The nature of security and risk in complex socio-technical systems

A partial application of Critical Systems Heuristics (CSH) to Finnish Security Strategy for Society (YTS)

Juho Reivo
Master's thesis
Digital culture
Department of Art and Culture Studies
University of Jyväskylä
December 2011

JYVÄSKYLÄN YLIOPISTO

Tiedekunta – Faculty HUMANITIES	Laitos – Department DEPARTMENT OF ART AND CULTURAL STUDIES
Tekijä – Author Juho REIVO	
Työn nimi – Title The nature of security and risk in complex socio-technical systems – A partial application of Critical Systems Heuristics (CSH) to Finnish Security Strategy for Society (YTS)	
Oppiaine – Subject Digital Culture	Työn laji – Level Master's Thesis – Pro Gradu
Aika – Month and year December, 2011	Sivumäärä – Number of pages 74 (+8 pages appendices)

Tiivistelmä – Abstract

This thesis explores the relations of security, risk, and to some extent safety, in complex socio-technical systems. Focus is mostly on the societal level, but basic and theoretical structures of systems in general are looked at while trying to increase the understanding about the multitude of interactions that various systems have to each other and how those affect security. Security is identified to being relative and behaving differently in real open system environment when compared to simple systems.

Technology is ubiquitous to a modern developed society, and Finland is one of them. This is why digitised and networked technology and its development need to be looked at the same time as social aspects. As security is a subjective matter, it becomes a matter of how it is managed in social – often political – and technical means. In a world that is constantly thinking of security and risks, where security is often seen or made to seem as absolute and unquestionable, control is less and less in the hands of those who pay the burden for it. It is discussed how systems may be counter productive to security as well as be used to create profit while transferring the costs as even greater risks to the society.

There is a façade of discourse that both precludes citizens from defining on their own which risks they are willing to expose themselves to, and creates the illusion that a group of experts – governmental or not – is the one and only source that should be trusted to define what is best for people. This is deconstructed by reading Finnish government's Security Strategy for Society (2010) while applying a version of Critical Systems Heuristics as framework, for bringing forth some of the underlying assumptions. Analysis of the document shows that in a complex socio-technical system there are several avenues of influence that affect decisions concerning security and risk, and that an individual is not the central benefiter of the security and preparedness systems at the moment.

Asiasanat – Keywords Security, risk, complexity, socio-technical systems, networked technologies, emergent behaviour, expertise, Risk Society, Critical Systems Heuristics (CSH), Security Strategy for Society (YTS)
Säilytyspaikka – Depository University of Jyväskylä
Muita tietoja – Additional information

JYVÄSKYLÄN YLIOPISTO

Tiedekunta – Faculty HUMANISTINEN TIEDEKUNTA	Laitos – Department TAITEIDEN JA KULTTUURIN TUTKIMUKSEN LAITOS
Tekijä – Author Juho REIVO	
Työn nimi – Title Turvallisuuden ja riskien luonne kompleksisissa sosio-teknisissä järjestelmissä – Critical Systems Heuristics:in (CSH) osittainen soveltaminen Suomen Yhteiskunnan turvallisuusstrategiaan (YTS)	
Oppiaine – Subject Digitaalinen kulttuuri	Työn laji – Level Pro Gradu
Aika – Month and year Joulukuu, 2011	Sivumäärä – Number of pages 74 (+8 sivua liitteitä)

Tiivistelmä – Abstract

Tämä tutkimus selventää suhteita turvallisuuden, riskien sekä kompleksisten sosio-teknisten järjestelmien välillä. Käsittely tapahtuu pääosin yhteiskunnallisella tasolla, mutta eri järjestelmiä ja niiden yleisiä sekä teoreettisia perusrakenteita tarkastellaan kokonaisuuden ymmärtämiseksi paremmin. Samalla pyritään parantamaan käsitystä niistä monista yhteisvaikutuksista joita eri järjestelmillä on toisiinsa ja miten ne vaikuttavat turvallisuuteen. Turvallisuus on tunnistettu olevan suhteellista ja käyttäytyvät eri tavalla todellisissa avoimissa järjestelmissä ja avoimessa järjestelmien ympäristössä, verrattuna yksinkertaisiin järjestelmiin.

Teknologia on alati läsnä nykyaikaisissa kehittyneissä yhteiskunnissa, joihin Suomikin kuuluu. Siksi verkottuneita digitaalisia teknologioita ja niiden kehitystä on tarkasteltava samanaikaisesti sosiaalisten näkökohtien ja toimintojen kanssa. Koska turvallisuus on subjektiivinen asia, seuraa kysymys siitä, miten sitä tuotetaan ja hoidetaan sosiaalisin – usein poliittisin – ja teknisin keinoin. Maailmassa, jossa aina ajatellaan turvallisuutta ja riskejä, ja jossa turvallisuus usein nähdään tai saadaan näyttämään ehdottomalta ja kiistattomalta, kontrolli turvallisuudesta on vähemmän ja vähemmän niiden käsissä, jotka viime kädessä kärsivät niistä aiheutuvat haitat. Tutkimuksessa käsitellään myös miten järjestelmät voivat vaikuttaa kielteisesti turvallisuuteen sekä miten niitä käytetään hyödyn tavoittelussa siirtämällä kustannuksia ja kasvavia riskejä yhteiskunnan harteille.

On luotu peittävä diskurssi, jolla estetään sekä kansalaisia määrittelemästä itsenäisesti niitä riskejä joille he ovat valmiit altistamaan itsensä, että uskotellaan asiantuntijaryhmän – valtiollisen tai ei – olevan ainoa oikea lähde, jonka tulisi määritellä, mikä on parasta ihmisille. Tätä dekonstruoidaan tulkitsemalla Suomen yhteiskunnan turvallisuusstrategiaa (2010), käyttäen sovellettua versiota Critical systems heuristics menetelmän rakenteista, tuoden esiin joitain taustalla olevia olettamuksia. Analyysi asiakirjasta osoittaa, että monimutkaisessa sosio-teknisessä järjestelmässä on useita vaikutusväyliä, jotka vaikuttavat päätöksiin turvallisuudesta ja riskeistä, ja että yksilö ei ole keskeisin hyötyjä turvallisuus ja valmiusjärjestelyjen järjestelmistä tällä hetkellä.

Asiasanat – Keywords Turvallisuus, riskit, kompleksisuus, sosio-tekniset järjestelmät, verkottuneet teknologiat, esiin nousevat ilmiöt, asiantuntijuus, riskiyhteiskunta, Critical Systems Heuristics (CSH), Yhteiskunnan turvallisuusstrategia (YTS)	
Säilytyspaikka – Depository Jyväskylän yliopisto	
Muita tietoja – Additional information	

Table of Contents

1. FOREWORD

This thesis explores an endless, somewhat entangled, web. Ideas will be drawn from many fields of research: mathematics, sociology, digital culture, cultural theory, politics, economics, computer and communications technologies, networks, security, organisational psychology and even biology. Taking a peek at fair and even use of technology and networked systems that have become ubiquitous and critical to our wellbeing is like taking a trek down a rabbit hole: there is no certainty where all the interconnectedness leads. When one thread is pulled, at the other end is a network of interconnected topics and views. The field of complexity is a diverse but relatively new area of research. Thus, it has been an excellent adventure to a new frontier, where very few roads have been laid down – and the roads that are there are almost recent and they lead everywhere.

I began writing this thesis in 2008 as a part of RIESCA-project at Laurea University of Applied Sciences. I became interested in this project as I was preparing to work on my thesis to the University of Jyväskylä, where I have studied Digital Culture in the faculty of humanities. The general framework for the thesis idea and topic was formed with this background in mind. After an interruption of being employed by the government in a security role for a time, it was largely re-written in 2011 to its current form, changing some of the earlier approaches and goals.

RIESCA was a Tekes-funded project and done in co-operation with Laurea, the University of Oulu and the University of Kuopio being the main institutions involved. RIESCA stands for "Rescuing of Intelligence and Electronic Security Core Applications". One of the project's main points of interest was national (computerised) critical systems along with critical system infrastructure and information security. Research into these topics is considered important to further enhance Finnish national security (Sihvonen, Knuuttila & Rajamäki, 2010, p. 8-10).

My approach to this topic area reflects the benefit of having acquainted with a number of various "worlds" – or socio-technical systems – with their own cultures and intricacies. Limited military training in aviation and technology spheres; event production and project work stemming from a BA degree from Humak University of Applied Sciences; computer systems and digital culture through work and studies in this Master's Programme at the University of Jyväskylä; and on several levels of security and safety via work, education and research. I have found this diversity useful in exploring the different aspects and views related to the topic area. Diversity of views is also reflected in this thesis on how the subject matter is approached, although this is due to the subject

matter itself as well. At hindsight, one specified field of higher expertise would have been useful for deeper analysis of a more specified target, but in that case this would be an altogether different thesis. This is taking a holistic view on security, risk, complexity and the world we live in.[1]

Support and guidance for this thesis were primarily given by professor Raine Koskimaa of University of Jyväskylä and principal lecturer Juha Knuuttila of Laurea University of Applied Sciences. Additional mental, physical, moral and intellectual support was received – sometimes unbeknownst – from family, friends and colleagues. To each of you, for your part in helping me, I owe my gratitude and give my thanks, one and all.

1 Generally it is considered that things used to be simpler in the past, and that they have gotten more convoluted and intentionally obscured. Perhaps it is because of this that diverse multidisciplinary holistic approach is needed. The topic area is so ambiguous from constant change and development that robust science is a challenge. Academic research in this, and the complexity topic – which can be misunderstood as chaos – remind of quotes from Terry Pratchett's books:

> *"But then... it used to be so simple, once upon a time.*
>
> *Because the universe was full of ignorance all around and the scientist panned through it like a prospector crouched over a mountain stream, looking for the gold of knowledge among the gravel of unreason, the sand of uncertainty and the little whiskery eight-legged swimming things of superstition.*
>
> *Occasionally he would straighten up and say things like "Hurrah, I've discovered Boyle's Third Law." And everyone knew where they stood. But the trouble was that ignorance became more interesting, especially big fascinating ignorance about huge and important things like matter and creation, and people stopped patiently building their little houses of rational sticks in the chaos of the universe and started getting interested in the chaos itself -- partly because it was a lot easier to be an expert on chaos, but mostly because it made really good patterns that you could put on a t-shirt.*
>
> *And instead of getting on with proper science scientists suddenly went around saying how impossible it was to know anything, and that there wasn't really anything you could call reality to know anything about, and how all this was tremendously exciting, and incidentally did you know there were possibly all these little universes all over the place but no one can see them because they are all curved in on themselves? Incidentally, don't you think this is a rather good t-shirt?"* (Pratchett, 1992, p. 7-8)

> *"Mere animals couldn't possibly manage to act like this. You need to be a human being to be really stupid."* (Pratchett, 1990, p. 161)

2. RESEARCH QUESTIONS AND FRAMING

In this chapter the general background for this thesis is looked at, and the different issues connected with the topic are introduced. The research questions are formulated and selected methodology is described. Relevant concepts of the topic area are also presented and explained.

2.1 Background

The discussed topics stem largely from the same shift in global discourse of security that began after the September 11th terrorist attacks in New York and Washington, USA, in 2001. Using the steps laid out by Norman Fairclough, it can be said, that most security related projects in the past decade – and indeed, this thesis – are materialisations of re-contextualised security related hegemonic discourses (Fairclough, 2005, p. 42-43), which continue to develop and shift from that day to far into the unknown. Such far reaching effect it has had that in some ways we are marking time as before and after 9/11. Certainly in the security field (as well as aviation) this is so, and as security has been integrated or identified in almost every aspect of life, many common, previously not security related, things have also been given – consciously or subconsciously – the same time stamp as a side effect.

Before 9/11 views on security and safety were different. New discourses and paradigms had already been in the making for a couple of decades, but they were more or less in the back seat. Afterwards the development was rapid (with emphasis on USA, slightly less in other western cultures and even less in other parts of the world, it seems). And as new hegemonic views of new enemies and threats emerged, it was also seen that old methods and views on preparedness needed updating as well. This process still continues, but it is not only the tangible that we are trying to get the grasp of, according to Beck:

> *"The 11th of September stands for the complete collapse of language. Ever since that moment, we've been living, thinking and acting using concepts that are incapable of grasping those events. The terrorist attack was not a war, not a crime, and not even terrorism in the familiar sense. It was not a little bit of each of them and it was not all of them at the same time. No one has yet offered a satisfying answer to the simple question of*

> *what really happened. An explosion of silence has followed the implosion of the Twin Towers. If we don't have the right concepts it might seem that silence is appropriate. But it isn't. Because silence won't stop the self-fulfilling prophecies of false ideas and concepts, for example war. This is my thesis: the collapse of language that occurred on the 11th of September expresses our fundamental situation in the 21st century, of living in what I call "World Risk Society.""* (Tsilonis, 2002, p. 18-19)

One part of these discourses has been the implication that security is "absolute", that there is only one way to be safe and secure. Often this is accompanied by the belief that only one responsible entity may be the expert on the matter. Security has been presented as beyond negotiation and alternative. This seems somehow parallel to technology, as it is as inflexible as a machine.

Discourses and language are not the only ones developing. Technology and connectivity – internet – are everywhere. We are using more and more sophisticated machines and systems in our everyday life. Our life is by far a life of systems (social security, voting, banks, food production) and shaped by what some apparatus may require (pin codes, filling forms, controlling computer with mouse and keyboard). They are meant to support our living, to make it more comfortable, but machines and systems also make us dependent on them. For western urban people it is a symbiosis of sorts on both individual and societal levels – each needs the other to survive.

Technology and systems are means to organise our lives. There is a feeling that they are getting out of hand. We are creating more new technology, more new systems: technology is accelerating. It not just the newness, but also change and its accelerating rate. Time from drawing-board to market for developed technology has shortened so that checks and assurances of safety have problems (Kirwan, 2001, p. 78-79). The gaps between new technology that "shift the paradigm" have grown shorter and a new jump should be expected. But to what direction? Or has it already begun?

Internet is not only the sum of its technology, hardware and software. It is also a living thing with people inhabiting it and creating new meanings, new ways of using it. It is the prime example of an almost incomprehensible complexity of social behaviour and technology. As much as technology is accelerating, so is it becoming more and more complex from all the new systems integrated together. New technology is creating risks on being new or being different than previous, not being tested properly and adding to the overall complexity of the whole.

People, and the society around us, are worth making safeguards for. Finland has police, military,

rescue services, healthcare and other authorities to have their preparedness plans to support the nation in times of need. General guidelines for all of these are in the document Security Strategy for Society. It is a comprehensive strategy that tries to cover all critical functions needed to sustain Finnish society. This includes both social and technological means and systems, as Finland is one of the foremost technologically advanced societies with a lot of integrated technology. As that technology is part of our structures of interaction as well as support, it stands to reason that while looking at societal concepts, other eye is simultaneously fixed on technology.

2.1.1 New dangers of modern risks

Ulrich Beck has been writing about "Risk Society" for a few decades, but his ideas have not lost their weight – if anything, their reasoning is seen more clearly now. Great disturbances, crises and disasters – the so called low frequency high impact events – are part of coffee table conversations now. Dangers, perils and hazards are not of gods nor demons any more, but they come from industrial, technological, scientific and economic progress. We are able to harness more power, link to so many more and affect the basic fragments of our being that when an unseen glitch happens the effects may be catastrophic. Risk Society is not a single idea but more of a portrayal of the process how these risks are misunderstood and mishandled in our modern constantly self-reflecting world.

Some of the headlines from news in 2011 are direct examples of these risks coming to life. Earthquakes and subsequent tsunami on March 11th showed how nuclear power plants have inadequate safety measures when disaster strikes close enough and is only a step more powerful than imagined. Waves crashed over the barriers and when electricity was down, control was lost from all units. (Jamail, 2011, n.p.) In the United States of America, the September 8th Southwest blackout was not the biggest of its kind but showed how little is needed – one mistake from one operator in one substation – to cause a cascading effect that crossed national borders, shut down several states and nuclear facilities (Medina, 2011, n.p.). A malicious attack to brake equipment at a water pumping station – a critical infrastructure to society – was carried out via computer networks from abroad in November in Springfield, USA, demonstrating how risks can come from afar (Nakashima, 2011, n.p.). Gene manipulated crops have escaped into the wild with the potential to do same kind of harm that any non-native organism can do to an ecosystem – especially as the crops have naturally cross-bred already into a variant that is resistant to at least two herbicides (Coghlan, 2011, n.p.). Not only are these incidents themselves examples of mismanaged risks but also how

potentially catastrophic effects they have, as after the initial incident they enter into peoples lives. Interruptions in services may be fatal in the immediate but changes in ecology via new agents, toxins, radiation or other changes may be much more devastating.

Risks stemming from complexity are in general not handled but relabelled, which only lets them grow and adds to their eventual impact. "Nothing can go wrong, and if something does, there is no danger" is a modern mantra. Modern risks are insufficiently understood as new kind of complex challenges that often propagate from system to system and transcend any national borders. They can be hidden with politically influenced semantics, artificial norms, and transference of their direct and indirect costs from those that cause them to those that suffer them. The impacts are forced on to individual victims, and socially as well as economically the benefits are reaped by corporations. Burden of individual responsibility is lost as decisions of safety and risk are divided bureaucratically into fractions; the organised un-responsibility takes away any clear accountability. Regardless of who may be responsible, and how well-intentioned, greedy or malicious the act, the fact remains that modern societies possess the potential to wreck havoc globally. Beck calls risk societies those that have to face the challenge of having created risks that could, or will, ultimately destroy them (Beck, 1990, p. 97-98, 102, 123) .

2.1.2 Changing ways of social influence

Politics in general, as influence and manoeuvring towards a goal, is as present as ever, even though the political landscape has changed. The manner of taking part in communal and societal affairs has changed and evolved during the last decades. New ways to participate, for example by technologically enabled means, are at odds with systems that make our societies – nation states and our governments – which are build on top of their preceding institutions. The cycles are faster and reflection on actions can be almost instantaneous. Areas of affairs previously seen more or less non-political have been politicised more than before.

No nation is separate from others as goods are imported, and no society is fully out of reach from others. Modern organisations are transcending space and time being everywhere and nowhere by use of information highways. According to Anthony Giddens, three factors have had great significance to social development: the physical environment, political organisation and cultural factors. Of those, political and cultural factors have changed, and physical factors have been much replaced by economic factors. Looking around now, we can be fairly certain that information

technology will be a great influence, but it is yet to find what its future companions look like. (Giddens, 1997, p. 64, 300-301, 522-527)

It seems still safe to assume that politics is one of the main driving forces in social development, while, it too, has developed. People are said to be more individualistic, yet there is longing for shared communities. Ulrich Beck states that individualism has changed its meaning and manifestation, and become reality. It is not the egocentric form, but the self-organising and self-determining kind that does not want to be chained to institutions, expectations, money or the like. Via the treasures of intangible valuables – such as dialogue, friendship, compassion, own time, fun etc. – this individualism has grown to co-exist and co-operate with equal need for communality. Communality and co-operation creates bonds and groups in all levels, and those tight or loose groupings can be seen as activism for that particular (vague or specific) cause. These individualistic interests, and combinations of interests, act as focal points around which new groups gather. That is – at least in a broader sense – political.

More and more things are being politicised, and one can take sides, make a stand or support a cause while shopping, travelling, surfing the net etc. The current generation is politically active in ways that were not considered previously. Not just "freedom" to organise in given ways, but freedom to organise in any manner. The people seem to see the idea of freedom only given lip service from the institutionalised politics, according to Beck. Previous generations, and institutions created by them, seem to handle and understand this current situation poorly. (Beck, 1998, p. 2-9)

While screaming slogans of apoliticality and walking the other way at the sight of institutionally organised political activity, people are actually being most definitely political. New political activity is other forms of involvement, and at the same time this denies the institutions their resources of valuable volunteer labour, money, supporting votes, memberships and so on. The main difference of these two types of political participations seems to be that old social classes, political parties and other organisations are no longer communal groups but interest-groups with their own agendas (Lash, 1995, p. 217).

Modern individualism is not about belonging to old social, economic, education, or national factions but to several more non-specific, changing – and often virtual – groups. This all indicates that people are still very much interested in politics, even though institutionalised politics is often reviled. Also, it can be seen that needs, reference-groups and viewpoints are multiple and much more scattered. If there is a widening gap between those who decide and the rest of the society, is

there truly freedom to determine how one lives, security of expectations, and positive assumption that their needs are being attended?

