data transfer by evaluating the credibility of source on history information, trust or comparing the received information to constructed general view.

4 Some challenges within Trust Management in High Security Cloud Environment

We examine some challenges within trust management in high security cloud environment such as in public authority cloud. Focus is on problems which are derived from modern collaboration tools and situation where threat of a malicious actor is present. Malicious actor is motivated in preventing or disturbing decision making or operative ability of authorities.

4.1 Semantic Web

Semantic web is widely envisioned to be an extension of current web, where documents are annotated with meta-information. This meta-information describes the contents of the document on information level and enables the content knowledge to be processed by a machine [8]. The meta-information links explicitly documents with each other and improves the knowledge retrieval by structuring the scattered information. It is essential for semantic web to be open to everyone to provide knowledge and information available for every user. The challenge arises on the uncensored contents. The evaluation of the trustworthiness of knowledge and how the information can be used is on the consumer side. Methodologies on estimating the reliability of information source becomes vital [9; 10].

High security public authority environment is not open environment similarly as Internet as whole. The user group is limited and in theory very strictly controlled. Public authority environment provides a trusted environment and to have an access to it, actor should be included in some trusted role. The strength of this trusted environment is that an authority can provide detailed and reliable information to every consumer according to special expertise. The weakness is that how it is controlled when authority makes a statement outside the field of own expertise. The status as an authority in some field does not imply the expertise in every field of authorities. This ends up in same situation as in open Internet. One might trust information that is not reliable. Actually situation in public authority environment is slightly more concerning because of the reliable nature of environment. The reliability of the information should be evaluated on the contents relation to information provider. As a result on this finding we argue that a controlled user group in trusted environment does not exclude the requirement of trust management for content. In addition we argue that more framework of the environment is specialized and more roles participate within, trust management role as part of content management is increased.

4.2 Social networking

Social networking has become an effective tool for networking and maintaining social relations by people [11]. The private applications have also become more common in also business world and part of work equipment in offices equally as mobile phones or computers. These tools are seen also effective for information sharing between authorities. Especially in operative situations the need for common platform of information is acknowledged. If expertise of each participated authority is provided the value of situational awareness is tremendously added. Furthermore the cooperation in operative situation is improved and resolution for situation will be facilitated [9].

The challenge is how the ownership of the combined information is determined and who is responsible on the interpretations of the summarized data or the faults that occur. Because the ownership of the data is questionable and hardly controlled after summarization, the requirements for good data management are difficult to fulfill. For example Finnish authorities have special demands for data management when processing sensitive data or data regulated by special legislation. These demands include for example traceability of operations, control of access, lifecycle management and quality management [12].

The security classification of data is also a problem. Some authorities can have access to more secured or sensitive information than others. This data can be crucial information during some operative situation regardless of the authority in action. System must have proven and tested processes for management and accessibility of secured information generally, in operative situation and after the operative situation is over.

4.3 Collaborative reviewing

As stated in previous chapter public authorities often process very sensitive data. It can be that a data fragment itself by one authority is unclassified but with combination of different aspects on same matter by different authorities, overall knowledge can be security classified. Combination of several information sources affects to security classification of data which implies that summarized result should be controlled with additional security measurements. This kind of functionality must be implemented carefully in order to maintain the operative effectiveness between authorities [9].

The collaboration platform with combined knowledge from different authorities has indisputably benefits in operative actions and decision making. The downside is that the centralized information also composes an alluring target for hostile reconnaissance operations. It must be recognized that information system evolved is a so-called honey pot for malicious actors and authorization methods and access policies should be implemented and maintained carefully [5; 6].

4.4 Sensor Networks

One key element composing situational awareness is to use information gathered from different sensors. These automatic sensors measure the environment and supply data from the surroundings. Sensors can be static installations or they can be mobile equipment transported by the units connected to the system [9; 13]. Devices that are used in transmitting the information on situation for requestors can be also the information provider. These mobile devices can produce very useful and by nature dynamic aspect to a situation for different kind of purposes. But the mobility is the risk itself because it is attached to some organizational unit. The information from the location of the unit is also transmitted or exposed with the data transferred. This might be a safety risk to unit and the personnel in it.