2.1.3 More knowledge, more complexity

This age of risk societies is an age of knowledge. As Beck states, "*the more modern a society becomes, the more knowledge it creates about its foundations, structures, dynamics, and conflicts*". Knowledge has the bad habit of forcing decisions to be made and contexts for action opening up, which, at times, makes it an unwanted commodity. (Beck, 1998, p. 85)

Our world is getting bigger and more complex every second. One way to measure the size, scope and the increase in complexity of our existence is to look at the amount of data that is created, processed, stored and discarded yearly in this information and communication centric world of ours. A recent study noted that digital universe passed the zettabyte (1 trillion gigabytes) mark last year and at this rate of acceleration, by early 2012 it will pass two zettabytes. While three quarters of information is generated by individuals, 80 percent of it is passed on at least once to some company or organisation, making information both "mobile" and in some way or another influencing others beyond ourselves. This heap of digital files – approximately 500 quadrillion in 2011 – is estimated to grow several magnitudes in the next five years, yet only a fraction more people tasked with managing them will be employed. (Gantz & Reinsel, 2011, p. 1)

In part, this seeming mismatch of knowledge management needs and resources will be handled by more and more powerful automated solutions increasing the amount of meta-data (more information about information) needed for meta-level management. As a curious expression of how complexity works, this will both increase and decrease complexity. More information adds to systems internal complexity but at the same time unorganised is transformed into organised as limited portions are "un-comlexified". (Knodt, 1996, p. xvii-xviii)

Another impact of more and more knowledge is how it changes our perspective of the world. What was previously the realm of tradition, is substituted by science. Social and institutional structures are, and have been, reconstructed to accommodate this new world with constantly changing contexts. Knowledge emancipates, sets us free, with the price of insecurity and individuality. (Beck, 1998, p. 85)

2.2 Structure and methodology, research question

This thesis, that intersects the fields of digital culture and security studies, looks at aspects of modern risks in complex systems. Complex systems are specified to mean socio-technical systems, as modern risks inevitably travel across both territories. More closer examination also reveals that concepts, such as safety and security, are closely linked with risk. A special area of security and safety known as critical systems (which manifest as critical infrastructures) is used to explore the nature of these risks, security and safety, as well as society in the process. Finnish National Security Strategy for Society ([YTS], 2010), that describes the governmental public view of national socio-technical critical systems, is used to contrast the theoretical insights to a more real world. To formulate this as a research question, this thesis seeks to create more understanding of the issues related to security in an increasingly digitising world by asking, what influences security in complex systems.

It is not for this thesis to lay out what (or who) the influences are, but to illustrate that there are influences, and that they are multiple in sources and reasons. Partly, this is due to subjectivity, which is demonstrated for instance in Veikko Heinonen's doctoral dissertation, in which his premise is that security policy perceptions and selections of political actors can not be understood to be derived from singular understandings of meaning of state, security nor ethics (Heinonen, 2011, p. 16). As political actors and other interest groups involved in security, safety, risk and technology policy setting and decision making are not acting with identical ideas, motivations, understanding, or other background – in other words, can not be combined to one context group – one can not expect unanimous endeavours towards common good, nor the good of a particular individual.

This is a qualitative study and follows the hermeneutics research approach (“Hermeneuttinen analyysi”, n.p.; “Hermeneutics”, n.p.; Väkevä, 1999, n.p.). This involves making observations that are understood to have subjective interpretations. Further in this thesis, the subjective nature of reality and observations of systems is supported by employing the Critical Systems Heuristics (CSH) method, which is described later. Before that, the theoretical field of the subject matter is approached using the hermeneutic spiral (“Hermeneutic Circle”, n.p.; “Hermeneuttinen tulkinta”, n.p.), which refers to the idea that a whole can not be understood without looking at its parts, and its parts need the whole to be understood. Thus, it is required to explore both, and alternate between them, to further understanding. The hermeneutic spiral is seen throughout this thesis going from general to specific and back, from big to small, from local to global, from small parts of speech acts

to national policy, from system nodes and links to complex networks. Hermeneutics approach works well in creating further understanding and links between such multidimensional subjects as risk, security, complexity and socio-technical systems.

To support the hermeneutic approach, another methodology is used to assist. Critical Systems Heuristics (CSH) is used in a limited and applied manner as a framework to explore an example case. This is done as part of hermeneutics and in such form, that CSH by itself can not be seen as the methodology for the whole in creating understanding. CSH is a tool that fits well with the intentions of this study and subject matter. It is a series of categorised and labelled questions that explore the reference system's boundary assumptions by contrasting “what is” and “what ought to be”. It is presented more fully before being applied.

The constraints of a Master's thesis limit the depths that this topic area can be explored. Considering the nature and structure of complex systems, it is only possible to explore and include in this thesis an arbitrarily limited portion of a never ending and ever expanding entity. As for why *Security Strategy for Society* (2010) – also know as YTS (in Finnish: *Yhteiskunnan turvallisuusstrategia;* formerly Yhteiskunnan elintärkeitten toimintojen turvaaminen, YETT) – is singled out of all other policies, and undoubtedly high stacks of plans and directives: it is the conveniently collected publicly available manifestation of a socio-technical security system aimed to cover all parts of a society – and thus, very likely, also complex risks. Additional argument for the use of only YTS alone as material is that, such a document is a bureaucratic aggregate, which does not allow meaningful tracing of originators of ideas, or their motivations and reasoning. Any other sources would only add to that (and are thus used sparingly). We would be uninformed which way any singular additional information is biased in relation to the document contents or intentions, but most importantly, how viewpoints have changed over time, which is a central concept in complex systems. Thus, the author sees it prudent, given the intended scope of inquiry of thesis, to limit analysis to the excerpts of this one document to attain (a temporal) glimpse of comprehension.

The structure of this thesis is that, first, the main concepts and backgrounds of the contexts are discussed. After that, the theoretical frameworks regarding topic and context are presented, while shifting towards the real world. After that, a methodological tool is identified and demonstrated as part of the analysis of YTS. Lastly, the observations and the whole are discussed in the last chapter.

2.3 Main concepts

One of the central ideas of this thesis is that anything can be connected to anything, that everything is connected to everything else. It is only a matter of how many degrees of separation there is between them, and understanding that the connection can be made through intangible as well as tangible means. The most interesting concepts here are not the networks and what they connect, but what are the phenomena (security, risk, culture, power, knowledge, and so on) that appear in and around them – although the actual networks (how, and for what, they are used, as well as their structures) affect the phenomenons.

2.3.1 Systems: technical and socio-technical

> *"A system is a purposeful collection of interrelated components that work together to achieve some objective."* (Sommerville, 2006, p. 21)

That straight-to-the-point description of systems says it all. Except, there are different types of systems that do different things in different environments. There are general abstract descriptions of systems but in all cases systems are also context specific and sensitive to both, the effects of the actions and the environment that the system is in. There is no system that is absolutely "*closed*" (computers crash, temperatures and oxidation are the death of any machine after enough time) but complex systems are always "*open*" by definition.

Two different general definitions of systems significant in relation to this thesis (although other systems sub types – biological, ecological, psychological, language, traffic, humans, cars, internet, trade, etc. – are visited) are mentioned: *technical* systems, and expansion of that, *socio-technical* systems. The first does not make in this any particular reference to any particular technology or mechanic. The latter implies in this that social (human) behaviour is part of the system function in a capacity more than mere input/output.

Realising that all systems are somehow connected via technical/mechanical, digital/electrical, human/social or other means, makes defining – naming, limiting, labelling – them ambiguous and arbitrary. In a manner, it is a trick for our benefit – to simplify a complicated matter, make it more manageable (even though ill-defined system will be as ill-managed). From a practical standpoint,

this is the level of uncertainty that we must bare and accept to function. Sometimes this "jump" from one system type to another in the greater system process is used purposefully. For example a so called "airgap" separating internet and a stand-alone network that has a human operator physically connecting them both.[2] This act may be only mechanical but is likely to have some meaning assigning, selection and sense making involved that takes the whole process to the realm of socio-technical.

Another difference that technical systems have is represented considering organically developed versus made systems. In the latter, technical (or bureaucratic ones for that matter) systems are made for a specific purpose in a specific environment. More organically developed systems – such as social traditions or large old software systems – have vague objectives and less efficient means, with possible remnant functions of other systems that have merged with it over time.

2.3.2 Complexity

These are digital times in many ways. Not only in how things are connected, data conveyed and presented, but how all that has also changed our behaviour, culture, points of reference. Bigger, more, faster, and more complicated – all thanks to ever developing science and technology.

Complexity has much of its origins in mathematics. While solving a famous mathematical problem about the city of Königsberg's bridges, an 18th century mathematician Leonhard Euler inadvertently started a branch of mathematics called graph theory. He saw the problematic bridges as nodes that were connected by links, which abide by certain rules and properties. And so it came to be that it was the properties of the network in the graph (rather than a single ingenious answer) that was proof. (Barabási, 2002, p. 10-12)

Euler was not the only mathematician to contribute to network theory. Paul Erdos and Alfred Renyi published very influential papers – of which influences we are still struggling to get past. Part of their influence was to bring graph theory to the real world. Before, it was about regular theoretical graphs that were neat and unambiguous. After, the regular graphs were the exception when compared to irregular and complicated real networks. Unfortunately they worked with the

2 Malicious computer worms Stuxnet and Duqu have caused great concern. The former is considered the first attack designed against industrial targets (factories, power plants, refineries) and to cause physical damage. They both also utilize a new attack vector. They spread to removable media (namely, usb thumbdrives) to intentionally leap to systems that are not connected to networks. In essence, they use not only technical networks, but social (human) networks to spread. (Symantec, 2011, n.p.)

assumption that these networks are random and equated complexity with randomness, which does not hold true any more. Their "random universe", where everything ultimately is average and every node is equally connected, is not so. (Barabási, 2002, p. 19, 22-23)

The most simple and common notion of complex systems is that something is more than the sum of its parts. Complex systems have to be thought of as wholes, and in consideration with their surroundings. Their meanings and functions can not be understood properly by taking them apart to components or out of their environments. (Bullock & Cliff, 2004, p. 4)

When enough separate nodes and clusters of networked nodes connect together, something happens. It is not directly linked to neither the number of components nor to the number of interactive connections between them, as quality of both types of those system components plays a role. Manifestation of new system properties is called *emergent behaviour*. These come in different forms and sizes. Different disciplines still struggle to explain the phenomenon: emergence of a giant component (maths), phase transition (physics), forming of a community (sociology), and so on (Barabási, 2002, p. 18).[3] Complexity is such a system property. When emergent behaviour manifests, that could be used as an indicator that a system has become somehow complex. True complexity still should not be confused with complicated, like for instance what many interconnected large technical systems are (Hanseth, 2007, p. 4-5; Bullock & Cliff, 2004, p. 1).

Technical systems – for instance computer software – have components but lack understanding of their part in the whole of the process, and only process inputs to always produce the same outputs, with minimal additional interaction outside the system. Socio-technical systems do not always produce the same output from the same initial circumstances as they are influenced by the external world. Most notably however, socio-technical systems present emergent properties, which can not be affiliated only with singular components but all the components and all the interactions and meanings between all of them. These interactions, that manifest as emergent behaviour, and both active and passive interaction with outside world, make socio-technical systems often complex systems that can be in interaction with several other systems creating a larger system that in turn can be part of another. (Somerville, 2006, p. 21-21, p. 23)

Another description of complex could be subjective: for instance, when a socio-technical entity, which usually are in dynamic temporal flux, feels too complex for someone to fathom. This could

3 One of the recent addition to this list would be neuroscience as a study concluded that the brain is a highly interconnected complex network (van den Heuvel & Sporns, 2011, p.15775). Mind may thus be an emergent property of that network.

be presented in systems theoretical terms as when one can not keep track and/or control all the changes and meanings that nodes and clusters have (Luhmann, 1996a, p. 24). There are only a limited amount of things that a person can remember and manage, yet it is individual and there are technical aids to assist, as well as methods of simplification.

A subjective stance would not bode well for scientific enquiry, if it was the only way to perceive complexity. It is not. There are several approaches to define and measure complexity, as Bullock and Cliff state in their compilation of examples from other authors: computational versus statistical, structural versus functional, hierarchical, algorithmic complexity – to name a few. Complexity research is still quite new and fractioned area of research. There is a small multitude of definitions and terms which to choose from, depending on which field of science one is inclined to draw their views on complexity. (Bullock & Cliff, 2004, p. 6-8)

2.3.3 Risk, security and safety

Risk is a rather new concept. Before, in the pre-industrial times, there was only good or bad fortune. These were explained by attributing them to gods (external) or personal prudence (internal). Assigning blame to external sources (people, systems, rules, aliens etc.) still to this day is used as a protection from responsibility (Luhmann, 1996b, p. 3).

Niklas Luhmann has tied risk to developing from those old concepts as merchant economy developed, and being fully conceived when modern society came to be (Luhmann, 1996b, p. 3). Risk is still, however, eluding conclusive definition. Its counterpart (not opposite), safety, can be used to somewhat define it (Hollnagel, 2008, p. 221), but that will ultimately lead to a paradox: *there is no absolute safety*. Like a shadow, everything has a risk (and its more positive sibling, opportunity), even though it is not build into anything (Kallinikos, 2007, p. 52). Rather, *risk is an emergent property of a complex system*.

Creation of risk is connected to making a decision – a selection – in a system. In a complex system, there are multiple possibilities for nodes to make connections and those connections to make sense. When there is possibility that the system may produce more than one outcome, of which some are less or more desirable than others, we have risk. We do not have absolute control over any complex system and no absolute certainty of any outcome. Thus, there are multiple variations how to achieve the same goal. The selections exclude some possibilities and activate contingencies in others. These

cause expected and unexpected side-effects. As Luhmann puts it: "*there is no safe way to make decisions*". (Luhmann, 1996b, p. 3-6)

Security is as elusive as risk. We can only say that there are dozens of credible expressions and that most authors agree to it having a positive connotation (Vuori, 2011, s.94). From a linguistic point, security and safety are translated in Finnish language with only one word, "*turvallisuus*". For the general purposes of this thesis and considering the source document, security and safety may be interchangeable, but where distinction is made, *safety is in relation to protection from more immediate harm*, while *security refers to activities taken to prevent harm or circumstances that facilitate it*. Of these two, security is used as the inclusive and broader main concept.

Security is not connected only to aggression, or to bodily or material well-being. *Comprehensive concept of security* is used as a term in Finnish government policy documents. It comprises of military, political, societal, economical and ecological dimensions of security (Heinonen, 2011, p. 61). Vuori also bases his examination of security on the Copenhagen School, from where Finnish government has accepted the aforementioned dimensions, which allows for a wide range of angles in approaching security studies. The Copenhagen School premise is that, security is a socially constructed, inter-subjective and self-referential practice, achieved through speech acts. Vuori contests that, it is not security but *securitisation* that is a speech act, which is used to construct or label security issues – often with political motivations. (Vuori, 2011, p. 9-10)

And if security – and risk – are not politicised outside of their sphere, they can be politicised internally. One dichotomised security discourse would be the discourses of soft (often linked with "social" aspects and "everyday security") and hard (often linked with "technical" approach and responses to bigger threats) security. These discourses can be seen competing globally (aid, support or sanctions versus military action), as well as in smaller circles that have different organisational cultures and objectives meeting, as has been examined for instance in multi-organisational event security setting (Reivo, Vuoripuro & Pelkonen, 2010, p. 127-128).

2.3.4 Relativity of risks and security of complex systems

Complexity is connected to unpredictability and thus to dichotomy of insecurity versus security of expectations. When a system, and thus a structure, is created, it is for increasing the probability of an outcome that is expected. Consider the rule of law in society to bolster amicable behaviour,

mass production to ensure identically acceptable items, postal service as means to convey messages reliably, the uniformity of the @-sign in email addresses instead of guessing which string of characters are for contacting, haiku-poem, or a watch to tell the time at any time of day and at the same rate as all the other watches. And still, no system is perfect.

The more complicated and detailed the expected outcome, the more unlikely it is. The more we allow ambiguity – variety, leeway – the more secure we can be in out expectations. Therefore, most often expectations are formulated only to extent that is needed. (Luhmann, 1996a, p. 307-308). This is not unlike applying the Grecian Maxims' rule of quantity, even though an expectation may not be articulated as speech: only so much is needed to, as the subsequent actions require (Shoham & Layton-Brown, 2009, p. 230). The implication is that risk is related to what is both expected as a result and what is expected of the system. Security, thus, also becomes relative, and happens not only before the fact but also after, in the form of contingencies. Unfortunately, as all the aspects that affect a complex system are not known, no accurate estimates can be made. And even if they can be made with decent accuracy, those would only apply to situations where the system was capable of handling the input (format, manner, size etc.), and not be bypassed by something unexpected.

As complexity creates more and more vectors and conditions for threats, this creates challenges from the point of view of security and scarcity of resources. How to protect a complex system when one can not be distinguished from others systems due to interconnectedness – where to draw the line on what to defend? And when something is selected: what is left out, what are the criteria, and do those affect negatively (or especially positively) on someone or some other systems?

Complexity is generally understood as a problem that needs to be taken into account (Bullock & Cliff, 2004, p. 9). But is complexity always a problem? Complexity can be applied to security in the positive. Sometimes intentionally, sometimes re-imagining a side-effect. Size and amount of complex data and meta-structures may provide some security (via fully or partly intended obfuscation) by hindering purposeful acts as special knowledge and understanding are needed to make any sense of a system. The uncontrollable nature of complex systems can be seen as a safeguard for free speech and action. Complex structures create risks of high-impact events that threaten vast areas via connected secondary and tertiary systems, but at the same time that same structure makes it unimaginable that a big enough truly complex system could be totally wiped out and more likely that parts of such remain intact. These, to name a few, are at least ostensibly benefits of complexity. Yet, they too, only increase the odds and make no lasting promises.

2.3.5 Critical systems, critical infrastructure

Critical systems and criticality, which here mostly refer to perceived importance and non-replaceability, are not to be confused with critical studies and critical approach, which concern themselves with oppressive relations. However, the Critical systems heuristics (CSH), which will be discussed later in this thesis, is of the latter variety, and will be applied to the former. Thematically, they both do share a common element in faults.

Critical infrastructures, in general, are what are needed for systems, and the society, to function, either providing direct or indirect support. Often one system is dependent of others and so is the case with most critical (infrastructure) systems as well, thus creating complex (socio-technical) systems with functional, logical or physical interdependencies. In other words, they are critical sub-systems, usually providing what is considered basic-level service, needed for the whole to operate properly. There are many definitions what precisely are critical infrastructures. One concise description would be:

> *"... arrays of assets, networks (either physical or virtual), processes, and organisations whose incapacitation or destruction would have a severe impact on the nation's security (economic or physical), public health, safety, or any combination thereof".* (Visarraga, 2011, p. 1)

United States, which is the leader in this field, has in one governmental report identified economic markers as common denominators for critical infrastructure: public investment, capital intensiveness and importance to economy (Moteff, Copeland & Fischer, 2003, p. 14-15). A more systems theoretical approach to identifying critical infrastructure is to observe if it performs routine services to other systems, is closely coupled with them, can not be replaced easily, and any interruption would cause serious harm to other systems or humans. The technically inclined have a tendency to limit defining critical systems to only simple purely technical systems, as greater inclusion increases complexity and makes systems harder to manage. In reality, critical systems definition has to be broaden, as technological advances are incorporated, systems integrated and more critical interconnected parts are identified . Egan notes, that under stress – a feeling of imminent danger perhaps – it is more likely that more things are read to be critical infrastructure than could rightly be defended during less stringent times. (Egan, 2007, p. 5)

The politically inclined have had much debate over time concerning societally critical

infrastructures – and before that, infrastructures – without reaching any robust definition. A lot of room has been left to manoeuvre depending on what the speaker has wished to include and what is their frame of reference. This has been seen to lead to convoluted policy or downright intentional misuse while playing politics, at least in the United States. The impacts of the level of accuracy in defining critical infrastructure is two-edged: definitions may create (wanted or unwanted) imperative or possibility to act. (Moteff et al., 2003, p. 10-12, 14)

As can be seen from the broad definitions, and considering both interconnectedness of systems and ever present scarcity of resources, as Rushby notes, it may be necessary to determine levels of criticality on critical systems (Rushby, 1994, p. 49). This, in a way, seems counter-intuitive to critical systems, as they are about the basic needs and thus simplicity. These basics are, however, produced with much more advanced networked systems these days than they may have been historically. Still, critical systems are a special case in systems thinking, as they – in theory at least – represent the bare minimum that is needed for the greater system to function and do its core task. Transferred to real world, this is to say, critical infrastructure is the bare minimum what is needed for society to survive and function. What is left unanswered, however, as selection is implied, is whose and what level of function of basic services (internet, electricity, phone service, water etc.) is deemed critical enough.

In the Finnish government's Security Strategy for Society, critical systems are represented by *vital functions*. Although this term implies its operation is not strictly connected to any specific (technical) system for it to perform, nevertheless, a system is required. In this, preparedness gains flexibility when not committing to only one way of doing things, and as a side effect it releases criticality from some systems. However, this does not remove the criticality of that system that is used to perform the vital function, when it has been selected. Thus, for used here, critical systems hold true.

3. THEORETICAL APPROACHES

The broad subject matter that is approached is inevitably connected to many theories. First is examined the societal context in the form of Risk Society, which grounds to the world. Second, systems theories, structures and security aspects are looked at. Third, the nature and effect of technology are discussed. Lastly in this chapter, risks, risk behaviour, risk management and control are addressed.

3.1 Risk societies and the modern risk culture we live in

Ulrich Beck sees the era of post-industrialism and modernity changing to new modernity without any revolution, collapse or official decree, but via almost inconspicuous high-speed techno-economical dynamics. Even small changes that penetrate all levels of society can have huge impacts (Beck, 1995a, p. 12-14). This reflexive modernity, as he calls it – the modernisation of modernity, the rationalisation of rationalisation – may see progress turning into self-destruction (Beck, 1998, p. 19). It is not only the seen and intended that changes society, but also unseen and unintentional (Beck, 1995b, p. 245). This is the world where we live in.

The reflective practises, and subsequent changes in actions, systems, that follow those observations, are part of the core of modern risk society. We do not only look at what has occurred and what that means as part of history, but what is happening and what that means now to our future. Thus, we are constantly making small corrections while focusing further and further into the future we imagine happening. In this Beck has identified a reversal in our underlying temporal perception. When previously our past gave us a road from present to future, now our anticipation of future (possibilities, risks, contingencies) dictates our present behaviour. (Beck, 2000, p. 100)

Future is pregnant with possibilities and imagining these causal sequences actualising to present is what we anticipate. We create contingencies even though we do not know when these events may unfold – and prepare for those surprises as well. This happens based on our cultural orientations, institutional arrangements and personal preferences. Contingencies are "a cultural belief, a social attitude and a fundamental institutional trait combined". (Kallinikos, 2007, p. 53)

Charles Perrow's classic "normal accident" is recognition of built-in, almost inevitable, risk(s) in

tightly coupled complex systems (Perrow, 1999, p. 5). It in itself is also a bright example, of how risk society has affected us, when we have a phenomenon so named. On the other hand, our "risk aversion culture", as Humphrey calls it, has safety coming first. So much so that accidents are denied out of existence. Every mishap is seen preventable (in hindsight, at least) and so, someone has to be responsible. (Humphrey, 2004, n.p.) Motor vehicle “accidents” are a good example: they apparently only happen if someone has broken the rules. It becomes increasingly difficult to know what a person can do as risks are seen everywhere, and we have started to forbid more and more things in the name of safety and security. Taken to the logical extreme, when everything is a risk and nothing is safe to do, interaction seizes, isolation reigns and nothing can be done. Experiencing risk has become the norm in life. (Beck, 1995a, p. 22, 26; Lash, 1995, p. 193) Risk has become a subconscious fear that "*requires illusion and fantasies of certainty*", as put by Michael Gunder, for us for us to defend against constant feeling of anxiety (Gunder, 2008, p. 196, 201).

Staring only at risk models based on history and calculations will make us blind to unseen threats, that have not previously manifested. Those new risks are played down and are pretended to be quantifiable, even calculated as impossible since they are yet to appear (Beck, 1995b, p. 246). What is problematic with risks threatening societies, is that most of those are slow to appear, latent, cascading, happening on many levels and – most difficult of all – are not noticeable by our senses. This makes identifying and alerting of these threats very difficult, especially when they are beyond the scope of our understanding or imagination (consider 9-11) and quite possibly only explainable by complicated scientific theory, that many can not or will not understand (consider global warming). (Beck, 1995a, s.18)

To understand the true meaning of how this relates to risks and security, one has to appreciate Beck's clarification of the differences in use of terminology of his and his fellow risk society theorists, Giddens and Lash, of "reflection". While the two see reflective modernisation to be bound to knowledge, Beck emphasises unintended consequences (Beck, 1995b, p. 245). While they use "awareness" as a medium, Beck uses "unawareness". Our constant reflections and subsequent actions have ripple effects. However, he emphasises that not unawereness nor unintendedness, mean there is no knowledge – only conflict of who knows and what. (Beck, 1998, p. 90; Ciborra, 2007, p. 27)

Culturally risks have saturated our everyday life, are part of all discussions, all decisions, part of every topic and action (Beck, 1995a, p. 16-17). Beck sees risks, not magically appearing or invented, but (knowingly or unawares) hidden within institutions of every level that are tasked to

protect from them. Risks escape from institutional control creating cumulative and latent threats. His logic is that, as risks are observed, compared, classified, normalised and prepared for, this process does not really eliminate them but only masks them behind a façade of control. As is apparent, this works fine for small, simple and local risks, but as the façade only hides the threats allowing them to slowly grow, they become big, complex and multi-area or even global until the veil is lifted and the dam bursts. Views by Pidgeon and O'Leary concur with this, emphasising how social and cultural aspects of organisations facilitate these build-ups (Pidgeon & O'Leary, 2000, p. 16, 18).

This part of risk society behaviour seems to be even in Beck's view the result of historical development. Objections and counteractions to this status of affairs have been seen. The nefarious aspects that he seems to see in it, are the opportunities for exploitation of this system by tweaking classifications and threshold values, which allows hiding new risks by "administratively renaming" them as "not-risks", and therefore as something that someone other than the one causing them must share and endure. Thus, the problems of risk society are twofold. First, we as societies rather deal with effects than real causes of threats – and even if we do, only as far as we can feel, imagine and understand them. Second, the uneven use of power (and transference of costs to others that follow) in institutional structures build to counteract threats, which actually may end up creating only bigger risks. (Beck, 1990, p. 97-98)

3.2 Systems and socio-technical systems

Systems can not properly be discussed without defining their environment. Environment is not limited by boundaries. It is what a system excludes itself from, yet it includes every other system besides the reference system itself. Even though one can not exist with out the other, environment is not dependent on systems and systems have only limited possibility to affect the environment. No system can determine the full relationship between another system and its environment. (Luhmann 1996a, p. 17-18)

> *"Everything that happens belongs to a system (or to many systems) and always at the same time to the environment of other systems. Every determinacy presupposes carrying out a reduction, and every observation, description, and conceptualization of determinacy requires giving a system reference in which something is determined as an aspect of either the system or its environment. Every change in a system is a change in the environment of other systems; every increase in complexity in one place increases the complexity of the environment for all other systems."* (Luhmann, 1996a, p. 177)

This can be put in other words with an example. The infinity and complexity of the system called "the world" (or “the universe”) is demonstrated in trying to produce knowledge of it. Our knowledge will always be incomplete and the more knowledge we produce, the more we add new knowledge and complexity to the world. (Hanseth, 2007, p. 7-8) As no system is capable of the same level of complexity as its environment ("*such a condition would abolish the difference between system and environment*"), systems are necessarily selective and capable only to both limited representation of its environment and itself (Luhmann, 1996a, p. 25, 182).

Systems can be decomposed in two ways. First method sees them as formed of subsystems ("internal system/environment relations"). Second method sees systems composed of elements and relational links between them. The difference is, as Niklas Luhmann explains, akin to a house being composed of rooms (which are used for different purposes) in the former, and of nails, bricks, floorboards etc. in the latter. This has significance when measuring complexity. One way is to count the elements and the relations between them. This does however turn relations to only quantifiable links while stripping them of meaning, which the rooms represent in the example. (Luhmann, 1996a, p. 21)

When there are too many node elements for everyone to connect to every other, selection must occur, which implies contingency, which in turn is shadowed by risk (Luhmann, 1996a, p. 25). "*Something is contingent insofar as it is neither necessary or impossible; it is just what it is (or was or will be), though it could also be otherwise*", as Luhmann defines it (Luhmann, 1996a, p. 106). Selection is generalisation and thus system assumes the risk in the form of insecurity of imperfect knowledge (Luhmann, 1996a, p. 327).

The imperfect knowledge is used by socio-technical systems – like communities, risk societies – as they are self-referential, self-reflecting (for example administratively, judicially, via media and so on). In a simpler manifestation, a system only recognises the difference between itself and its environment. Otherwise there would be no reference point to understand anything, to create information (Luhmann, 1996a, p. 9). In the complex, systems constantly reassess themselves and make a multitude of corrections to their previous course, applying the same principle.

> *"We term hypercomplex a system that is oriented to its own complexity and seeks to grasp it as complexity, because the attempt – since it occurs within the system and must be established as self-description – produces more than itself. It also creates new kinds of possibilities for unseen reactions. System planning necessarily produces hypercomplexity. Planning that experiences this will attempt to include it in its planning: that is, will plan itself and its effects together. Thus budget planning creates exaggerated reports of needs, and the one who is planning can take this into consideration. But what holds for a reflexive planning of planning holds for planning pure and simple: it can be observed, and therefore it leads to possibilities of reacting to its own observation of planning, but not in ways that were originally planned.*
> *Since the difference between planning and observing planing cannot be eliminated – however much planners would like an "invisible hand" – there can be no point of equilibrium in the system for this difference or for the tension it creates. "* (Luhmann, 1996a, p. 471)

3.2.1 Structure of connections

System descriptions *linear* and *complex* are descriptions of levels of interaction: communications between network components (Rushby, 1994, p. 42). The structure of society is a network, and network logics boosted with ICT enabled pervasiveness *"substantially modifies the operating and*

outcomes in processes of production, experience, power, and culture" (Castells, 1999, p. 468). As Lash sees it, old societal structures are been replaced by structures of information and communications (Lash, 1995, p. 154). And Ciborra puts it as plainly, albeit in a more security oriented framing:

> *"Digital technologies are technologies of representation that can be used to augment other techniques or representation, such as risk calculation and management. Taken all together, these are powerful tools to represent, calculate, control, mitigate, reduce and transfer risk"* (Ciborra, 2007, p. 25).

Whether digital or face-to-face communication, global community is the open environment where connecting bonds must be made (Giddens, 1995a, p. 149). Connections in a network are made between nodes (people, computers, routers etc.). A clustering coefficient is obtained by dividing the number of actual links between nodes, that are connected to our observing node, by the number of links there could be between them (if each node is connected to all the others). It measures clustering and how tightly connected a cluster around the observing node is. A random network has a very low clustering factor compared to an interwoven network that is biased to work, collaborate, act and communicate together. *Societies are thus not truly random*. (Barabási, 2002, p. 46-47, 51-53) To emphasise how non-random complex networks really are, the large hubs that have central position and are connected to several clusters, have the statistical probability of being random "*smaller than the chance of locating a particular atom in the universe*" (Barabási, 2002, p. 62).

Distribution of these connecting links follow a mathematical expression called a *power law.* While most nature's quantities follow a *bell curve* that is peaked in the middle (illustrating that there are only few extremes and a lot of average), a power law distribution (also called a *scale-free network*) is a one-sloped decreasing curve that illustrates the existence of a few rare large events (or in this case heavily interconnected hubs) and a lot of small ones (or, single nodes with only a few links). Clustering is not only a unique societal property but ubiquitous generic property seen from molecular level to economical to ecological networks. (Barabási, 2002, p. 67-68, 71)

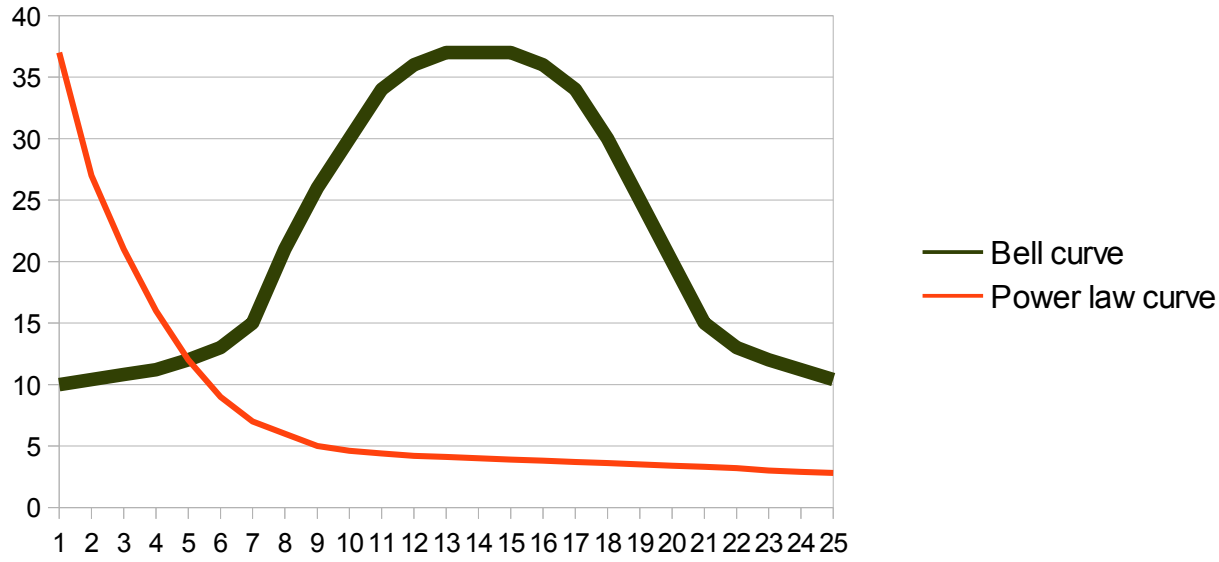

Fig. 1. Example illustrations of a bell curve (drawn here with a thicker line) and a power law curve. A bell curve, which is named after its shape, depicts an emphasized "average" in the middle of the curve and relatively few extremes in both ends of the curve. A power law curve depicts emphasized extremes: the few with many (left end of the curve) and the many with few (right end of the curve).

Open networks have no limits on expanding as long as they have similar enough codes for communicating with the other systems nodes and clusters they integrate with. The nodes connecting networks become positions of power used to "*shape, guide and misguide societies*" (Castells, 1999, p. 470-471). The codes – made of cognitive homogeneity and standardised information – are simplifications of scattered discontinuous cultural reality and facilitate transporting risks (Kallinikos, 2007, p. 67). In other words, shared experiences and reference points – news feeds, religions, political events, and other cultural texts for example – that influence how we feel and relate to others are used to control how (or if) these systems connect to others (others being us as individuals or as links to greater networks).

The much popularised, but misunderstood, "six degrees of separation" between all people has a mathematically calculated equivalent for the internet: the average distance between any two documents online is approximately nineteen clicks. The number was found to be proportional to the logarithm of the numbers of nodes in the network. These *small world effects* and small separations are apparently present in every network. The level of high interconnectedness is a sign of a network that has surpassed its critical point where nodes are only connected by around one link on average.

As more links are added the average distance collapses fast and within a few steps almost all nodes can be reached. The amount of nodes in a network does not significantly increase the average distance due to the logarithmic term: a hundred times larger network only has two degrees higher separation than a smaller one. This however does not mean specific nodes – people, documents etc. – are easy to connect to if we are not somehow biased towards them. Testing all the links of all the nodes that are met by following all the links of all the other nodes quickly rises to exponential numbers which simply is not feasible. We can not test all the connections. It is *not a random selection* we make when we follow a link towards our intended goal. (Barabási, 2002, p. 33-35)

Finding our intended goal is also challenged by the fact that socio-technical systems are socially constructed and in a state of constant change (Reiman & Oedewald, 2007, p. 749). This is very true in human societies. When organisations and socio-technical systems are discussed, however, this is not always expressed. Some do not deal with this aspect, some ignore it, but most often it seems the dynamic nature has been internalised and understood in the use of the word organisation, although with slight variations. Organisations as complex systems could be compared to measuring particles in quantum mechanics. Heisenberg uncertainty principle (“Uncertainty principle”, n.p.), in simplified form, states that one can only either measure their position or their momentum. This reflects how Reiman and Oedewald summarise many in recommending it would be more appropriate to speak of organising instead of organisations. As they put it: "*what we perceive as an organisation is the (temporary) outcome of an interactive sense-making process*". Likewise, they describe organisations as "emerging patterns" of activity, where incomplete information is used in collective perpetual reality-building process. (Reiman & Oedewald, 2007, s.750)

Barabási's mathematical view supports this. In his terms, organisations are order, and order (instead of natural randomness) begins to form when nodes begin (to have reason/bias) to interact/connect beyond their immediate vicinity. This is when emergent behaviour begins, or using a physics term, a phase shift occurs. (Barabási, 2002, p. 75-77)

Organisations and societies are not stable. The structure of nodes and the links between them is not permanent. In a way, it is only a question of measure and quality of instability. We can only observe either the current state of an organisation or the rate of its change with any accuracy. This presents any number of challenges when dealing with risk, complexity and society.

3.2.2 Perceptions and management of risks

How systems are used impact how risks present themselves in systems. Tight and loose couplings refer to "*metaphorical slack or flexibility in the system*" in its parameters for it to operate. Coupling implies that there are at least two entities that are somehow connected. John Rushby lists loosely coupled systems being usually less time sensitive, more tolerant of unexpected behaviour, more adaptable for new purposes, are likely to function in a changed environment, and allow human intervention if a fault occurs. At the same time, tight couplings are more efficient and produce more expected output. (Rushby, 1994, p. 42-43, 45)

Defining terms related to risks is also a challenge. Failure of and in a system can be a matter of availability, reliability, safety, or security, to name a few. But even if observing these are limited to only a narrow field, like computer systems, there are still varying interpretations of each of those system properties. It may therefore even be a challenge to identify whether there even is any fault. Maximising dependability is "*to maximize the extent to which the systems works well, while safety ... tries to minimize the extent to which it can fail badly*", as Rushby puts it. These goals may even be at odds. Due to this ambivalence, a system may be operating reliably, as it was meant, but still be unsafe – at least in certain scenarios – and vice versa. One example how to deal with such problems would be to transfer risk to the social realm and individual operators with user instructions, warning labels and legal disclaimers. (Rushby, 1994, p. 9-10, 14)

Risk is inevitably linked with social definition, as are its derivatives. As Pidgeon and O'Leary explain Turner's views, a disaster is defined with social terms, "*as significant disruption or collapse of the existing cultural beliefs and norms about hazards*", and not by its physical impacts (Pidgeon & O'Leary, 2000, p. 16). The negative outcome is mostly not the worst possible due to the imperative of system design, which aims to produce good outcomes and creates a bias for a positive end result (Hanseth, 2007, p. 5). Ciborra offers a sharp insight to differences between technological and social understandings of risk:

> *"Purely technical assession is binaric* functions / doesn't function *where unwanted occurrancies can be seen as "features" of a system. On technical side, it may not be clear to whom the risk is limited to or what level of harm it may produce (on social side). In an economical and social view risk is thought in terms of the the level of satisfaction or dis-satisfaction to an outcome."* (Ciborra, 2007, p. 33)

Even though risk has an accepted definition, that becomes more convoluted the more the definition is explored further. Risk is often defined as the combination of *presumed hazard impact severity and possibility of that hazard actualising* (Rushby, 1994, p. 11; Hellström, 2007, p. 420). Related concept of security is connected to *expectations becoming true*. The more we allow ambiguity – variety, leeway – the more secure we can be in our expectations. Therefore, most often expectations are formulated only to extent that is needed. For risk this means that if expectations are made ambiguous, they are less risky. (Luhmann, 1996a, p. 307-308)

Looking at risks "backwards", from what has been written of safety, we can see some properties of socio-technical systems that can influence risks. Reiman and Oedewald echo other researchers in saying "*safety is as much an aspect of practice as is any element that makes a skillfull worker*". Safety, in general, is thus not knowledge but how that knowledge is applied. If safety is dismantled to only tangible parts or separated from its context, it disappears. (Reiman & Oedewald, 2007, p. 748-749)

Risk calculations force qualitative aspects to be quantified. An example about how risks are calculated is to look at one of the salient mathematical definitions of risk from the works of Kaplan and Garrick. Their "set of triplets" is a risk equation consisting of scenarios, probability and measure of damage. Scenarios in this refer to listing of all the possible things that can go wrong. Measure of damage may mean any number of things, although a common convention is to convert any value (be it human life or machine parts) to monetary value, which is highly subjective and often ethically challenged. Probability in the equation is explained as being the subjective understanding that may or may not include supporting statistical data, but which ultimately rests on the "educated guess", and may be influenced by different factors. Derived from that, as probability is subjective from the point of view of the observer, then so must be the risk. (Kaplan, Garrick & Apostolakis, 1981, p. 944; Ciborra, 2007, p. 28-31, 35)

Despite the written reservation even in the original equation, stating that thought should be given also for events not listed (Kaplan et al., 1981, p. 946), and though in their later work the scenario component was broaden to be more complete via methodological change in the equation (Kaplan, Haimes & Garrick, 2001, p. 808), the risk estimates still depend on pre-determined lists of possible fault scenarios and does not offer viable solutions for unforeseen scenarios. Not only would there be need to map out all single component malfunctions, but also all the combinations, which would create an exponentially growing scenario table (Kaplan et al., 1981, p. 946).