Also the security classification discussed in earlier chapter might become an issue when collecting information and centralizing the knowledge. Sensors monitor conditions for operation but they also provide information on the surroundings of the own unit which can expose vulnerabilities on operation. Data provided by the sensors might be a basis for some decision which increases the demand of reliability of data. Security issues arises also when a sensor and its feed is controlled by malicious actor.

4.5 Durability on Trust

Situation awareness gives context to all operative decisions. Constructing situational awareness it is essential to rely on the information available. In public authority environment, also progress of time must be taken into consideration. If information from data source is correct and reliable today, it does not guarantee reliability and correctness tomorrow from same source. This applies especially in crisis situation where malicious actors exist and the threat of disinformation is present.

In crisis situation the importance of credible data transfer is significantly increased. Maintaining reliable awareness of situation, it is important to eliminate all insignificant data feed relation to friendly operative actions. During the escalation of crisis, the construction of high security public authority cloud or network is dynamic and under constant change. New geographical locations become available or contaminated network nodes are disconnected from core security cloud. The possibility to evaluate realtime trustworthiness of single data feed is very limited. The trust properties must be adopted and referred accordingly the dynamic features of the environment. At the same time security of the sensitive data must be preserved and unachievable to outsiders [14].

Current research on trust management has mainly focused on trust between two actors or entities. Almost without any exception research is observed by a happyday scenario where every participant is trustworthy until otherwise proven. There are published algorithms how to evaluate trust in each moment. However in dynamic environment trust is not a static feature of an entity and the durability of trust cannot be taken granted. In public authority environment we must ensure data flow correctness and create methodology to eliminate noise. In this paper we discuss on a situation where a trusted node forfeits credibility and how it can be detected. We approach the challenge by questioning the credibility of nodes at all times. This approach emphasizes the property of trust as non-absolute metric. We examine the credibility of data feed in more detail by observing delegating trust metrics within network, maintaining the subjective trust metrics, analyzing the data flow against the past data flow and eliminating the abnormal information.

5 Proposed approach for durability on trust

In this chapter we define the problem and propose approach for durability on trust. After definition we explain the approach in more detail. Let us define the problem as follows (see figure 1.):

> *Asymmetric trusted relation between A and B at given time of T, does not guarantee trust in same relation at T+1. How the change of credibility on B can be detected at T+1?*

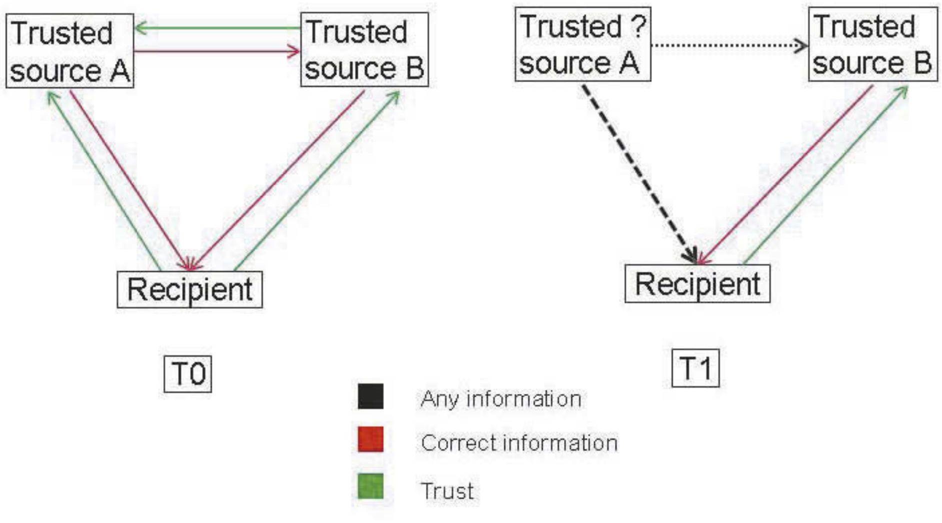


Figure 1. Illustration of the problem

In our approach we propose four simultaneously applied methodologies in order to detect the change on credibility and maintain the durability of trust in core system in order to improve situation awareness. This concurrency on methodologies ensures the reliability of our approach. If requirement for any of methodology is relaxed, the risk for losing situational awareness will increase.