Thus, Kaplan and Garrick's model is useful only in non-complex technical systems and should not thoughtlessly be applied to socio-technical systems. The "set of triplets" equation of risk is not in fault in itself, but one must observe that each of those triplets is highly prone to distortions and fits poorly to systems with "welter of societal aspects", as they themselves note (Kaplan et al., 2001, p. 814).

Another mathematical approximation is the so called “80/20 rule”. The popular understanding of it is that only about 20 percent of a quantity is responsible for the 80 percent of impact. When it actually applies, there is the mathematical expression *power law curve* behind it. Power law curve shows mathematically how few large events generate most of the impacts of risks, and how there are considerably more and more of lesser and lesser impact risks. To put in another use, few major hubs that have many connections to lesser hubs (which connect to even lesser hubs or singular nodes etc.) can be seen near the end of a power law curve peak. These hubs, that fit to the "20", are valuable as targets for malicious acts due to the perceived disruption they would cause to the system. (Barabási, 2002, p. 66, 70, 72)

Highly interconnected networks will not suffer much impact from losing a couple of nodes or a hub. Loss of functions is not a gradual process either. Only when enough nodes have been removed, a critical point is abruptly reached, beyond which the remaining network breaks to unconnected islands. The so scale-free networks that abide the power law are resilient to random removal of nodes (failures) due to the inherent property of their system topology. However, targeted removal of bigger hubs will affect the network much faster and make otherwise safe system seem fragile. In all cases, it has to be noted, small nodes are affected disproportionately. Transferred to real world, this can be concluded to imply that individual people are at more risk being affected in the event of disruptions in any systems. (Barabási, 2002, p. 112-113, 114, 116)

To paraphrase Little, designed security and safety of any system is only effective if the threat and design intersect (Little, 2004, p. 57), and this applies to societal level also. It is here that we should be reminded about the "Law of Standards" coined by John Sowa (Sowa, 1991, n.p.), which basically states that people almost always adopt a system that is simpler than the intended one, and of Roland Barthes', who “killed the author”. Barthes explained how the author of any text (which can be taken broadly to be anything from a tangible work of art to a system design) may have intended to mean any number of different things that the user/reader/experiencer may never know (Barthes, 2002, p. 223). It is more than likely that the "readers" of the "text" misinterpret it and apply it to suit their own new and current needs via their own background, situation and

capabilities. These explain – in part at least – for instance the gap between design and user experience, why systems do not work properly, why even well defined systems may be a risk, and why end results may not be as expected. Also, the prevalence and preference of simple systems (Ciborra, 2007, p. 41).

As Giddens lists a few of the characteristics that bureaucracy (Giddens, 1997, p. 287) projected to computer programming, identified by Max Weber, one has to wonder if something of these same characteristics have reflected back to us, because we have the tendency to conform according to the systems we use. Outcome over undeviating operation, or personal and inclusive instead of detached and exclusive, could be very welcome change. Loss of long linear clear-cut hierarchy and inflexible bureaucracy would be a threat to systems that depend on them, not to the existence of societies. From risk perspective, this would likely increase insecurity of expectations for processes and perceived insecurity, but end result seems less clear cut. A less rigid system may reduce unintended consequences.

User experiences of socio-technical systems vary. If a system has features that users (or operators, or clients – depending on the viewpoint) do not consider beneficial or useful (including faults), they may go around or even start permanently working around these problems. This will prevent the experience of these features, but also impact the system processes. (Sommerville, 2006, p. 55)

For security and safety – meaning expected outcome – there are measures that can be taken to ensure adherence to system. Actual and figurative barrier systems are used in internal as well as external prevention as well as protection. Barriers may be physical (against energy, material, people), functional (pre-conditions before action; changing the state of something), symbolic (signals, warnings, signs etc.) or incorporeal (rules, procedures, customs etc.). Some barriers are more social constructs than technical, but all require some social constraint – ethics, morals, fear of punishment etc. – for them to work absolutely (or at all). These methods are amoral and are often used in a combination for anything: to define, limit and protect organisations, power, critical infrastructures, data, freedoms – physical objects and ideas alike. (Hollnagel, 2008, p. 225-227)

Barriers only increase the odds of security and safety. But when it comes to finding viable means to genuinely eliminate risks of complex systems, for instance Hanset and Ciborra concur with Perrow's recommendation: "do not build them!" (Hanseth, 2007, p. 10). This, it seems, is unlikely in our current society.

3.3 Technological development and critical systems

Hellström defines infrastructural criticality as strategically connected systems that "*focus society's total vulnerability to a few particular points in the system*". Not only are the services of these systems required, but adversely, because they are required, they become the weak point. As risk analysis needs to define critical infrastructure broadly when preparing for "dynamic pressures" that disrupt society, from the perspectives of vulnerability reduction and economical efficiency of management, pinpointing is crucial (Hellström, 2007, p. 427).

Egan charts criticality with five levels depending on the consequences of failure. Two notable attributes are approximations that indicate how almost inversely comparable amount of technology is to the likelihood of it being a large technical system. The more critical the infrastructure, the more likely it is that it is a large technical system. Yet, great majority of technology is simple, small and not considered critical. (Egan, 2007, p. 11)

> "*Technological change can reduce some risks while aggravating others or even creating new ones. Three aspects of emerging technologies will influence risk: connectedness; the speed and pervasiveness of technological change; and the fundamental changes in the landscape they might induce.*" (Organisation for Economic Co-operation and Development [OECD], 2003, p. 12)

While we advance our technology, we at the same time create new risks. One can not be without the other. It seems that we can not cease to innovate, but at the same time, as Hellström asks, "*whether the human (physical) condition only can be improved at the expense of a heightened social and psychological anxiety*" (Hellström, 2003, p. 380)?

One reason that risk have shifted from low-impact/high-frequency incidents towards high-impact/low-frequency events is digital technology and computer systems. (Ciborra, 2007, p. 26; Kalliniakos, 2007, p. 58-59). Technology has had considerable impact in this. Our culture's prominent new feature is the timelessness that technology – particularly digital communication – has presented us (Castells, 1999, p. 462). Technology has also in essence gathered all the figurative eggs of and via systems in the same basket and then hung all the baskets together in the air with a few connecting threads. This poses considerable risks as a feature of technical systems is that they are incapable of dealing with unexpected events. What is not meant to be processed, it excludes.

"*Technology can not handle (that is absorb, creatively react, ignore, forget, or dissimulate) unforeseen incidents, even though technologists attempt to construct systems that respond to emergent events...*" (Kalliniakos, 2007, p. 55).

An example to demonstrate the differences of a technical system would be a board game. Basic game play is simple following of logical rules. Contingencies, thinking several steps ahead, are still within the grasp of an advanced machine, and still within the system's designed limits. A truly creative adversary – or foe with malicious intent – could entertain the notion of using solutions outside the overt rules, specifications and algorithm of the system (which may or may not be good for the game). The same effect would be from overwhelming forces of nature or any other unconsidered event akin to a relative deus ex machina. Technology's limitation lies in the functional closure as well as its simplification: "*we can deal with reality by simplifying this into a closed domain and specify how the technology can deal with each element in this domain and its states*" (Hanseth, 2007, p. 7-8).

Some of the unforeseen can be counteracted by creating some leeway, flexibility or margin in to the system. Ever accelerating cycles of research and development this may not be possible. When Kirwan explains Hudson's four perils that accelerating development of systems create, we can see that at least two of those also have much meaning – even outside technical realm. One is about how systems – and therefore system users – move closer and closer to "the edge" the safer the systems become and thus leaving less and less margin for error in a failure. The other peril is about how much further and further the designers of the systems are from the users and real use. Response to them would be better situation awareness (a new system) and involving users more all the way from the beginning of creating systems. (Kirwan, 2001, p. 84-86)

Complexity of systems, especially heavily technical, is also partly due to mixing and layering of newer technology on top of older. Despite influence of technology on complexity, managing critical systems is not only a technical issue, but equilibrating social needs and resources without causing undue interruption (Hellström, 2007, p. 418, 426-427). This balancing act comes to view particularly when looked at critical infrastructure that is in private hands. Investing in resilience is justified if, and only as far as, regulation demands it due to its economic inefficiency. Share-holders have no motivation to support such actions. (Egan, 2007, p. 14)

In the 2003 report about critical infrastructures for the United States congress, it was noted that, even though critical infrastructure implies indispensable uniqueness, even these systems have to be

prioritised (Moteff et al. 2003, p. 12-13). This is due to lack of resources that the country has, but also for the overuse and politicized misuse of the term. But even because of system design, when system is deemed critical, simultaneously some components or properties of it will be more critical than others. Holmstöm notes that systems are generally constructed so that most of their parts are needed for system to function, and "*being critical part of a system is a normal state of being to most parts of any system*" (Hellström, 2007, p. 420). This is true for basic human designs, while natural systems display much more tolerance to sustain basic function in disruptions. The common feature for tolerant systems seems to be robustness via high interconnectivity. (Barabási, 2002, p. 110-111)

"I*n general, safety-critical systems benefit by having few, linear, and known interactions, and and from loose coupling*", states Rushby, and continues contributing predictability to linear interaction and how that "*facilitates comprehension of the behaviour of the system*". Unwanted or unexpected interactions may cause hazards or security concerns. He notes, with computer systems in mind, that simple internal interactions may not be possible when loose couplings are wanted, but takes up a general position on the side of simple interactions. This may not always be possible if additional safety and dependability measures add interactive connections (Rushby, 1994, p. 45).

When technology matures enough and becomes complex enough, it becomes part of the socio-economic domain and can not be separated from it for study nor control. And there is difference in how much change different types of steps forward in technical evolution bring forth. Change may be incremental innovation, radical innovation, transformation of system, or change in the techno-economic paradigm, as Hellström sums up Freeman and Perez. (26 Hellström 2003, s.370-372)

"*The philosophy of laissez-faire – it's safe, as long as it has not been proven to be dangerous; and the philosophy of precaution – nothing is safe, as long as it has not been proven harmless*" (Beck, 2006, p. 10). The question of safety ("Is it safe?") is in a manner of speaking displaced in modern research and development. When previously any R&D project would be tested in a lab before production, now the opposite hold more true. Production comes first and proof of safety (and/or security) after. Effectually safety is presumed and empirical testing only enforces those presumptions by checking only what is presumed safe. Particularly dangerous complex systems can only be tested insofar as which parts are presumed safe. (Beck, 1990, p. 179)

Rushby writes about measuring risk of highly ("ultra") critical computer systems, that their failure rates are (or lack there of) are impossible to validate properly. He goes on to say that, "*...the requirement for ultra-criticality is so many orders of magnitude removed from the failure rates that*

can be determined empirically in feasible time on test, that essentially all our assurance of has to come from subjective factors...". In other words, it is impossible to calculate the fault levels of the most important systems (in the time allowed), and that is why the design, creation, implementation and upkeep methods and processes – as well as the people behind them – need to be evaluated to gain some level of assurance. The more critical the system, the more rigorous the control system needs to be. (Rushby, 1994, p. 37-38)

The time from development to market has shortened drastically and this has created problems for guaranteeing safety. The first (or internal) part is about using enough time beforehand to test new technologies before commercial pressure pushes them to the market. The Second (or external) part of the problem is the lag that regulation has in relation to new technology. New regulation has to wait for proper testing and verification and after it has first been made official, it will take time to mature. Old regulation may not cover the new while bureaucratic system plays catch-up. In addition to this, Kirwan notes also that not only is needed proper understanding of the technology but also how the human operator is affected and what influence the "acceleration/deceleration of commercial interests" have. (Kirwan, 2001, p. 78-79, 88)

Even though humans have been called the weakest link, there is a strong perspective on how technology is failing humans in helping us do our part of security and safety, as technology is riddled with problems in user interfaces, usability, increasing demands, insufficient training and knowledge of systems (Brostoff & Sasse, 2002, p. 41-42). These problems do not appear out of air. What shields us from overly technologicated existence is our failures. Although human errors are said to be the cause of many a mistake and catastrophe, existence of our capacity to fail is mandatory for our self-preservation instinct. Humans make errors. To the systems we design and build, and in how we use them. This will never change, and that should keep us healthily wary of technology. (Beck, 1990, p. 184)

Technology has a considerable impact on our daily survival – one way or another. It has become ubiquitous. Although we give it meanings, it still is only part of the socio-technical system, and (for the moment at least, before true artificial intelligence) only the supporting structure that can not function on its own. But to understand complexity, writes Barabási, we have to move beyond the skeleton of the network. The focus should be on the dynamics, relations and processes within the connecting links. (Barabási, 2002, p. 225)

3.4 Risk out in the world

The actualisations and perceived risks to the real world can be read from official reports. Complex risks pop up in them more and more. One comprehensive and influential report (in which Finnish experts also participated in creating) about risks of the future in globalised world is by the Organisation for Economic Co-operation and Development (OECD, 2003). It names four contexts of risk, that will have most affect in the near future: demography, environment, technology, and socio-economic structures. In summary, these will be the reasons why conventional hazards and vulnerabilities will become new risks, and why more powerful ways for risks to shift in systems, time and place appear.

What we have waiting for us in the future, according to the report, is that population will grow by half from current 6 billion to 9 billion by 2050. As many as 3 billion more people may live in cities creating large concentrations of population and assets increasing the likely impact of any risks. Increasing poverty and social inequalities have adverse effect to risk mitigation. Global interconnectedness of transport, trade and information systems networks have positive impact to information gathering, processing and communication (including emergencies) but also provide more ways for negative effects to propagate. Technologies involved in cellular and genetic level advancements may have consequences that current level of understanding can not foresee and there may be irreversible damages. Several different level private and governmental, local and international institutions are influencing policy and attitudes and conflicts of interests hinder managing risks. Mass media influences risk perception and the tendency is towards entertainment value instead of information. Global warming is likely to increase the frequency and intensity of extreme weather events and the general reduction in biodiversity is likely to intensify other negative effects. (OECD 2003, p. 10-13, 37-49)

Using the report's views as a reference point, we have a more global picture of risks. For the most part, it is much the same that Ulrich Beck was already two decades ago underlining. The reports findings seem to confirm that the numbers of natural, technological and health related disasters have and will rise rapidly in recent decades (OECD, 2003, p. 33-36). Although Ulrich Beck's early risk society rhetoric is thick of heavy ecological message – not without merit – the observation provided by Giddens about it is interesting one. Ecological problems, damages, mishaps and crisis are in fact indicators of many other, often even more complex, problems that are not ecological (Giddens, 1995b, s.255).

Both the causes and effects of major impact risks are complex, not to mention so profound that after them, there is no going back to the world that was. Nuclear disaster, ecological alteration with toxins or genetic changes, wildly spreading nanotechnology – these are examples of major threats that are often used by Beck. Normal risk logic, standards and measurements are void with these level of events. *Firstly*, time and place do not restrain these events: there is a beginning that may be seen only afterwards (latent) but the effects have no meaningful end. *Second*, damages (primary, secondary, tertiary etc.) will be global, dispersed, source is hard to pinpoint and indemnifications are impossible. *Third*, when effects are so all inclusive and massive, there is no real way to set up in advance any mitigating after-incident care or control, as nothing could stand in their way. This leads to – has led to – after-compensation being replaced by preventative measures. But this only works with recognised risks and risk levels. "*Not only is prevention taking precedence over compensation, we are also trying to anticipate and prevent risks whose existence has not been proven*", as Beck clarifies it. (Beck, 1990, p. 163; Beck, 2006, p. 5-6)

> "*Here* [industrial consequence society] *there is inequality; poverty attracts risks. But the inequalities diminish in the global surplus of risks. Pollutants do not spare the drinking water of directors general*". (Beck, 1998, p. 25)

The side effect of complexity make us more equal to one another. One of the similarities that connect people globally are shared global risks, as morbid as that may seem (Beck, 2006, p. 2). Yet, if looked closer, for example dominant European and United States governmental risk beliefs and issues are not the same and clashes are unavoidable. And as Beck also suggests, risks of the western Europe are not the same risks that poor parts of Africa or war torn areas of Asia suffer. The uncertainties and threats that we suffer have reduced hugely, in comparison with them, therefore allowing us to concentrate on developing "*luxury risks*". Many of the risks that we face are caused directly or indirectly by the advanced technology used to support our lifestyle. (Beck, 2006, p. 4, 9)

In the survey conducted on behalf of the Advisory Board of Defence Information (MTS) of the Finnish Ministry of Defence, Finns were asked among other things about security and risks.[4] In addition to question related to it, two questions in the survey were directly about terrorism, which offers itself to show how we approach risks. Terrorism (risk) and counter-terrorism (counter action; not opposite nor counterbalance) have been in vogue for the past decade in security discourse. They have been spoken about globally by policy makers but the implications have changed over time.

4 Approximately two-fifths expect world to be more insecure, against one fifth that saw future in positive light in the next five years. In this survey can be seen that approximately half of the risks that were deemed current and surveyed, were not related to basic needs, but are related to or stem from more complicated situations. (Advisory Board for Defence Information, 2010, p. 13-15)

First there was action and reaction, but later there have been signs of having the emergency and threat been kept alive and upfront and used to political ends. As Humphrey says, "*counter-terrorism seeks to achieve the impossible, a risk free world for our risk aversion culture*". Needless to say, no strategy can remove risk from existence. (Humphrey, 2004, n.p.)

This can also be read from Perrow's *normal accidents*, which one can expect in certain systems. One of the classic examples of these simple risks actualising as a complex hazard was the Three Mile Island nuclear reactor accident. All errors in design, in equipment, by operators, in procedures, and in operating environment were small in themselves, and all systems had backups because hiccups were seen possible in a complex system. Normal accidents were anticipated, but that was not enough. It was the interaction and intersection of all these problems (not one individual one) that explained the accident (Perrow, 1999, p. 7).

Beck agrees that technology continuously improves, but that still only improves statistical probability of safety and doesn't eliminate risk. As the logic goes, if the risk can't be prevented or controlled, it is justified and therefore allowed to exist. Although a catastrophe makes the point on societal scale, one does not need to consider the safety of nuclear plants, as travelling in any vehicle is enough in an individual's case: cars get into accidents and the odds increase the faster we go, but we still do not disallow it altogether. Probable safety means that mathematically even extinction is a possibility, even if we socially are not willing to accept it. (Beck, 1990, p. 125)

> *"Risk is socially constructed and that the adoption of the technical and naive perspective, or any narrowly positivistic methodology, is per se based on a choise of values regarding the definition of what risk is and to what extent it is acceptable"*. (Ciborra, 2007, p. 42)

Defining risks and identifying their sources also affect how they are handled. The OECD is also worried about the influences of the seen future developments to risks and risk management. Complexity and scale are seen to increase, contexts, responsibilities and perceptions to shift. Views on the challenges and flaws in assessment methods of modern risks have also been listed in the report. In short, risk models are less than real, linear link between cause and affect is still expected, long-term effects are neglected or a closed system is assumed, and human factors are neglected or over simplified or quality of those is disregarded over quantity. Understanding risk is part of the challenge of responding to them. As the report states, "*resources are limited and scientific understanding of the issue may be incomplete and opinions and interests contradictory*". (OECD, 2003, p. 15-16)

In light of the many difficult social aspects, OECD recommends including more public participation. This is seen to "*make the process more democratic, improve the relevance and quality of technical analysis, and increase the legitimacy and public acceptance of the resulting decisions*". All those who may have any kind of a stake in a matter should have say in it. (OECD, 2003, p. 95)

3.5 Whose risks?

Decisions – selections, standardising, classification – about security are influenced in many ways. From motivations, the point of reference, situational awareness to conveyance of information about them. Some of them are “built in” and others are activities from outside. Identifying these is pertinent for understanding risk transference.

3.5.1 At the core of decision making

Systems may find themselves in a competitive situation. This conflict arises when one systems can not attain its goal(s) without at least reducing the other systems possibility to do so. This "special type of social experience" usually happens when there is scarcity (Luhmann, 1996a, p. 382). From coalition game theory perspective, the motivation in a competitive situation is to seek the right coalition, which depends much on how the pay-off will be divided among the participants (Shoham, & Leyton-Brown, 2009, p. 368, 371). This is a bias factor when conflicting sides decide on their actions and contingencies. In general, competitive situation means insecurity and has been found and proven to hamper communication, cooperation and progress (Luhmann, 1996a, p. 384).

Social systems are formed with communication and thus observing communication is the way to examine socio-technical systems structures. (Luhmann, 1996a, p. 164) In addition of identifying phenomena in the communication process, one can identify phenomena in, for instance, themes and contributions, and scrutinise what may have been the reason behind it (Luhmann, 1996a, p. 172). "*Every communication invites protest. As soon as something specific is offered for acceptance, one can also negate it*" (Luhmann, 1996a, p. 173).

However, even before negation is possible, one has to have some inkling of what is communicated. Mostly, that is as much as we can understand. "*Symbolic representations – words, in other words – are generally devoid of their constituting embedded meanings and values*", says Gunder. Reflecting Barthes, he continues, "*words never convey the speaker's truth and complete intended meaning*". Part of this non-understanding is also due to loss of initial context. (Gunder, 2008, p. 193)

Thus considering theories of language and communication, even if any communication of symbolic

representations is conveyed as correct as possible and received as intended, there is no requirement for acceptance. On the other hand, intention and motivation may not be to acquire acceptance. If only considering extreme meaning and utilisation of this, it quite seems remarkable that we are able to communicate at all. But actually, we in any case only see a distorted representation of reality in the same manner like any system is incapable of fully describing itself or its environment. We live and act with only some level of summaries as our guides. Essential to these summaries and abstracts is understanding the essence of the systems purpose. The core task of the organisation has to be appreciated in assessment of complex socio-technical systems. The core task refers to a shared purpose that "*is neither an aggregate of all tasks the organisation has to perform nor a single key-task performed by some critical members of the organisation*". (Reiman & Oedewald, 2007, p. 752)

Reiman and Oedewald summarise the use of core task as means to "*understand and assess the aspects of organisational culture that either prevent or allow the organisations to function safely and effectively*" (Reiman & Oedewald, 2007, p. 754). These aspects are the cultural conceptions the organisations has about its core task. If the core task is misinterpreted the organisation may select unsuitable criteria for action, even if their conduct is without error. This allows for seeing organisations as "*dynamic, ambiguous and emerging cultural phenomena*". Organisations create and recreate their own constraints that can diverge from the requirements of their core task. All the perceptions of the core task direct organisational dynamics and emergent properties. (Reiman & Oedewald, 2007, p. 754-757)

3.5.2 Entangled techno-economic paths

Many decisions regarding things, including security, may be due to misplaced strive to higher and higher efficiency. Artificial levels of required efficiency for economic or political systems are what professional politicians and experts demand of the masses. Anyone found lacking is then seen negatively. Social components are forgotten. Efficiency is important, but in a complex societal system, individuals can not see eye to eye on what that is. But more than that, since dialogue is still simplified to the notion that there is only one single optimal path, we either ignore the other paths or compete against them. It may be more inefficient to try to force one single view or action than to accept and promote several, both in economy as in risk management. (Beck, 1998, p. 16)

Markets are becoming global – despite protectionistic tendencies – even though all companies do not sell globally or even export near. Even local companies still have to take global markets into

consideration, try to sell where ever they can and possibly do that indirectly through subcontracting or as part of a networked cluster. (Castells, 1999, p. 95)

A global economy can act in real time as a unit in planetary scale (Castells, 1999, p. 92). Despite that, at least in the immediate future, it seems, labour, technology, goods and services will still not be free from nation states, or their collectives, to be part of open markets. National regulation and policies still dictate many aspects of economies, even though the target customers might be outside their borders (Castells, 1999, p. 98). This angle is pertinent:

> "*...risks are systemic in the sense that they tend to emerge from the interactive properties of complex and pervasive technologies and their social context, or more specifically, from the infrastructures that embed and enforce these technologies. This means that it is difficult to dissociate systemic risks from a wider social order: just as many technological systems are themselves intimately connected to dominant social, economic and political frames of action, so will their accompanying risks be tied to techno-economic paths and lock-ins which are hard to negotiate away.*" (Hellström, 2003, p. 369-370)

In a world that is sensitive to risks, experiences and expectations collide in economics, sciences and judicial systems with routines of *risk justification and calculation* (Beck, 1990, p. 129-130). One effect of risk societal action is that there is conflict on how risks of producing all kinds of "*goods*" and "*bads*" are shared, counteracted, monitored and justified: who decides how they are distributed. (Beck, 1995a, s.18).[5]

When companies provide goods and services that take (possibly unnoticed) positions as "critical", it would be prudent to invest in reliability and safety of production processes for those goods and services. However, they often are in need of incentives. And, although the provided goods and services may be in demand, there may be for instance some risk to the environment. Should companies be forced to respond to this, they are likely to find a way to externalise their burden and costs. They thus have incentive to both affect the systems and use them to their own advantage. As Egan notes, governments provide a variety of emergency services, and those taxpayer financed services may be used as safety net for failures of private companies, thus transferring some of their risk. (Egan, 2007, p. 14)

5 A conflict episode between nation state and “the markets” (private investors) was seen when Greese contemplated having a democratic vote on financial matters that deeply affect citizens. This mere idea caused shock in private and governmental financial experts, as well as politicians. This shows how national politics have influence in international affairs, but the reaction also shows how little democracy is valued, as experts refused to relinquish their positions of control. (Schirrmacher, 2011, n.p.)

3.5.3 Whose in charge around here?

The question of "who should decide" (which is more productive than "who's responsible" / "who's to blame") is a tricky one. It has historically changed from tribal leaders to local rulers, from emperors to representatives, but it is now suggested that, more than ever, it is the individual who (and the choices of many individuals) decides what to do.

As institutions struggle to answer and rationalise the new breed of risks, this inability becomes more apparent to the individual who is left alone. The consequence is mistrust of all these institutions and alienation from expert systems. Responsibility of choice is dumped on those who can not taste, small, feel, or sense these complex threats. With words of Beck, "*global risks enforce an involuntary democratisation*". (Beck, 2006, p. 8, 12)

People are "freed" to be individuals as part of the post industrialist risk society (Beck, 1995a, p. 19). Individuals are more and more expected to decipher and understand complex prospects, that were previously addressed in or with support by social peer communities, while taking responsibility and considering fully the consequences (Beck, 1995a, p. 20). Having the possibility to decide for yourself is not always a blessing. Constant assessing of options, possibilities, risks and contingencies is taxing. "*Where freedom becomes a cage, many choose the freedom of the cage (new or old religious movements, fundamentalism, drugs or violence)*" (Beck, 1998, p. 10).

Allowing public authorities and institutions to make more and more decisions for the people seems understandable in this light. While noting this, we also have to note the distinction between the idea of freedom and the social reality of it, the "*contradiction between potentiality and the reality of freedom*" (Beck, 1998, p. 68-69). Obeying of authority and authoritative experts is, according to Giddens, very much a tradition with historical continuity, and a sense of legitimacy stemming from that. Still, an "expert" and "layman" are relative terms and always specific to particular context (speciality field of knowledge) (Giddens, 1995a, p. 117-119).

If regulators would dare to assess risk of a complex system, their challenge would be to get enough knowledge and understanding to identify where the hazards are, when even the system managers may not be aware (or forthcoming) (Egan, 2007, p. 13). As Beck sees it, there are two sides to this. Fast developing technology doesn't allow for rigid regulation and thus we need experts to control them. On the other hand, as if surrendering behind a façade, democratic institutions are signing away their authority to the caste of "technocratic shadow-cabinets". Government, parliament,

judiciary – all serve as justifiers and enforcement agents for the true rulers. (Beck, 1990, p. 171)[6]

Regarding the "who's really in control"[7] doubt, there is a very real challenge that computerised technology has created in that area, as it has taken over. When previously security and safety was handled among other work by those who specialised in that particular task and had tacit knowledge from experience, now the responsibilities have shifted to those whose primary knowledge-base is in computer technology. They may have even taken over in several different processes of different fields. They are also relatively more younger, less experienced and less credentialed than their counterparts may have been before. (Egan, 2007, p. 10)

> "*The coalition of technology and business becomes shaky, because technology can increase productivity, but at the same time it puts legitimacy at risk. The judicial order no longer fosters social peace, because it sanctions and legitimates disadvantages along with threats, and so on.*" (Beck, 1998, p. 38)

The concrete method for this re-taking of power would be through opening the expert councils that set the norms and decide how implementations are done (Beck, 1990, p. 246; Hellström, 2003, p. 381). The actual remedy, however, to this technological monopoly, as suggested by Beck, is to philosophically separate the *discourse of security* and *discourse of security through technology*, which are seen as one and the same. Security is a relational definition abiding rules and open to interpretations. It can – and has to be – redefined if it creates actual insecurity in disguise. (Beck, 1990, p. 244)

The other method Beck pushes for hampering (complex) risk creation is to reverse the burden of proof. Anyone affected would no longer need to change the minds of all the different institutions

---

6 Two negative examples of high level experts and position of power in Finland from recent years:

First, a glaring recent example of resetting norms for benefit, as well as how questionable expertise may be. An expert from the Finnish Radiation and Nuclear Safety Authority (STUK) admitted to picking a number limit for a safety zone "*out of a hat*". This definition has been de facto law for over a decade, as the authority to define these has be delegated to STUK from the government by legislation. The expert and STUK now later have decided to change that number because it was inconvenient for the company planning a new reactor. (Nelosen Uutiset, 2011, n.p.)

Second, a potential conflict of who gets to decide about security and activities in a crisis was reportedly playing behind the scenes, between Finnish government and military. The convoluted politics aside, attention was brought to effective bureaucratic coup that has been happening, where military has been positioning themselves as the overall authorities in the event of national crisis. Also, security authority institutions were said to have been showing signs of less co-operation and bolstered organisational boundaries towards government and democratically elected political leadership. (YLE news, 2010, n.p.)

7 It could be remarked that the so called *economic super-entity* of only 737 companies, which have accumulated 80% of the control over the value of all transnational corporations (Vitali, Glattfelder, & Battiston, 2011, p. 6).

and companies. Instead, the promises and assurances of the marketers would no longer be enough, as actual proof of safety – even in the long run – would need to be presented before hand. The way complex technologies and systems are, providing such proof would be a considerable burden. In this, conflict can be seen. (Beck, 1990, p. 247-248)

3.5.4 Us, them, risks, security and freedom to tell about it

Conflicts were and are a much used means of identifying and exclusion. The us-versus-them stance was used during the cold war and it is used in today's rhetoric. It creates borders between people, organisations, societies, communities. It is not always or often an objection towards "the other", but can be part of internal politics and power struggle (Heinonen, 2011, p. 57). Particularly intangible threats are used, as tangibles could be examined, dealt with and would not permit such polarisation, exaggeration, and being used as justification for unfavourable policies (Vuori, 2011, p. 10).

Enemy stereotypes give power and authority to act. Responding to them gets the highest priority and all objections can be swept under the rug. Enemies create consensus (Beck, 1998, p. 143). The defined – often vaguely defined – enemy gives definition to "us" – "the ones opposed", "the ones not them". The conflicts between these factions have today more and more been transported and kept alive in new arenas (trade, diplomacy, technological development etc.) (Heinonen, 2011, p. 83). Likewise, the transporting of conflicts, risks "travel" through process-like cycles of design, building, initial recognition, debate, official acceptance, description, regulation and monitoring. Many actors in any of these cycles in any socio-economic context could affect the risk, its perception and management. (Hellström, 2003, p. 381)

As Heinonen states, the Parliamentary Security Policy Monitorin Group, that seemingly crafts publicly assembled and accepted security policy, uses mainly the same few experts as do the preparers of the actual policy (Heinonen, 2011, p. 135). Defining "threat", "threat assessment" and "security related risks and hazards" are considered the most important part of official security policy in Finland (Heinonen, 2011, p. 183). Public participation has been seen inconvenient necessity by the political parties, but only due to party politics and changes in political arenas (Heinonen, 2011, p. 127). However, security policy elite of experts and actors are forced to consider public opinion, both when argumenting and while trying to persuade the opinion to the side of the argument. Capturing public opinion that translates to support in elections is also a considerable influence to creation of public policy and speech. (Heinonen, 2011, p. 144)

In Finland, over the last decade or so, there have been increasing demands of taking the public opinion into account in major decisions. This is based on the notion that only decisions that have broad public support may be considered binding. Mostly this has been seen practised with presenting the support of at least two biggest political parties (relative representative parliament majority) as being sufficient. (Heinonen, 2011, p. 134)

To be able to create security policy that many can agree on seems to require avoiding specifics. In a study conducted by interviewing experts in Finnish government service across most of the ministries, it was concluded that the experts felt that there are several areas to improve security policy creation. Overly consensus seeking culture was seen to hamper genuine public security discussions, and resulting documents end up vague and convoluted. Some goals, used means to attain them, and even some basic concepts have not been defined. Ministries push their own agendas with out coherent big picture. Internal security is also perceived to have a lesser status in security policy. (Peltola, 2010, 4-5, 8)

According to Heinonen, it is surprising that Finnish political parties have been willing as well as able to keep security policy and decision making separate from other public politics, in the hands of security policy elite. Parties have even tried to avoid discussions about the ideological and political nature of security policy. Instead, it has been represented as a more of a factualised and parametric technical matter. (Heinonen, 2011, p. 240-241) [8]

In general, what was previously held apolitical has now increasingly been dragged out to the political arena, or at least has been tagged with non-professional non-governmental politics (Beck, 1995a, p. 33). The public awareness of risks has opened debate and requirement for open justification about subjects and themes which have previously been dealt behind closed doors (Beck, 2000, p. 99). Internet and electronic media have been hailed as the saviours of free speech, and all-around freedom as derivative of that. It is unbound, active, reciprocal and enable contacting billions across the borders of institutions, states, beliefs and geography (Beck, 2000, p. 105).

There are, however, limits to Internet's power – even though the recent "arab spring" upheavals around the middle-east suggest otherwise. The social networks there were random enough and the

8 One way to look at how the political field in Finland has positioned regarding security is using Heinonen's analysis about discourses of allying militarily. He sees that in the dichotomy of "*for*" and "*against*", the former sees risks stemming from social and environmental threats, and the latter sees risks stemming from aggressor violence and interest conflicts that generate military threats. Based on their rhetoric, the "for" seem to base their threats to past and their means to future, while the "against" seem to anticipate new threats and have old means. (Heinonen, 2011, p. 233-234)

communication service hubs were not effectively taken out. Never the less, internet is not a utopia come true.

Web-mapping of internet topology has shown that we're not able to see but a fraction of the total (Barabási, 2002, p. 56). Internet is not equal nor fair when it comes to distribution of information: linking being the operative word. The "catch-22" of internet fame is that *you need to be known to be linked to, but you need to be linked to in order to be known* (Barabási, 2002, p. 85). In other words, one is at the mercy of hubs and few super-hubs. The information has to get to be linked there for it to propagate. Otherwise, it is likely forgot to an unlinked separate “island” web-site or one-way link dead-end at the fringes (Barabási, 2002, p. 166).

Benefits and risk of any infrastructure or production can not ever be divided "justly" – not even by consulting experts. As Beck sees it, monopoly of knowledge that authorities have, must be dismantled and circle of participation must be extended beyond those the experts themselves deem relevant. Beck also notes that decision making has to have open discourse and not be a matter of pre-determined minds defeating or trading off with opposition behind closed doors. (Beck, 1995a, p. 48-49). In conclusion, even though debates have been opened more and more, they are not to be taken for granted. Risks and contingencies are debated in many arenas and they are politicised, which should be kept an eye on, as the consequences may be far reaching. It is possible to use electronic media to help bring daylight to some of the more closed corners, but the internet does not automatically mean equal speech.

3.5.5 Whose risks should they be?

Often, when people say "it is a simple problem", they do not mean the problem is easy to solve. Especially they do not mean it is easy to solve in a manner that causes no, or least amount of, fallout. There are no simple solutions to complex problems, as H. L. Mencken's (Mencken, 1921, p. 158) idea has often been paraphrased and misquoted [9]. What people really mean is, they have a simple solution that benefit their own, and the cost and side-effects are left for someone else to bear.

Giddens comments that, traditions that gave science exceptional prestige and kept it separate from the wealth of knowledge that mundane people have, have been taken down. Esoteric knowledge still

9 Paraphrased version of the quote: *For every complex problem there is an answer that is clear, simple, and wrong.* The original: “*... there is always a well-known solution to every human problem — neat, plausible, and wrong*.” (Mencken, 1921, s.158)

protects specialists, but no one can be expert in everything. It has also already been seen how expert knowledge is both specialised and controversial. (Giddens, 1995b, p. 251)

> "*The proponents of a "technical" approach to risk management have long considered that the public's perceptions were unfounded and should not interfere with the objective assessment of risks. At the same time it is increasingly accepted that although the public perception of risk can be wrong (for instance if it is distorted by orchestrated campaigns by vested interests), there is no objective and unique measure of risk. Risk has a multitude of dimensions, some of which involve ethical considerations. A number of different views can thus be pertinent and legitimate, and confronting this variety of standpoints is part of risk management.*" (OECD, 2003, p. 16)

Experts versus layman: does it always have to be someone else to decide for you; does it matter how many ignorant people are deciding when only few expert know. Neither should be given unchecked, unquestioned, absolute power – it is only on loan to experts, people are not to be forced to be wards of expert systems.

> "*One of the crucial aspects of the heated debate that has taken place in the past fifteen years between proponents of a "social" approach to risk management and those favouring a "scientific" approach pertains to the role of government in the public's perceptions of risk. The former school of thought focuses on the value-laden nature of risk, and advocates a representative form of government that would follow and reflect the public's preferences with respect to risk management. The latter emphasises the need to allocate rationally society's limited resources for risk management based on objective assessments, and advocates a preference-shaping form of government that would correct the public's "misperceptions" regarding risks.*
>
> *The challenge for governments is to strike the right balance between these polar models. In other words, they must avoid founding risk management policies solely on experts' evaluations or, alternatively, on reactions of the public, and instead work with both experts and citizens to prioritise and regulate risks based on sound reasoning. Recommendations for action in this respect fall into two categories: developing risk awareness and safety culture; and enhancing dialogue and building trust.*" (OECD, 2003, p. 269)

In the grander discourses of how risks should be understood and controlled, if not conquered, are two opposite – and according to Beck, flawed – interpretations. First, the *objectivism* based in

science, which tries to subject all risk to equations, diagnosable only by technology, and always be in total control. Second, the *relativism* based on culture, which points to variations, fluctuations and differences in values, measurements and thresholds between times, places and social aspects when risks are estimated, making things appear threatening and harmless at the same time. As interesting as this would be to explore further, suffice to say both approaches can and are used in creating positions of power for the expert. (Beck, 1990, p. 111-112)

Positions of power, and subsequent creation of inequality, have been increasingly challenged by philosophical critical approach ever since the days of the so called Frankfurt school. In a manner, this needs to be done to security as well. This chapter consisting of theory and research has build the case, that there is no "one security", nor are the risks same to all – event though all are at risk and risks have grown and shifted due to complexity. And even though technology does offer tools for security, the cost is increased complexity and new risks. We are immersed in technology, incorporating technical systemic aspects in human societal interactions, and that has effects to our behaviour. Amidst this, it has been shown that risks are many and on many levels and can not be contained. Risks are subjective and are not shared equally, nor are the related costs divided evenly, due to many competing influences. If security has been seen, or made out to be, as untouched by political and interest group influence, it can now be seen that it is not. Finland does not differ in this. Experts in power in systems are likely to have their own agendas when coming up with security policy and designing risk management plans. To examine this last part, in the next section of this thesis, the Finnish government's *Security Strategy for Society* (2010) is considered applying the *Critical Systems Heuristics*, which is a suitable tool to uncover bias in system participants.