Our methodologies are:

- Propagation of trust metrics within network
- Dynamic maintenance of subjective trust map
- Current data flow analysis according to past data flow
- Elimination of abnormal information

Three first methods analyze the credibility of nodes in system. The fourth method analyzes the knowledge and approves that some of the data sources are not credible. From the situational awareness point of view, these methods cause single data fragments to be vanished from the entirety and their correctness to be neither interesting nor relevant. For strategic decision making this approach is more useful to build knowledge from data feeds and achieve improved situational awareness. It also means that the abstraction level of the trust is higher and the correctness of information is evaluated by the trust analysis with all actors within security environment. The proposed methods imply that single data fragments are blurred whether they are correct or not. Methods emphasize that knowledge and the overall awareness are more important than single data feeds or even single sources. On next chapters we examine methodologies in more detail.

5.1 Propagation of trust metrics within network

On propagation of trust metrics, each node is responsible to propagate its' up to date trust metrics from neighbors to other nodes within network. Each node saves the information of trust metrics that it receives. This methodology enables that the recipient node can monitor the neighboring nodes indirectly. Indirectly means that the change of credibility is detected by some other node or nodes. For example if (B does not trust A) and (Recipient trusts B) then Recipient does not trust A (see figure 2.).

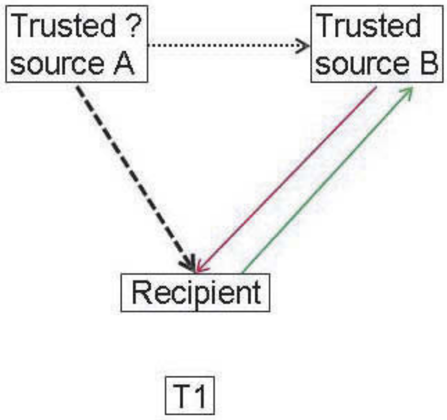


Figure 2. Evaluation credibility of source A on basis of trusted data from B

Propagation of trust metrics allows constructing also trust paths of information and more importantly isolate less credible nodes from information exchange. The latter feature is important especially in high security network in order to disable nodes that are hosted or controlled by malicious actors.

Because propagation of metrics is continuous activity, it is comparable to data transfer metrics delegation between Internet routers. The challenge arises in this kind of activity, how to detect a loss of trust in single node on time. Another challenge in system architecture is how to deal with untrustworthy node. On evaluating the significance of doubt, it must be considered, should the delegation of trust metrics be limited or more crucially the data itself. If the data transfer to unreliable node remains the unchanged, it enables the transfer of disinformation in some cases.

Naturally on this kind of evaluations there is always a possibility of misjudgment of credibility. The probability of misjudgment increases especially in crisis situation facing new and previously unknown situations. By misjudging the credibility, the consequences can be dramatic and the operative ability endangered.

We propose operations and essential properties for dynamic construction of high security cloud environment and for detection of credibility change.

One key property is a threshold of trustworthiness in environment. This fixed value means defines the baseline for sufficient credibility. This threshold is bounded to subject during evaluation. The implication is that every node has list of own expertise as a property list on which the trustworthiness is evaluated. For trust metrics outside own expertise node treats as router. This also means that the judgment of credibility for node is made only based on its own expertise not the information it transfers for other nodes. It is also essential that each node evaluates other nodes subjectively and according to own expertise. The implication is that trust metric of a node varies within network nodes. Moreover nodes can have several trust values for one node depending of the expertise.