4. CRITICAL SYSTEMS HEURISTICS AND THE SECURITY STRATEGY FOR SOCIETY

In order to show that complex security issues in socio-technical systems can be affected, the Finnish national strategy for securing functions vital to society is analysed. First, the methodology is presented and discussed. Then, a practical reading is done, followed by discussions of findings.

4.1 Methodological framework

Critical systems heuristics (CSH) is a qualitative methodology framework for reflective practise developed mainly by Werner Ulrich. It is a series of questions used to make visible the common biases and exclusions that we use unwittingly to restrict and set limits to our systems. In other words, CSH can be used to explore what reservations and requirements of power and control are embedded in decisions. It is a tool for systems with social dimensions, to understand multiple perspectives. (Ulrich & Reynolds, 2010, p. 243-245)

> *"*[Basis of CSH is] *...the simple notion that all approaches, methodologies, methods, whether described as systems or something else, are partial, in the dual sense of (i) representing only a section rather than the whole of the total universe of possibly relevant considerations, and (ii) serving some parties better than others"* (Ulrich & Reynolds, 2010, p. 247).

CSH was developed to a methodology during the last ten years mainly by Werner Ulrich, based on his previous work as well as the works of C. West Churchman, Jurgen Habermas, and – ultimately – Immanuel Kant's critical philosophy (Ulrich & Reynolds, 2010, p. 247). As Ulrich sees it, CSH's three main pillars are in its name. Heuristics takes its meaning epistemologically from ancient Greek and refers to finding and discovering. Critical is the approach taken, as there are no single right answers. Relevance of systems thinking is dual, as systems are a reference point to which we base our assessments, judgements and critique, as well as systems being our spheres of thought and understanding which we limit, build and define with our boundary judgements. (Ulrich, 2005, p. 1)

The questions in CSH are called boundary questions. They try to make "*explicit the boundaries that*

circumscribe our understanding". Boundaries circumscribe all our thinking about situations and systems, and these systems of individual understanding are called in CSH as reference systems. Any one autonomous actor has their own reference system, which they base their actions. (Ulrich & Reynolds, 2010, p. 245, 254)

Sources of influence	**Boundary judgements informing a system of interest (S)**			
	Social roles (Stakeholders)	*Specific concerns (Stakes)*	*Key problems (Stakeholding issues)*	
Sources of motivation	1. *Beneficiary* Who ought to be/ is the intended beneficiary of the system (S)?	2. *Purpose* What ought to be/is the purpose of S?	3. *Measure of improvement* What ought to be/is S's measure of success	**The involved**
Sources of control	4. *Decision maker* Who ought to be/is in control of the conditions of success of S?	5. *Resources* What conditions of success ought to be/are under the control of S?	6. *Decision environment* What conditions of success ought to be/are outside the control of the decision maker?	
Sources of knowledge	7. *Expert* Who ought to be/is providing relevant knowledge and skills for S?	8. *Expertise* What ought to be/are relevant new knowledge and skills for S?	9. *Guarantor* What ought to be/are regarded as assurances of successful implementation?	
Sources of legitimacy	10. *Witness* Who ought to be/ is representing the interests of those negatively affected by but not involved with S?	11. *Emancipation* What ought to be/are the opportunities for the interests of those negatively affected to have expression and freedom from the worldview of S?	12. *Worldview* What space ought to be/ is available for reconciling differing worldviews regarding S among those involved and affected?	**The affected**

Fig. 2. CSH boundary questions represented as a table with categories and labels (Ulrich, & Reynolds, 2010, p. 244).

4.1.1 Boundary questions

CSH uses twelve boundary questions, that have two modes, *the ideal* ("what ought to be") and *the realistic* ("what is"). These can then be contrasted by each other. The questions are divided to two intersecting categories which are further divided. These main categories are t*he sources of influence* they examine and what are the *areas of system interest*. Sources of influence have four labelled areas of question in two categories. The first area questions, for *the involved,* are about *sources of motivation*, *sources of control* and *sources of knowledge*. The second area of questions, for *the affected,* are labelled as *sources of legitimacy*. (Ulrich & Reynolds, 2010, p. 244-245)

Each labelled area of questions has three questions. They are by the three categories of areas of systems interest: *social roles* (stakeholders), *specific concerns* (stakes), and *key problems* (stakeholding issues). These three sub-categories, while intersecting with the four areas of inquiries, create a table that has twelve boundary questions. Answers to those questions reveal boundary judgements. (Ulrich & Reynolds, 2010, p. 244-245)

> "[By utilising CSH] ...*we can review an entire set of boundary judgements (CSHq1–12) associated with any one reference system in the light of another set of boundary judgements belonging to a different reference system*" (Ulrich & Reynolds, 2010, p. 246).

4.1.2 Discussions about CSH

By contrasting answers different actors give, we can see how communication is going cross purposes or how much everyone is talking past each other. In CSH this is understood to be because they have different reference systems. CSH tries to help in revealing this, and thus allowing a clearer picture of how to improve understanding. (Ulrich & Reynolds, 2010, p. 246)

If, when communicating, we are not clear of our own reference system, we risk misrepresenting ourselves and others misunderstanding our intended meaning as something else. If, on the other hand, we are aware of our reference system and its boundary judgements, but do not state them, we risk misrepresentation again in the form of others not being aware what the limitations and reservations are. (Ulrich, 2005, p. 2)

CSH is meant to be used for two purposes. The self-critical reflective practice, or projected to an

outside entity, as emancipatory practice (Ulrich, 2005, p. 3). But as even Ulrich recognises, there is a difference between emancipatory interest and emancipatory commitment (or even emancipatory imperative) (Ulrich, 2003, p.332). He also recognises one of these positions of inequality in our prevailingly expert-driven approaches to applying science and knowledge. As Ulrich formulates it,

> "*Concerned lay people may be listened to, but when it comes to judging an issue, they are not really considered competent. Underlying concepts of expertise and rationality are in this sense 'monological' (leading to a monologue of experts) rather than dialogical*" (Ulrich, 2003, p. 326).

The main critique to Ulrich and CSH has been regarding situations of coercion. Midgley questions what use may CSH be when those with vested interests are likely to seek control of the situation, close debate or even use force against those who challenge them (Midgley, 1996, p. 44-46). To this Ulrich has responded that CSH can still be used in polemical manner, to provide a counter argument for the prevailing system and situation (Midgley, 1996, p. 46-47). From the standpoint of this thesis, these emancipatory activities, and the related critique, bare little weight. In the manner this analysis is intended to be carried out and presented, no emancipatory actions are expected to take place, or actively sought.

4.1.3 Application

In this thesis, although still safely in the realm of systems, it is attempted to import CSH to be used in a new context, namely security and risk. This is – as far as has been possible to verify – a first. The methodology has no objections or reservations to be utilised in this context. CSH makes no conflicting assumptions about the nature of systems, and its reasoning coincides with for example Luhmann's systems theoretical description (as previously discussed), of how system can not fully describe itself or its environment. In other words, it is applicable to complex socio-technical systems as they have been presented in this thesis.

What is different to the standard application of CSH, is the used source, and related changes. In this instance, only the first nine boundary questions are used and the three questions in the category for the affected (“sources of legitimacy”) are excluded. They can be considered being moot and/or being beyond the scope of this study, as they are significant in the more practical and emancipatorial application of CSH.

CSH is normally applied to human participants answering the questions. But a practical reading and textual analysis to a ready document can be done using CSH as structured questionnaire as the basis of the analysis. It is to be noted that not all questions may find any or adequate answer in the document.

Answers will be based on the reading of the text. The obvious critique to this practice would be the influence of the reference system of the reader in regards to the answers. This would have more merit, if it were that the reading would be seeking to contrast the qualitative differences of the reference systems and the boundary judgements. However, the purpose of this reading is only to meaningfully identify the existence, if any, of boundary judgements in the selected text. Concentration must be on the system, not the individual experience (Lash, 1995, p. 192).

Any contrasting is used mainly only for indicative purposes and further identification is to be made carefully. The contrasting can be made against any other reference system that diverges of that of the read text. In this thesis the contrasting boundary judgements will reflect those discourses sketched in theoretical portion of this thesis. These can be considered as the expected ideal based on the presented theories. They can be seen counterbalancing or counteracting “risk societal behaviour” , taking the position of the "ought to" answers.

4.2 Reading of Security Strategy for Society with CSH

For the source material the Finnish government's *Security Strategy for Society* (2010) is selected. It is also know with acronym YTS, from Finnish: *Yhteiskunnan turvallisuusstrategia* (formerly known as Securing the Functions Vital to Society; *Yhteiskunnan elintärkeitten toimintojen turvaaminen,* YETT). It is singled out of all other policies, stacks of plans and directives that the government and its ministries have. It is the single publicly available focal point of a socio-technical security system aimed to cover all parts of a society in any disruption or emergency. This is why it is the document describing the system that is also likely to encounter and consider complex risks, thus making it likely to yield some insights related to the topic of this thesis.

The publicly available online English version is mainly used, with some translational differences checked from the Finnish version. The document is done every few years (previously 2003, 2006) by the Secretariat of the Security and Defence Committee (TPAK) in co-operation with the heads of preparedness of the ministries. Selected authorities, organisations and representatives of business community were also given possibility to participate. Ministry of Defence TPAK office provided lists of participated heads of preparedness and those expert entities who participated to a seminar about the strategy prior to its current incarnation. They are included in the appendix section. This information is not readily available among the documents, nor the websites, nor is there any comprehensive monitoring which sources input has been transferred on from previous strategies to the current version of this aggregate document.

Not all of the policy is significant for answering CSH boundary questions. Deeper research into the backgrounds and policy subject matter might reveal more, but are beyond the scope of this thesis. Some parts of the policy concentrate only on conveying facts of established international agreements as well as references from other policy documents. Parts of the policy directly linked to nation's internal security and safety offer more relevant material than that related to security policy with obvious international and military dimensions.

4.2.1 Reading

In this section are presented the general characterisations of what can be understood as the answers for the boundary questions and noteworthy extracts from the document. Contrasting the found

answers is done in the following section. Collection of selected parts of text from the policy related to each boundary question can be found included in the appendices at the end. Texts are arranged in groups according to the three (I-III) categories of *sources of influence*, each consisting of three questions as per three categories of *areas of system interest*, thus being true and corresponding to the same order as expressed in CSH source material, for the first nine boundary questions.

I. Sources of motivation

1. Beneficiary: *Who is the intended beneficiary of the system?*
Mainly the document promotes the view that defending the territorial area is the highest function of the system, without considerations that there would need to be any discernible beneficiary. Some of the used language does differentiate and juxtapose between the general population and those involved in business activities, when sharing of burden is concerned.

> *"... this can only be built on the recognition by the business community that the benefits of co-operation are worth the resources invested in it" (YTS, 8).*

> *"... the population and the business community's basic needs"* (YTS, 36).

2. Purpose: *What is the purpose of the system?*
The purpose of the document is to lay out the overall government controlled systems that may be used in case of disturbances or disasters. The purpose of those systems is to protect the nation state's land, society, and economy.

> *"The most important tasks of Finland's foreign, security and defence policy is to safeguard national sovereignty, territorial integrity and basic values; promote the population's security and well-being; and maintain the functioning of society"* (YTS, 3).

3. Measure of improvement: *What is the system's measure of success?*
The document does not offer any means to gauge the success of its functions – core or otherwise. Several references are made to objectives, criteria, monitoring and reporting, but not even vague short or long term objectives are presented.

> *"The principles, objectives and implementation criteria for Finland's security and defence policy were provided in the Finnish Security and Defence Policy Report in 2009"* (YTS, 1).

"Elected [municipal] *officials should fully familiarise themselves with and be involved in the objectives of preparedness"* (YTS, 6).

"In co-operation with the subordinate administration and co-operation partners, ministries draw up a report on a regular basis on the functioning of crisis preparedness and development needs to the Security and Defence Committee [TPAK]*"* (YTS, 63).

II. Sources of control

4. Decision maker: *Who is in control of the conditions of success of the system?*
As TPAK is in the prime position to control the creation and development of YTS, it can be seen as the one determining the success of the system. Within YTS, it is clear that several known and unknown entities influence the success of the systems functions.

"The Security and Defence Committee, supported by the meeting of the heads of preparedness of the ministries, is responsible for the joint monitoring of the Strategy in co-operation with the different authorities, the business community and organisations" (YTS, 4).

"The Prime Minister directs the activities of the Government. The Prime Minister's Office assists the Prime Minister in the overall management of the Government and in coordinating the work of the Government and Parliament" (YTS, 4).

"The Government directs, supervises and coordinates the securing of functions vital to society. Each competent ministry does the same within its respective administrative sector" (YTS, 4).

"The Ministry of Defence is responsible for co-ordinating comprehensive defence activities. Coordinating the comprehensive defence approach involves synchronising measures of the public sector, that is, the Government, State authorities and the municipalities, and the private sector and voluntary activities by citizens in order to maintain the functions vital to society under all circumstances" (YTS, 5).

"The Security and Defence Committee (TPAK) assists the Ministry of Defence and the

Cabinet Committee on Foreign and Security Policy on matters relating to comprehensive defence and its co-ordination. The Committee monitors changes in the security and defence policy and situation and evaluates their effects on comprehensive defence arrangements. The Committee has the task of monitoring and co-ordinating the different administrative sectors' comprehensive defence measures." (YTS, 5).

"Other EU policies also have a significant impact on Finland's possibilities to secure society's vital functions during disturbances" (YTS, 10).

5. Resources: *What conditions of success are under the control of the system?*

The system is meant to control resources and has available the resources reserved for both normal times and emergencies, as well as reserves for catastrophes and military defence. It does not control all resources for long term requirements, and sufficiently large or specialised events will require outside co-operation to maintain all – even vital – functions.

"In addition to national preparedness, the preparedness measures taken in the European Union, the agreement on the International Energy Programme and the multilateral and bilateral agreements on economic co-operation in crisis situations concluded with a number of countries contribute to security of supply" (YTS, 7).

"Information and communication technology (ICT) services, transportation and the office ownership and management are amongst the service entities where outsourcing is typical. Another trend in the business community is internationalisation. The Finnish business community is part of a global network where industrial plants merge and through the flows of raw material, information and people become an entity where change is permanent" (YTS, 7).

"The co-operation between public and private sectors and its continuous development are essential because the main part of the resources required by security tasks is, as a rule, owned by the business community" (YTS, 8).

"Arrangements on medical supplies, defence materiel and securing electricity transmission systems have been made under the auspices of Nordic co-operation. The Treaty of Lisbon provides the opportunity to deepen Nordic co-operation" (YTS, 12).

6. Decision: *What conditions of success are outside the control of the decision maker?*
The government can not reliably know what resources will be made available to it from outside its own system, beyond what is precisely agreed contractually. Authorities can only prepare for finite amount of scenarios. This is limited by knowledge and economics. The disturbances and catastrophes are not exact and by definition would not develop into such if they could be anticipated and prepared for – or even prevented.

> *"Long, even global value chains and the internationalisation of companies have significantly decreased the preconditions of national authorities to regulate, steer or control the activities of companies"* (YTS, 8).

> *"Some sectors such as telecommunications, transport, energy and financing are obligated to preparedness by legislation"* (YTS, 8).

> *"It is not possible to secure all vital functions merely through national arrangements"* (YTS, 10).

> *"The premise of Finland's security of supply is the proper functioning of the single European market"* (YTS, 37).

> *"If need be, the authorities prepare to guide, regulate and categorise networks and their services as well as user groups according to their relative importance"* (YTS, 41).

III. Sources of knowledge

7. Expert: *Who is providing relevant knowledge and skills for the system?*
All branches of government and authority organisations are utilised. Members of TPAK and heads of preparedness for different ministries are central experts. Additional expertise is available from some NGOs, educational establishments and business community.

> *"The Security and Defence Committee, supported by the meeting of the heads of preparedness of the ministries, is responsible for the joint monitoring of the Strategy in co-operation with the different authorities, the business community and organisations"* (YTS, 4).

> *"Apart from municipalities and their co-operation bodies, the actors of the regional state*

administration, parishes and religious communities, universities and other educational establishments and the units of the business community that contribute to the service production of the local government play a key role in regional preparedness and securing functions vital to society. Organisations, too, are important service providers and actors in building preparedness" (YTS, 6-7).

8. Expertise: *What are relevant new knowledge and skills for the system?*
Development of improved threat identification and management capabilities are requested, and NGOs and industry being internationally networked is seen important and valued.

"They [educational establishments] *produce and maintain resources and expertise that support the authorities and, in addition, implement education and communication that support and promote preparedness"* (YTS, 9).

"Various organisations run sports, cultural, youth and other societal activities, representing a significant segment of our civil society. The ability to recognise individual needs is one of the strengths of these organisations. They are often extensively networked, both nationally and internationally" (YTS, 9).

"Security research which is based on national approach provides targeted information to support decision-making, identifies new threats and opportunities in a rapidly changing world and develops courses of action, instruments and systems for the management of various disturbances and crises" (YTS, 9).

9. Guarantor: *What are regarded as assurances of successful implementation?*
No assurances are given.

"For the basis of preparedness, preventing and combating threats and, further, for securing the functions vital to society the ministries are given the responsibility to develop, steer and monitor strategic tasks in accordance with the requirements of the security environment" (YTS, 2).

4.2.3 Analysis of reading

This document is a limited presentation of the system. It is simultaneously part of other complex systems and a hub, a collection of complex systems, which are linked together at least via the connections of YTS, security and Finland. By intrinsics of complex systems, by reasons of security, and by sheer impracticality it can not present everything included to this system entirety. Observations can be made based on what is included and what is excluded.

To put the document better in perspective, it has to be said to the credit of YTS, it is more comprehensive than the limited framework of CSH allows to present. It manages to include a wide range of efforts essential to the *comprehensive approach to security*, and it is a developing system, constantly reflecting the security environment. Regardless, YTS is not forthcoming with answers to CSH questions. This is slightly worrisome, as by themselves the questions and their answers are basic level inquiries and relevant information needed to meaningfully form a reliable opinion of a system. Reading such a document necessarily becomes an interpretation of nuances. For interpretation and understanding, having a reference point is a requirement. With YTS it very much comes down to defining the core function of the system(s). This is difficult due to different ways YTS as a system can be interpreted – which is even before the “barthesian” challenges of interpretation are considered.

There are many ways to benefit from security and large system like YTS directly and indirectly, depending how one is positioned. Functions vital to society are supposed to be secured in all conditions, as presumably several – if not all – components of them are needed to sustain necessary functionality. But as has been noted, a hierarchy of criticality develops in systems. The document makes no mention how this issue is met if selections are needed to be made. Prime Minister's Office is established as the overall coordinator. A general implication, about deciding who or how, is left to the discretion of the abstract authority organisation on whose domain an issue lands. This leaves unknown the (likely) beneficing parties and reasoning behind possible uneven shortages. The question thus becomes, who benefits more than others, as it is abundantly clear that YTS benefits one way or another everyone in Finland, and through networks beyond that.

The system is meant to keep businesses safe as well as economy and societal conditions as such that doing business can be considered viable and attractive in Finland. At the same time, however, it is stated that business community may in their part choose not to participate in this strategy if it is not economically justifiable. In other words, even though their operating environment is supported and

services provided, if businesses do not get anything out of it in addition to that, they are not even expected to participate. This, it has to be noted, is related to direct activities with security of society, and disregards any general partaking via taxes or other financial mechanisms, which gains government may choose to direct towards security. Although the general beneficiary may be all the members of the society, the unintended beneficiaries are those corporate entities that take the free ride-along. Document does mention of a national system where some companies can take part in securing the supply system from food to military technology (YTS, 2010, p. 7).