If node is detected untrustworthy by sufficient amount of neighboring nodes, it means that combination of trust metrics concerning a single node falls below a predefined threshold. After detection, the isolation information of this node is sent to all other nodes. It is essential that the decision of untrustworthiness can be made by any node collecting the trust metrics. This allows decentralized control of environment and instant responses in highly evolving situation.

In dynamically constructed high security cloud environment there is two special cases of node operations. If a new node is attached, exist of new trusted node is delegated to all trusted nodes in environment. If any node is detached from environment, removal of node is delegated to all trusted nodes in environment.

The system must have also centralized administration operations in order to relax requirements in unexpected situation and to allow operation despite the trust values. These operations allow increasing or decreasing the threshold of trustworthiness and in extreme case the initialization or refreshing of trust metrics.

5.2 Dynamic maintenance of subjective trust map

Subjective trust map was discussed slightly in previous chapter. Here we look it in more detail. We discussed already in introduction chapter, that an authority trusts own organization without any doubt, but for other organizations only according to expertise. The challenge in evaluation is that how the expertise can be evaluated when the evaluator has not enough expertise on subject. We propose subjective trust map as a solution of this challenge. It allows an organization to evaluate credibility of information sent by other organization with help and confirmation of third organization which has better expertise on subject. In other words the reliability of feed from C can determine trustworthiness of B if B and C trusts each other and C is trusted [15].

Subjective trust map is based on the idea that a recipient acknowledges in what relation B is to A. Relation is limited to role in context and that is why we can judge the trust metrics of the other nodes only by according their aspect or expertise. The basic principle is that the change in role or aspect might impact a change in subjectivity and preferences as well as ability to evaluate trust on other nodes.

Data structure of subjective trust map is composed as a list of arrays. Each item in list includes a node in consumer role. It means that the item is the receiver of data from other nodes. The array represents key – value pairs of all possible sources of data. Key is the source and value is the trust value of specified subject. The amount of items in list is the amount of nodes in the environment. The size of the array exponentially enlarges by the subjects that are determined for the trust environment and is 2n^k, where n is the amount of sources and k the amount of subjects (see figure 3). Mathematically subjective trust map of a consumer can be represented as matrix of vectors, where size of vector is the trust value of source.

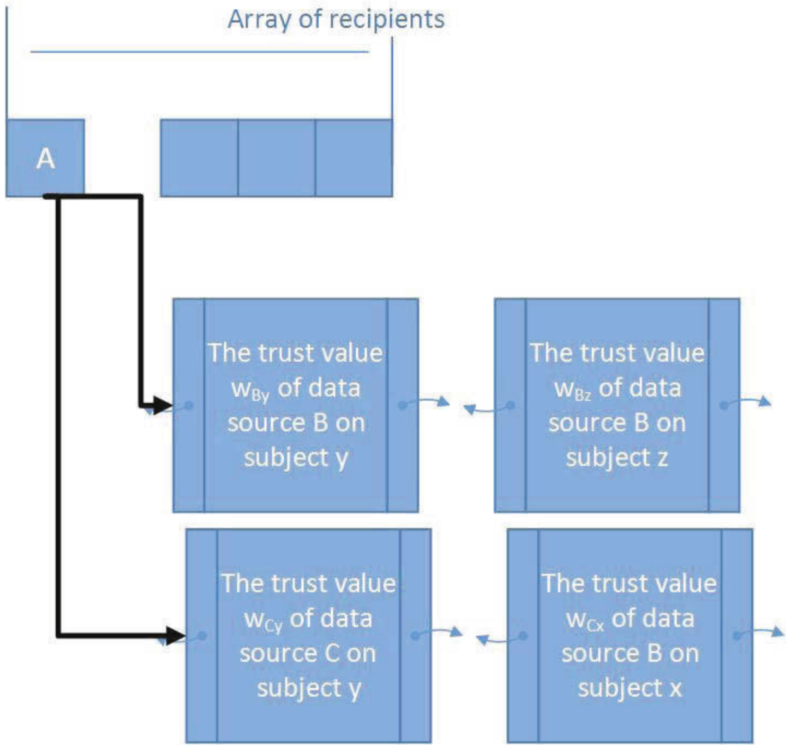

Array of recipients
A
The trust value w_{By} of data source B on subject y
The trust value w_{Bz} of data source B on subject z
The trust value w_{Cy} of data source C on subject y
The trust value w_{Cx} of data source B on subject x

Figure 3. Illustration of subjective trust map

Despite the computational requirements, it is essential that the maintenance of subjective trust map is continuous. This signifies that maintenance algorithms need more research in order to decide how the subjective trust map should be treated and what is relevant for each node. We find that some hierarchical approach in relation to neighboring nodes and organizational hierarchy (chain of command) should assist on computational challenge.

The visualization of subjective trust map can be represented as a heat map where red color indicates the loss of trust in nodes. This provides a new visualized aspect in improving situational awareness where we can monitor our system environment and outsiders in it.

5.3 Current data flow analysis according to past data flow

Real time comparison of data flow against predicted data flow can be also considered as a trend analysis of data flow. The purpose is to detect abnormalities from data feed against assumptions on normal feed. Of course the normal feed from the history must be collected and stored before in order to detect the possible changes. Usual method on data flow analysis is to apply statistical trend analysis models of received data flow. The trend is formed from three or more known samples of historical feed and analyzing their respective change. This method can be used for exploring secular abnormalities.

Crisis escalation can be a problematic situation, because it usually is out of ordinary and it might differ drastically on normal situation. On that purpose different scenarios can be made which are simulated or known escalations of different crisis events. Matching the abnormality to the different scenarios this can be a powerful tool on detecting a crisis at early stage and provide enough information to effective countermeasures.

As stated above, on crisis escalation this method can cause false alarm at initial state. However, narrowing timescale and shorten the trend observation period the system can produce predictions on how the situation might escalate. On the other hand widening the timescale and adding more samples for trend this method can be used in finding long term abnormalities which normally are lost in background noise. One example can be hostile intervention to a system and espionage without compromising the system directly.

Naturally this kind of analysis requires significant computational capacity and method is most useful in cases where crisis is at early stage. After escalation of the crisis situation computational tasks becomes relatively expensive to this kind of data mining analysis, because all capacity is needed for operational use.
One must also remember that data flow analysis prediction method is just as good as the model it represents. The functionality requires the baseline of samples from normal system activity and continuous evolvement of the baseline and model. Correspondingly development of different models and scenarios enables the improvement of situational awareness and enhance readiness for proactive reaction in sudden events. In military environment these scenarios and models are usually created and evolved in different kind of war games and simulations.

5.4 Elimination of abnormal information

When observing the situation and creating awareness from surrounding events, a single data fragments are not relevant. Data fragments become relevant only if sufficient amount of fragment represent similar phenomenon.

In this method statistical average and normality is used for reducing noise from feed and several knowledge flows are used for correction of specific data feed on situational awareness level. This method can be divided to four different phases. In the first phase we eliminate single abnormal data fragments from dataflow. In this context abnormal data fragment can be a single highly deviant message from source or from sensor which can be assumed as a mistake or a failure. Mathematically it means sample which differs significantly from average. These deviations should be eliminated in order to release computing power to relevant context. The single failure of source is eliminated from our system with other methodologies such as subject trust map analysis. It must be also noticed that in very rare cases a decision can be made based on a single source of information.

Usually this happens only when the decision maker is the observant. Of course another observant might do a different decision based on same observation. This fact relaxes the requirement of maintaining single data fragment on construction of situational awareness.

On the second phase it is essential to reduce the background noise from the feed. This can be made with filters which eliminate normal or predicted activity from the data feeds of the system. The samples of baseline and which were used for trend in previous method are useful on this noise reduction. The aim is to detect the information that is the most significant for the user. Naturally this means also that the filters for noise can vary depending of the need for information.

On the third phase the data feed should be normalized. The idea is to emphasize the possible phenomenon with data feeds that share similar knowledge. How the normalization should be done in various situations need more research.