What is safeguarded necessarily excludes something. Thus, it is not the purpose to safeguard all. Defining the core task is important. The laid out purposes are vague notions about ideals – even territorial area is not an absolute concept. The core purpose of the YTS as a system is not the same as those systems that are laid out in it, and that and any secondary purposes are mostly not mentioned. From a “barthesian” viewpoint, we can not know the precise true intentions of the creators of YTS. What we do know, however, is that YTS is subordinate to military and national/international security policy (Prime minister's office, 2009, 10). Moreover, YTS is for public consumption, and does not provide any practical information, only principles and how the first steps from those towards action are taken. Without clearer statement of what the aim is, it is impossible to make deeper analyses.

As the document on several instances describes the hierarchical activities of monitoring, informing and coordination, in doing so is described a bureaucracy and effectual means to disperse accountability. Such, and the lack of goals to be measured against and required to fulfil, create an “escape route” for those expected to act. Being secure and safe – as self-evident as it may seem – are not in any way useful measures of success. The manner this is achieved has value, the selections made have side-effects and costs. “You get what you get”, seems to be the hidden message. If the absolute sum total of society's resources were directed towards security, then that phrasing would hold some merit. And even though “black swan” type extinctions level risks have been given as extreme examples, most of the risks that are faced and deterred under the framework of YTS are considerably smaller, requiring only parts and portions of our resources – especially if threats are managed before they have grown. As the document mentions, what is planned for a catastrophe, can also be used in an emergency. Surely there are any number of gauges and reference points that are used to evaluate individual authorities, but it remains unclear what norms are, or should be used, to assess YTS. Setting objectives does not require exposing the means. As for how to improve the system, adding more transparent means to weight YTS' successfulness seems a good step.

Although TPAK is in the prime position to control the creation and development of YTS, looking into the system description provided by YTS, several participants and outside entities can be seen to have control of various segments of functions vital to society. Prime minister is named the overall director, but most authorities have heavy autonomy, and especially international business or political entities have varying levels of interest to co-operate and support Finnish systems. Especially in long term, it is recognised in the document that Finland needs to network internationally to secure materials, supplies and energy. Thus, any of these several interconnected nodes has influence over the functioning of YTS activities. This is in line with the overall development of globally networked world. Additionally, should the emergency be international and markets be disrupted, competition for resources may emerge and foundations for most plans would be shaken.

It can then be concluded that, security in mind, adequate level of national control in these matters is essential. It also matters that the ones making decisions about these systems are within the controls of the democratic principles. That in mind, the position of TPAK seems overly influential, based on impressions from the document. Given the lack of presented avenues of involvement or democratic representation – and without resorting to theorising about redesigning government – it can only be said that the people ought to be more in control of the system.

It is a very limited group that is heard regarding YTS. For expediency, it is natural that government would use its own staff. For all intents and purposes, it is desirable that those in a position that will have to confront emergencies are experts in a relevant field. Never the less, heads of preparedness, as well as permanent secretaries of ministries and other officials who are members of TPAK, are not democratically elected representatives. Neither are the representatives businesses, whose amount of participation to designing YTS are not elaborated despite several references.

When considered as a whole, the government is the single biggest hub in this multi-layered network – even more so if municipal authorities are count in as well. Yet, it alone is not able to support the whole socio-technical network that makes a society. Not even all the vital functions if the catastrophe level event prolongs, strains all areas of society and critical infrastructure simultaneously, or has a special component attached to it, for which a small nation can not have and maintain any or big enough preparedness for. In this, economics and selection come into play. What level of security is considered adequate: is preparedness for all or is it done an arbitrary number in mind. Whose and which systems are shut down first.

Interestingly, selection of systems is mentioned in the section about ICT. With ICT this is likely due that it seen as an imaginable possibility and easily – even surgically – executable. ICT is also the one controlling other systems, so this can be considered to refer also to selection targeting other systems. For the good of most, in an emergency, government may need to shut some services down. For accountability and protection from oppression, however, as examples from around the world have demonstrated, total control seems not advisable.

The document does not lay out what particular knowledge or skills would be required to support it. General impression is left that YTS is leaning towards the technical minded security when preparing for risks. This comes from several references to resources, material and supplies. This implication can be seen natural as functions considered vital to Finnish society requires tangible systems to support it, and the involved critical systems are technical in nature. Humans (compared to systems) are the more adaptable ones. Things related to public morale (values, education, culture, symbols and so on) are identified vital for a society, and in this document are filed under psychological resilience. At least in part, it seems that this too is mainly considered in technical terms (storage, register). When it comes to human needs beyond healthcare, the social of socio-technical society, it seems that this is delegated to NGOs.[10] This is to say, preparedness leans much more on technology, and it is likely expected that social issues handle themselves on the side and do not interfere with YTS functions. Although, to consider the public as one entity with converging needs is expedient for planning, doing so may create unforeseen consequences that may create friction and tensions, which in a time of crisis are counterproductive. The YTS does not address this issue and makes no mention how the actual plans approach this issue. It only refers to that it is not aimed towards the emergency of individual, only the nation. In the meanwhile, NGOs with their expertise in this field are trusted to manage consequences of this. If YTS requests for new risk detection and management, it would seem to have a need for to look into reduction of social tensions of any origin.

10 Although YTS mentions NGOs, they have not been part of the YTS creation and policy formulation. In the land of thousands of registered associations only few NGOs actually have had any knowledge of or connection to YTS. In a study by TPAK, conducted well before the latest YTS (and therefore may have improved since, to this latest YTS), it was established that ministries had widely varying level of interaction and attitudes towards NGOs, and possibility for citizen participation was non existent. Only three (Maanpuolustuskoulutusyhdistys, MPK – National Defence Training Association; Suomen Punainen Risti, SPR – Finnish Red Cross; Vapaaehtoinen pelastuspalvelu, Vapepa – Volunteer rescue services, consortium of organisations coordinated by SPR) were widely recognised as useful partners by the ministries (MPK and SPR both having legal requirements to prepare and assist authorities). Altogether fifty four NGOs were named by the ministries, of which fifteen were tied to MPK and twenty four to Vapepa. This creates two very disproportionately large hubs in the support network. Surprisingly – considering how central unions are in Finnish politics – only employer side has had major representatives participating. What is more, support and co-operation were seen one sided and scarce, and not providing a channel to participate. (Warro, 2009, p. 6-7, 12-13)

It is unthinkable to consider an alternative for security of this level to fail. Such an event would be something unforeseeable and catastrophic, Perhaps it is for this reason for that no guarantee or backup plan for YTS is given. On the other hand, refraining to make promises means there are none that could not be backed up nor broken. All are not guaranteed to be taken care of. There is no certainty that plans will work, or that designing them has been according to any specific ideals. They are given “as is”. Since YTS functions are for protecting the nation, keeping population safe and to keep society's wheels spinning, as long as these are true – regardless of the form, amount, or other factors – then the premise is that enough has been accomplished and the remainder keep carrying on with what they have. The goal of the system is not to be able to prevent all risks, but to manage them when they actualise. Risk and opportunity: none can stay in the moment gone by and future is change. Similarly, the collection of systems that is YTS is dynamic, evolving intention of preparedness. There is no guarantee of future, and thus we are only left to make contingencies. Such is the nature of security.

5. CONCLUSIONS AND FURTHER DISCUSSIONS

In this thesis central concepts for the topic have been made clearer, relevant theoretical discussions presented, and a reading done to a representable example with a suitable methodological framework. Risk, security and complex socio-technical systems have been explored and connected to time and place. The role of technology and networks has been established. This is what effects our digital culture, and this is what our digital culture effects.

Seeing life through risk can not happen without having an impact to both, the individual and the society. Security discourses are more and more present in our daily lives. The current financial crisis has had impacts that seem abstract to an individual (money lending between nations and businesses), but also have transformed into direct personal threat to survival, and in some places to violence. Some form of security discourse seems to have followed western civilisation intrinsically through out last centuries, from world wars to cold war. The September 11th 2001 can be seen as the father of the current discourse, that has already fostered new perspectives. These risks, wars, aggressions, conflicts, propaganda, exposure, communication have transferred to new areas, rapidly jumping from one network to another. And via networks ripples are created in new places and highly separated nodes are suddenly connected in a new way. We are creating links faster and every which way, and the first question are, “is this a risk to us”, “are we safe and secure”, and “how does this effect my future”, which all are fundamentally the same question. Without knowing better we can only make assumptions.

Critical Systems Heuristics used in this thesis to examine the Finnish Security Strategy for Society (2010) is one way to bring forth differing assumptions of how systems should behave. It is not an ideal candidate to demonstrate the full use of CSH framework, yet applying CSH to it has identified conflicts of interests. The YTS document is not an extreme example of system creators reference points differing from those that the system pertains to. The object has not been the full and exhaustive identification of these border assumptions, as limitations of this thesis and and selected source material do not permit that. This exercise has, however, brought forth some border assumptions, and other aspects as side product, to light.

In the Security Strategy for Society (2010) it is obvious that there are strong ties to the business community. The people are taken as one lump, and as separate of the business group. Technology and material needs are emphasised. Things are done mostly behind closed doors, presenting very

little possibility for partaking or feedback, to which modern citizens have grown accustomed to. Military defence, and crisis of that nature, have priority and dictate other preparedness measures. Support networks are expected to help, and markets that those networks are dependent on, are expected to remain stable. No guarantees are made – but at least we may be comforted by that the list of YTS preparedness functions and partaking authorities seems quite comprehensive.

The fact that these border assumptions can be seen, can not be taken indicative of any magnitude, or that there may be something particularly wrong with the situation. This does indicate that these observations should be looked closer to establish if something can be done to improve the situation. These border assumptions clearly demonstrate that even security, and security of critical systems, are not without subjective decisions and value selections. This reflects the similar findings put forth by Heinonen (2011). Although Finnish politicians may not like to talk about it, politics is played with security as well. Not even networks that could be though of as immune from influence, are not. Even though this may seem self evident from the words "policy" and "strategy" that are written in YTS, reality is not so outright. Thus, in other complex systems as well, it can be reasonably expected that subjective selections, as well as unintentional change, are present. Only simpler systems may boast with relative invariability.

It must also be noted that there is a possibility for misinterpreting critical reading as critique towards YTS and preparedness efforts. The mistake there lies in the assumption that the preparedness measures are questioned, when the true aim is to examine issues of systems behaviour and theory. Although YTS is a major connecting hub of national preparedness systems and a representation of part of a complex socio-technical system, it is not the whole picture. Similarly, anyone and everyone is connected to several complex systems affecting participation in others.

> "*No discourse participant is participant in one discourse only. As citizens, we are all part of diverse social systems and fulfil in these different systems various roles of a professional, private and public kind, which together offer a great variety of discursive chances*" (Ulrich, 2003, p. 331).

This statement continues, explaining that the experts and decision makers are also in multiple roles on multiple levels of several discourses and systems. They can not therefore be considered purely impartial, as has been argued, but also lacking expertise in other systems. Thus, there should be mixing and changing of roles depending on system.

These topics invite critique and counterarguments, as does also any subjective evaluation. One of

the tenets of Beck's Risk Society is self-reflective practises. This can and should be applied also to this thesis. Undoubtedly, along the writing process it already has. Ideas of how something may seem in the future, when read years from now, has had some influence to the text. Similarly has influenced the practise of thinking what writing is required to achieve a certain outcome, which is a series of minuscule contingencies to create coherent work, as much it may be a manifestation of subliminal confirmation bias. Science is not unambiguous. Decisions, observations, methods, context – all are influenced. As Beck puts it well, "*another computer, another researcher, another client, and another "reality" is the result*" (Beck, 1990, p. 174).

Complex socio-technical systems and human behaviour are unpredictable. This is what makes us human – apart of our failures, of course. Subjective analysis is subject to changed perspective in time, developed experience sphere, and new information, which all give variance to the results. It is also worth to remember that human behaviour and what can be observed of it, like systems, are not always sensible.

> *"We cannot assume that it is possible to eliminate contradictions in the social domain and, in consequence, in the theory of the social domain by purely logical means. If social life does not work in a purely logical way, then a theory of it cannot be formulated as free of logical contradictions."*
> (Luhmann, 1996a, p. 359)

Humans can be seen as complex systems, even when we are much more as well. Complex socio-technical systems we live amongst are not what we are. They are representations of what we do. Although our own little system does interact in complex ways with our surrounding systems, those systems are created by us in our cultures. For us in Finland, technical systems and digital networks are ubiquitous in most of our society.

Complex systems are part of modern technologies but are not synonymous with them. Not yet at least. It is reasonable to expect overall complexity to increase – much like entropy. Historically cultural periods have had the tendency to take counter positions to previous eras, and therefore similar counter movement to complexity may be behind the corner. Business minded might conceive a line of products that are at least outwardly providing extreme simplicity for users. In small ways this is can be seen already happening in all the devices we have come up with to help us manage our complex existences.

Technology will not disappear. It merely will (hopefully) become managed better. We will be able to control some of it better. Some of it, we will lose the control over to those with requisite knowledge and resources. Power then lies with hose who will control the technology and structures that control our social and societal functions. Question becomes, are we then labelled and treated according to one of the predetermined user profile categories, or are we able to maintain desired level of self-determination. Will we be allowed for ourselves to determine for which risks we give consent to subject ourselves to?

Stepping back, in the end one should consider the implications for further study. We can see that CSH could be applicable to any complex socio-technical system as it is. Should it be used more, and more data is generated, the results may warrant further study on CSH itself. It also is not purely reserved to the social field, but also to technical. CSH seems to have potential to be used in digital systems that mimic social interactions or manage them, and thus inherently make decisions. Both, the decision mechanisms, and the reasoning and bias behind the code, could be subjects of CSH. More importantly, two strands stem that warrant further research. Firstly, the level and means for participation and self-determination in designing security. In this topic, the principles of governance and freedom clash, but also the practicalities of organisation as well as confidentiality of security measures. As has been pointed out elsewhere, terrorists may kill but only the people themselves can take away freedoms and set adverse policies. This is to say, finding an equilibrium between aspects of security and aspects of freedom is still a work in progress. Secondly, the complex systems have been implied here to have several avenues of being influenced. The true control of (critical) complex systems need mapping and a methodology to determine the level and manner of influence. Risks can not be managed at all if they are not known. Furthermore, it is not only risks that need to be mapped, but those who through interconnectedness have influence on the systems. As contexts and motives change, a possibility merges that systems may become unreliable, and thus are not suitable for security. From the perspective of this thesis, this is as much of a social as it is a technical problem, and requires exploration from both directions.

REFERENCES

Printed sources

Barabási, A.-L. (2002). *The new science of networks*. Cambridge, MA, USA: Perseus Publishing.

Barthes, R. (2002). The death of the author. In D. Finkelstein & A. McCleery (Eds.), *The book history reader.* London, England: Routledge.

Beck, U. (1990). *Riskiyhteiskunnan vastamyrkyt*. Jyväskylä, Finland: Gummerus Kirjapaino Oy.

Beck, U. (1995a). Politiikan uudelleenkeksiminen. In U. Beck, A. Giddens, & S. Lash (Eds.), *Nykyajan jäljillä – refleksiivinen modernisaatio*. Jyväskylä, Finland: Gummerus Kirjapaino Oy.

Beck, U. (1995b). Mitä ymmärrämme teollisuusyhteiskunnan itsepurkautumisella ja -vaarannuksella. In U. Beck, A. Giddens, & S. Lash (Eds.), *Nykyajan jäljillä – refleksiivinen modernisaatio*. Jyväskylä, Finland: Gummerus Kirjapaino Oy.

Beck, U. (1998). *Democracy without enemies.* Cambridge, England: Polity Press.

Beck, U. (2000). *What is Globalization*. Cambridge, England: Polity Press.

Brostoff, S., & Sasse, M. A. (2001). Safe and sound: a safety-critical approach to security. In *NSPW '01 Proceedings of the 2001 workshop on New security paradigms*. New York, NY, USA: ACM.

Castells, M. (1999). *The Rise of the Network Society.* Oxford, England: Blackwell Publishers Inc.

Ciborra, C. (2007). *Digital technologies and risk: a critical review.* In O. Hanseth & C. Ciborra (Eds.), *Risk Complexity and ICT.* Cheltenham, England: Edward Elgar Publishing.

Egan, M. J. (2007). Anticipating future vulnerability: defining characteristics of increasingly critical infrastructure-like systems. *Journal of Contingencies and Crisis Management,* 15(1).

Fairclough, N. (2005). Blair's contribution to elaborating a new 'doctrine of international community'. *Journal of Language and Politics,* 4(1).

Giddens, A. (1995a). *Elämää jälkitraditionaalisessa yhteiskunnassa.* In U. Beck, A. Giddens, & S. Lash (Eds.), *Nykyajan jäljillä – refleksiivinen modernisaatio*. Jyväskylä, Finland: Gummerus Kirjapaino Oy.

Giddens, A. (1995b). *Riski, luottamus, refleksiivisyys*. In U. Beck, A. Giddens, & S. Lash (Eds.), *Nykyajan jäljillä – refleksiivinen modernisaatio*. Jyväskylä, Finland: Gummerus Kirjapaino Oy.

Giddens, A. (1997). *Sociology* (3rd ed.). Cambridge, England: Polity Press.

Gunder, M. (2008). Ideologies of certainty in a risk reality: beyond the hauntology of planing. *Planning Theory,* 7(2).

Hanseth, O. (2007). *Introduction: integration-complexity-risk – the making of information systems out-of-control*. In O. Hanseth & C. Ciborra (Eds.), *Risk Complexity and ICT.* Cheltenham, England: Edward Elgar Publishing.

Heinonen, V. (2011). *The state of Finnish security policy. A conceptual analysis of the Finnish debate on security policy in the early 2000s* Doctoral dissertation, Jyväskylä studies in education, psyhology and social research 416. Jyväskylä, Finland: University of Jyväskylä.

Hellström, T. (2003). Systemic innovation and risk: technology assessment and the challenge of responsible innovation. *Technology in Society*, 25(3).

Hellström, T. (2007). Critical infrastructure and systemic vulnerability: towards a planning framework. *Safety Science,* 45(3).

Hollnagel, E. (2008). Risks + barriers = safety? *Safety Science*, 46(2).

Kalliniakos, J. (2007). *Information technology, contingency and risk*. In O. Hanseth & C. Ciborra (Eds.), *Risk Complexity and ICT.* Cheltenham, England: Edward Elgar Publishing.

Kaplan, S., Garrick, B. J., & Apostolakis, G. (1981). Advances in quantitative risk assessment – The maturing of a discipline. *IEEE Transactions on Nuclear Science,* 28(1).

Kaplan, S., Haimes, Y. Y., & Garrick, B. J. (2001). Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk. *Risk Analysis*, 21(5).

Kirwan, B. (2001). Coping with accelerating socio-technical systems. *Safety Science,* 37(2-3).

Knodt, E. M. (1996). *Foreword.* In N. Luhmann, *Social Systems.* Stanford, CA, USA: Stanford University Press.

Lash, S. (1995). *Refleksiivisyys ja sen vastinpari: rakenne, estetiikka yhteisö*. In U. Beck, A. Giddens, & S. Lash (Eds.), *Nykyajan jäljillä – refleksiivinen modernisaatio*. Jyväskylä, Finland: Gummerus Kirjapaino Oy.

Little, R. G. (2004). Holistic strategy for urban security. *Journal of Infrastructure Systems*, 10(2).

Luhmann, N. (1996a). *Social Systems.* Stanford, CA, USA: Stanford University Press.

Mencken, H. L. (1921). *Prejudices: Second Series.* USA.

Midgley, G. (1997). Dealing with coercion: Critical Systems Heuristics and beyond. *Systemic Practice and Action Research,* 10(1).

Organisation for Economic Co-operation and Development (OECD). (2003). Emerging systemic risk in the 21st century: An agenda for action. Paris, France: OECD Publications.

Perrow, C. (1999). *Normal accidents: living with high-risk technologies*. Princeton, NJ, USA: Princeton University Press.

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: why technology and organisations (sometimes) fail. *Safety Science,* 34(1-3).

Pratchett, T. (1990). *Pyramids*. Reading, England: Corgi Books.

Pratchett, T. (1992). *Witches Abroad*. Reading, England: Corgi Books.