In addition to these traditional method we propose a method where correctness of data feed is compared with data feed from another source on knowledge level. Two data feeds that explain same phenomenon improves the knowledge on situation even if the aspect of sources differs.

In our proposal it is important to identify the phenomenon not the separate perspectives. If different actors express the same phenomenon on their own perspective, the reliability of the formed awareness on situation is improved. On the other hand, if three actors express same phenomenon and the fourth something divergent, the credibility of operative ability of fourth actor can be doubted. If this occurs in high security environment, the security of the system might be compromised and the reliability of the fourth actor should be analyzed.

6 Conclusions

In this paper we examined the trust management paradigm within the public authority context. We stated that in operative environment the credibility of data source is not a static quantity. We discussed the essence in composing situation awareness in relation of trustworthiness of data sources. We emphasized the asymmetric nature of trust and found that in high security environment the trust is never same with two actors unless there is no trust at all. We also noted that more framework of the environment is specialized and more different participants exist, the necessity of trust management as part of content management is increased.

We identified the five obstacles in high security cloud environment and looked in more detail to a situation where trust between actors might change during operation. Yet we noted that authorities in high security cloud benefit from different collaboration methods and we presented a formal challenge called a durability of trust and examined possible solutions to overcome credibility change.

As a solution to maintaining the durability of trust and in order to have sufficient information for situation awareness, four different concurrent methods were proposed: Propagation of trust metrics within network, Dynamic maintenance of subjective trust map, Current data flow analysis according to past data flow and Elimination of abnormal information. With methods presented, we can monitor the credibility of sources in cloud environment. We also achieve improved situation awareness, reliable security network and new crisis escalation prediction tools in public authority environments. We argue that proposed approach enables the collection of the sufficient information in order to improve situational awareness based on correct data.

We find trust management to be an emerging research area especially in networked public authority operations. Implementations of methods presented in this paper need more research and work to be computatively efficient in practice.

References

[1] Beck, S, *The Good, The Bad & The Ugly: or, Why It's a Good Idea to Evaluate Web Sources,* 1997, http://lib.nmsu.edu/instruction/eval.html, cited 8.7.2014.

[2] Altman, A, Tennenholtz, M, *Ranking Systems: The PageRank Axioms,* Proceedings of the 6th ACM conference on Electronic commerce (EC-05), Vancouver, 2005.

[3] Grandison, T, Sloman, M, *Specifying and analysing trust for internet applications,* In Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government, 2002.

[4] Ma, S, Wolfson, O, Lin, J, *A survey on trust management for intelligent transportation system,* In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science (pp. 18-23), 2011.

[5] Blaze, M, et al. *Experience with the KeyNote Trust Management System: Applications and Future Directions,* Proc. of First Int. Conf. on Trust Management iTrust 2003, Springer-Verlag LNCS 2692, pp. 284-300, 2003.

[6] Iltaf, N, Ghafoor, A, Hussain, M, *STEP-a: An Algorithmic Approach towards Trust Based Security in Pervasive Computing Environment,* InServices Computing Conference (APSCC), 2011 IEEE Asia-Pacific (pp. 330-336), 2011.

[7] Kagal, L, Finin, T, Joshi, A, *Trust-Based Security in Pervasive Computing Environments,* IEEE Computer 2001, vol.34, no. 12, pp. 154 – 157, 2001.

[8] Davies, J, van Harmelen, F, Fensel, D, *Towards the Semantic Web: Ontology-Driven Knowledge Management,* John Wiley & Sons, Inc., 2002.

[9] Mardziel, P, Bender, A, Hicks, M, Levin, D, Srivatsa, M, Katz, J, *Secure sharing in distributed information management applications: problems and directions,* In Proceedings of the Annual Conference of the International Technology Alliance, 2010.

[10] Richardson, M, Agrawal, R, Domingos, P, *Trust management for the semantic web,* In The Semantic Web-ISWC 2003 (pp. 351-368), Springer Berlin Heidelberg, 2003.

[11] Wasserman, S, Faust, K, *Social Network Analysis in the Social and Behavioral Sciences,* Social Network Analysis: Methods and Applications. Cambridge University Press. pp. 1–27, 1994.

[12] Finnish Ministry of Finance, VAHTI-instructions, "Hyvä tiedonhallinta- ja tiedonkäsittelytapa",https://www.vahtiohje.fi/web/guest/hyvatiedonhallinta-ja-tiedonkasittelytapa , cited 3.8.2014

[13] Chaturvedi, P, *Introduction to Wireless Sensor Networks,* International Journal of Advanced Research in Computer Science and Software

Engineering, Special Issue: Recent Trend in Computing, Volume 2, Issue 10, October 2012.

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

[15] Zhou, Z. X., Xu, H, Wang, S.P, *A Novel Weighted Trust Model based on Cloud*, Advances in Information Sciences and Service Sciences, 2011.

Authors

Jouko Vankka is a professor at the Department of Military Technology in the Finnish National Defence University. He received the M.S. and Ph.D. degrees in electrical engineering from Helsinki University of Technology in 1991 and 2000, respectively. He received the Degree of Bachelor of Social Sciences from Helsinki University in 1994. Since 2005 he has been with the Finnish Defence Forces.

Ltcol (G.S.) (Ret.) and chief of preparedness (www.nesa.fi) **Sakari Ahvenainen** is an ex communication officer of the Finnish Army. Since the 1990's he has been also a freelance researcher of warfare in general, information warfare, network-centric warfare and technology in warfare (etc.). As an information warfare researcher he has given six international presentation 1997 - 2002. Ahvenainen is a PhD student in Tampere University of Technology (main studies) and Finnish Defence University (side studies). Six of his articles has been published in the yearbook ”Tiede ja Ase” (Science and Weapon) of the Finnish Society of Military Sciences.

Heikki Lantto, Captain, is doctoral candidate in military sciences at the Finnish National Defence University and tactics lecturer in the Department of Tactics and Operations Art in the Finnish National Defence University. His main research interest is currently studying wargaming in operational warfare. He is a career officer since 2001 and has had various appointments in signal, communications and R&T positions during his service in the Finnish Defence Forces.

Pasi Hakkarainen is a former Finnish Defence Forces infantry officer (1996-2000), currently working as procurement manager. He received the M.Sc. (Econ), major in Information Systems and Computer Science, at University of Jyväskylä (2003). He is a cyber security student at JAMK University of Applied Sciences.

Captain **Timo Vestama** has been working as an officer in Finnish Defence Forces since 2001. He is currently assigned to the Western Army Command as a C4 officer. He graduated from the Staff Officer Course 65 in 2013 and after that completed the Advanced Technology Studies Course in the Finnish Defence University. Capt Timo Vestama has also studied Computer and IT engineering focusing on networks and communications and he is currently working to complete his engineering thesis about SCADA cyber security issues.

Kimmo Heinäaro is a researcher at Finnish Defence Research Agency. He received the Master of Science in Technology (Applied Electronics), at Helsinki University of Technology (2005). He has 15 years of experience in technology of tactical C4 systems.

Jussi Timonen is a Ph.D. Student at the Finnish National Defence University and working at the Finnish Defence forces C4 agency. His main research areas are information fusion, common operational picture and situational awareness in critical infrastructure.

Klaus Zaerens is a PhD candidate at the Department of Military Technology in National Defence University Finland. He received his MSc from the Department of Computer Science, Helsinki University in 2008. He has defined and managed deliveries of customized large capacity information systems in the field of telecommunications, finance, traffic and public sector from the year 1999. His research interests include cloud computing, distributed systems and transaction management in a high security environment.

National Defence University
Department of Military Technology
P.O. BOX 7, FI-00861
Helsinki ▸ Finland

Tel. +358 0299 800
www.mpkk.fi

ISBN 978-951-25-2599-7 (nid.)
ISBN 978-951-25-2600-0 (PDF)
ISSN 1796-4059