Prime minister's office. (2009). *Finnish security and defence policy.* In Prime Minister's Office Publications 13/2009 , government report. Helsinki, Finland: Prime minister's office.

Reiman, T. & Oedewald, P. (2007). Assessment of complex socio-technical systems – Theoretical issues concerning the use of organisational culture and organisational core task concepts. *Safety Science*, 45(7).

Reivo, J., Vuoripuro, J., & Pelkonen, N. (2010). *Communication and Security Management Co-operation in Large Events – Case: IAAF World Championships 2005 in Helsinki.* In R. Pirinen & J. Rajanmäki (Eds.), *Integrative Student-centered research and development work, sample of evidence series – Rescuing of intelligence and electronic security core applications (RIESCA)* (Vol. 1). Helsinki, Finland: Edita Prima Oy.

Rushby, J. (1994). Critical system properties: survey and taxonomy. *Reliability Engineering and System Safety*, 43(2).

Shoham, Y., & Layton-Brown, K. (2009). *Multiagent Systems: algorithmic, game-theoretic, and logical foundations*. New York, USA: Cambridge University Press.

Sihvonen, H.-M., Knuuttila, J., & Rajamäki, J. (2010). RIESCA, Rescuing of intelligence and electronic security core applications. In R. Pirinen & J. Rajanmäki (Eds.), *Integrative Student-centered research and development work, sample of evidence series – Rescuing of intelligence and electronic security core applications (RIESCA)* (Vol. 1). Helsinki, Finland: Edita Prima Oy.

Somerville, I. (2007). *Software Engineering* (8th ed.). New York, USA: Addison-Wesley Publishers ltd.

Ulrich, W. (2003). Beyond methodology choice: critical systems thinking as critically systemic discourse. *Journal of the Operational Research Society,* 54(4).

Ulrich, W., & Reynolds, M. (2010). *Critical systems heuristics*. In M. Reynolds & S. Howell (Eds.), *Systems approaches to managing change: a practical guide.* London, England: Springer.

van den Heuvel, M. P. & Sporns, O. (2011). Rich-Club Organization of the Human Connectome. *The Journal of Neuroscience*, 31(44).

Vitali, S., Glattfelder, J.B., & Battiston, S. (2011, October 26). The Network of Global Corporate Control. *PLoS ONE,* 6(10): e25995. doi:10.1371/journal.pone.0025995

Vuori, J. A. (2011). *How to do Security With Words – A grammar of securitisation in the People's Republic of China* Doctoral dissertation, Annales Universitatis Turkuensis B336. Turku, Finland: University of Turku.

Warro, E. (2009). *Kansalaisjärjestöt ja yhteiskunnan varautuminen*. Helsinki, Finland: Secretariat of the Security and Defence Committee (TPAK).

[YTS] (2010, December 16). *Security Strategy for Society*. Finnish government resolution. Helsinki, Finland: Ministry of Defence.

Online sources

Advisory Board for Defence Information, ABDI (MTS). (2010). *Finns' opinions on Foreign and Security Policy, Defence and Security issues 2010 (report).* Retrieved December 20, 2011, from http://www.defmin.fi/files/1685/MTS_survey_2010.pdf and http://www.defmin.fi/files/1686/MTS_Survey_statistics_2010.pdf

Beck, U. (2006, February 15). Living in The World Risk Society. In *A Hobhouse memorial public lecture 15th February 2006 the Old Theatre, London School of Economics, Houghton Street, London, England*. Retrieved December 18, 2011, from http://www.skidmore.edu/~rscarce/Soc-Th-Env/Env%20Theory%20PDFs/Beck--WorldRisk.pdf

Bullock, S., & Cliff, D. (2004, October 27). Complexity and emergent behaviour in ICT systems. Retrieved December 20, 2011, from http://www.hpl.hp.com/techreports/2004/HPL-2004-187.pdf

Coghlan, A. (2011, August 9). Weeds acquire genes from engineered crops. New Scientist. Retrieved December 21, 2011, from http://www.newscientist.com/blogs/shortsharpscience/2011/08/transgenenic-weed-doubles-its.html

Gantz, J., & Reinsel D. (2011, June). Extracting Value from Chaos. In *IDC iView.* Retrieved December 20, 2011, from http://www.emc.com/digital_universe

Hermeneutic Circle. In *Wikipedia*. Retrieved December 19, 2011, form https://en.wikipedia.org/wiki/hermeneutic_circle

Hermeneutics. In *Wikipedia*. Retrieved December 19, 2011, form https://en.wikipedia.org/wiki/Hermeneutics

Hermeneuttinen analyysi. In *Aineiston analyysimenetelmät – Jyväskylän yliopiston Koppa*. Retrieved December 19, 2011, from https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/hermeneuttinen-analyysi

Hermeneuttinen tulkinta. In *Kirjallisuusselvitys*. Retrieved December 19, 2011, from http://www2.uiah.fi/virtu/materiaalit/tuotetiede/html_files/120_kirjallisuus.html#herm

Humphrey, M. (2004). Working paper 2004/I – Human rights, counter-terrorism, and security. Retrieved December 17, 2011, from http://www.ahrcentre.org/working_papers/2004_1_Counter_Terrorism.htm

Jamail, D. (2011, June 16). Fukushima: It's much worse than you think. *Al Jazeera*. Retrieved December 21, 2011, from http://www.aljazeera.com/indepth/features/2011/06/201161664828302638.html

Luhmann, N. (1996b). Modern society shocked by its risks. In *Social Sciences Research Centre occasional paper.* Retrieved December 18, 2011, from

http://hub.hku.hk/bitstream/10722/42552/1/17.pdf

Moteff, J., Copeland, C., & Fischer, J. (2003, January 29). Critical infrastructures: What makes an infrastructure critical. In *Report for Congress Jan 29 2003 by Congressional Research Service, The Library of Congress, USA.* Retrieved December 18, 2011, from www.fas.org/irp/crs/RL31556.pdf

Medina, J. (2011, September 9). Human error investigated in California blackout's spread to six million. The New York Times. Referenced December 21, 2011, from https://www.nytimes.com/2011/09/10/us/10power.html?_r=1&scp=1&sq=blackout&st=cse

Nakashima, E. (2011, November 18). Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says. The Washington Post. Retrieved December 21, 2011, from http://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html

Nelosen Uutiset. (2011, September 26). Ydivoimaloiden suojavyöhykkeitä rukataan yhtiöiden toiveiden mukaisiksi – "Se 200 oli hatusta vedetty luku". *Nelosen Uutiset*. Retrieved December 19, 2011, from http://www.nelonen.fi/uutiset/kotimaa/kotimaa/ydivoimaloiden-suojavy%C3%B6hykkeit%C3%A4-rukataan-yhti%C3%B6iden-toiveiden-mukaisiksi-se-200-oli-hatusta

Peltola, M. (2005). Critical Analysis of the Finnish National Interests, National Security and the Security and Defence Policy. *Scientific Advisory Board for Defence (MATINE) summary report*. Retrieved December 19, 2011, from http://www.defmin.fi/files/1794/784_Peltola_Tiivistelmaraportti.pdf

Schirrmacher, F. (2011, November 1). Der griechische Weg - Demokratie ist Ramsch. *Frankfurter Allgemaine Zeitung*. Retrieved December 20, 2011, from http://www.faz.net/aktuell/feuilleton/der-griechische-weg-demokratie-ist-ramsch-11514358.html

Secretariat of the Security and Defence Committee (TPAK), (2009, December 9). List of participants December 9th 2009 NGO seminar and writers of YTS. In *email correspondence with secretariat.* Received September 30, 2011, from tpak@defmin.fi.

Secretariat of the Security and Defence Committee (TPAK). (2010, September 28). *Yhteiskunnan elintärkeitten toimintojen turvaamisesta (YETT) annetun valtioneuvoston periaatepäätöksen tarkistaminen,* Ministry of Defence document filing number FI.PLM.2010-3771 906/80.01.07/2009. In *email correspondence with secretariat.* Received September 30, 2011, from tpak@defmin.fi.

Sowa, J. F. (2006, March 17). The law of standards. Retrieved December 18, 2011, from http://www.jfsowa.com/computer/standard.htm

Symantec. (2011, October). *Duqu: The Precursor to the Next Stuxnet*. Retrieved December 20, 2011, from http://www.symantec.com/business/outbreak/?id=stuxnet

Tsilonis, V. (2002). The Risk Society – interview with professor Ulrich Beck. *InterPares*.

Retrieved December 17, 2011, from http://www.intellectum.org/articles/topics/gb_beck.htm

Ulrich, W. (2005). A brief introduction to critical systems heuristics (CSH). Retrieved December 19, 2011, from http://wulrich.com/downloads/ulrich_2005f.pdf

Uncertainty principle. In *Wikipedia*. Retrieved December 19, 2011, from https://en.wikipedia.org/wiki/Uncertainty_principle

Visarraga, D. B. (2011). Understanding Complex Systems: Infrastructure Impacts. Retrieved December 18, 2011, from http://www.mathaware.org/mam/2011/essays/complexsystemsVisarraga.pdf

Väkevä, L. (1999, April 19). *Hermeneutiikka tieteellisenä lähestymistapana*. Retrieved December 19, 2011, from http://wwwedu.oulu.fi/muko/lvakeva/Lisuri/hermeneu.htm

YLE news (2010, December 11). Ex-valtiosihteeri Volanen: Sotilaat hamuavat kriisijohtamista. *YLE Uutiset*. Retrieved December 19, 2011, from http://yle.fi/uutiset/talous_ja_politiikka /2010/12/ex-valtiosihteeri_volanen_sotilaat_hamuavat_kriisijohtamista_2212632.html

APPENDICES

A. Reading, excerpts from YTS

Lists of excerpts from Security Strategy for Society (YTS) that were selected in the reading using applied Critical Systems Heuristics (CSH). Selected texts are listed below each question, preceded by page number of the referenced document. Questions five and six have combined lists due to similarities of questions.

I. Sources of motivation (The involved)

1. Beneficiary: Who ought to be/is the intended beneficiary of the system? (is there unintended)

1: The principles, objectives and implementation criteria for Finland's security and defence policy were provided in the Finnish Security and Defence Policy Report in 2009.
2: The Resolution was written from the perspective of functions vital to society that will be secured in all conditions.
3:The most important tasks of Finland's foreign, security and defence policy is to safeguard national sovereignty, territorial integrity and basic values; promote the population's security and well-being; and maintain the functioning of society.
8: However, this can only be built on the recognition by the business community that the benefits of co-operation are worth the resources invested in it.
15: The systems created for emergency conditions can be used for managing disturbances under normal circumstances.
36: the population and the business community's basic needs and supports a sufficiently healthy state economy.
37: The general goals of security of supply are scaled to safeguard the population's livelihood and to uphold society's vital functions as well as the material preconditions for national defence.

2. Purpose: What ought to be/is the purpose of the system?

1: One of the fundamental tasks of the state leadership is to guarantee the security of society.
1: The principles, objectives and implementation criteria for Finland's security and defence policy were provided in the Finnish Security and Defence Policy Report in 2009. The Resolution on the Security Strategy for Society, based on a comprehensive security concept, concretises [sic] *these principles and goals.*
3: The Strategy has been compiled from the viewpoint of safeguarding functions that are vital to society in all situations.
3:The most important tasks of Finland's foreign, security and defence policy is to safeguard national sovereignty, territorial integrity and basic values; promote the population's security and well-being; and maintain the functioning of society.
4: The Government directs, supervises and coordinates the securing of functions vital to society. Each competent ministry does the same within its respective administrative sector.
15: The systems created for emergency conditions can be used for managing disturbances under normal circumstances.
36: the population and the business community's basic needs and supports a sufficiently healthy state economy.
37: The general goals of security of supply are scaled to safeguard the population's

livelihood and to uphold society's vital functions as well as the material preconditions for national defence.

3. Measure of improvement: What ought to be/is the system's measure of success?

1: The principles, objectives and implementation criteria for Finland's security and defence policy were provided in the Finnish Security and Defence Policy Report in 2009.
1: In addition, the changes that have taken place in legislation, the experiences gained in VALHA 2010 preparedness exercise and in the management of disturbances were taken into account in the review as well as the reports that assessed the utilisation and implementation of the 2006 Resolution.
2: Supported by the meeting of the heads of preparedness of the ministries, the Security and Defence Committee is responsible for the joint monitoring and development of the Strategy.
2: The Resolution further defines that the top state leadership shall be informed, on a regular basis, of the results of the monitoring.
2: The decision on the next review of the Resolution will be made by the Government.
6: municipal bodies. Elected officials should fully familiarise themselves with and be involved in the objectives of preparedness.
63: TPAK submits the results of the monitoring to the President of the Republic, the Government (the Cabinet Committee on Foreign and Security Policy) and the Parliament (in particular to the Defence Committee and Foreign Affairs Committee).
By informing parliamentary committees it is ensured that society's preparedness will be implemented in line with parliamentary guidelines.
In co-operation with the subordinate administration and co-operation partners, ministries draw up a report on a regular basis on the functioning of crisis preparedness and development needs to the Security and Defence Committee.

II. Sources of control (The involved)

4. Decision maker: Who ought to be/is in control of the conditions of success of the system?

1: The principles, objectives and implementation criteria for Finland's security and defence policy were provided in the Finnish Security and Defence Policy Report in 2009.
1: Each ministry, within its mandate, steers preparedness [...]
2: Supported by the meeting of the heads of preparedness of the ministries, the Security and Defence Committee is responsible for the joint monitoring and development of the Strategy.
2: The Resolution further defines that the top state leadership shall be informed, on a regular basis, of the results of the monitoring.
2: The decision on the next review of the Resolution will be made by the Government.
4: The Security and Defence Committee, supported by the meeting of the heads of preparedness of the ministries, is responsible for the joint monitoring of the Strategy in co-operation with the different authorities, the business community and organisations.
4: In emergency conditions, the Government, subject to a Parliament decision, may be authorized to use the additional emergency powers provided in the Emergency Powers Act.
4: According to the Emergency Powers Act, presently under review, the Government would introduce the statute on implementing the Emergency Powers Act after having concluded with the President of the Republic that the country faces emergency conditions.
4: Important aspects of foreign and security policy and other matters concerning Finland's relations with other states, associated key internal security issues, and significant comprehensive defence approach issues are handled at the joint meeting of the President of the Republic and the Cabinet Committee on Foreign and Security Policy [...]
4: Government decisions are made either at plenary sessions or within the ministry

concerned [...]
4: The Prime Minister directs the activities of the Government. The Prime Minister's Office assists the Prime Minister in the overall management of the Government and in coordinating the work of the Government and Parliament.
4: The Government directs, supervises and coordinates the securing of functions vital to society. Each competent ministry does the same within its respective administrative sector.
5: The Meeting of Permanent Secretaries and the Meeting of Heads of Preparedness are permanent co- operation bodies.
5: The Ministry of Defence is responsible for co-ordinating comprehensive defence activities. Coordinating the comprehensive defence approach involves synchronising measures of the public sector, that is, the Government, State authorities and the municipalities, and the private sector and voluntary activities by citizens in order to maintain the functions vital to society under all circumstances.
5: The Security and Defence Committee (TPAK) assists the Ministry of Defence and the Cabinet Committee on Foreign and Security Policy on matters relating to comprehensive defence and its co-ordination. The Committee monitors changes in the security and defence policy and situation and evaluates their effects on comprehensive defence arrangements. The Committee has the task of monitoring and co-ordinating the different administrative sectors' comprehensive defence measures.
5: Ministry of Finance is responsible for the general guidance and development of these systems and information networks; it is also responsible for the general guidance and directing of information security and ICT preparedness in the public sector.
8: The co-operation between public and private sectors and its continuous development are essential because the main part of the resources required by security tasks is, as a rule, owned by the business community.
8: Long, even global value chains and the internationalisation of companies have significantly decreased the preconditions of national authorities to regulate, steer or control the activities of companies.
10: Other EU policies also have a significant impact on Finland's possibilities to secure society's vital functions during disturbances.
16: In securing the functions vital to society the commonly accepted and observed principles of the Finnish society are to be followed.
63: TPAK submits the results of the monitoring to the President of the Republic, the Government (the Cabinet Committee on Foreign and Security Policy) and the Parliament (in particular to the Defence Committee and Foreign Affairs Committee).
By informing parliamentary committees it is ensured that society's preparedness will be implemented in line with parliamentary guidelines.
In co-operation with the subordinate administration and co-operation partners, ministries draw up a report on a regular basis on the functioning of crisis preparedness and development needs to the Security and Defence Committee.

5. Resources: What conditions of success ought to be/are under the control of the system?
6. Decision: What conditions of success ought to be/are outside the control of the decision maker?

1: Each ministry, within its mandate, steers preparedness [...]
2: Also other parts of the public administration, in particular municipalities, and the business community and organisations play an important role in the implementation of the strategic tasks.
3: The Resolution on the Security Strategy for Society (hereafter Strategy) provides the guidelines to ministries and also to regional and local administration for achieving these goals.
3: The measures required to implement the policy decisions of the Government Report on

Finnish Security and Defence Policy are discussed in the Strategy.
3: A number of decisions, strategies and guidelines related to preparedness and crisis management, issued by the Government and different administrative sectors are complementary to it.
4: The Government directs, supervises and coordinates the securing of functions vital to society. Each competent ministry does the same within its respective administrative sector.
5: The Ministry of Defence is responsible for co-ordinating comprehensive defence activities. Coordinating the comprehensive defence approach involves synchronising measures of the public sector, that is, the Government, State authorities and the municipalities, and the private sector and voluntary activities by citizens in order to maintain the functions vital to society under all circumstances.
5: Ministry of Finance is responsible for the general guidance and development of these systems and information networks; it is also responsible for the general guidance and directing of information security and ICT preparedness in the public sector.
6: Because municipalities for the most part have the responsibility for organising basic services and other functions vital to society, their role in local administration is central to society's preparedness and management of disturbances.
6: As a result, the roles and responsibilities of supramunicipal organisations and external service providers in preparedness related matters must be defined and well-functioning co-operation procedures are to be established.
6: The securing of functions vital to society as a whole is related to intersectoral activities between different administrative sectors and the co-operation between the state, municipalities, the business community and organisations.
6-7: Apart from municipalities and their co-operation bodies, the actors of the regional state administration, parishes and religious communities, universities and other educational establishments and the units of the business community that contribute to the service production of the local government play a key role in regional preparedness and securing functions vital to society. Organisations, too, are important service providers and actors in building preparedness.
7: Well-functioning co-operation between public authorities and the business community create and maintain security of supply in Finland.
7: In addition to national preparedness, the preparedness measures taken in the European Union, the agreement on the International Energy Programme and the multilateral and bilateral agreements on economic co-operation in crisis situations concluded with a number of countries contribute to security of supply.
7: Information and communication technology (ICT) services, transportation and the office ownership and management are amongst the service entities where outsourcing is typical. Another trend in the business community is internationalisation. The Finnish business community is part of a global network where industrial plants merge and through the flows of raw material, information and people become an entity where change is permanent.
8: The co-operation between public and private sectors and its continuous development are essential because the main part of the resources required by security tasks is, as a rule, owned by the business community.
8: This requires, from the perspective of the business community, the possibility to efficiently provide products and services for the needs of the authorities on the commercial basis, which allows it to contribute also to societal discussion.
8: Some sectors such as telecommunications, transport, energy and financing are obligated to preparedness by legislation.
8: However, this can only be built on the recognition by the business community that the benefits of co-operation are worth the resources invested in it.
9: They produce and maintain resources and expertise that support the authorities and, in

addition, implement education and communication that support and promote preparedness.
9: NGOs play an important role in, for example, search and rescue, air rescue operations and maritime search and rescue, civil defence and fire fighting, voluntary defence as well as organising first aid and psychological support.
9: Various organisations run sports, cultural, youth and other societal activities, representing a significant segment of our civil society. The ability to recognise individual needs is one of the strengths of these organisations. They are often extensively networked, both nationally and internationally.
10: It is not possible to secure all vital functions merely through national arrangements.
10: Other EU policies also have a significant impact on Finland's possibilities to secure society's vital functions during disturbances.
10: In accordance with the Solidarity Clause of the Treaty of Lisbon that came into force in 2009, the Union and its Member States act jointly in the spirit of solidarity if another Member State is the subject of a terrorist attack or the victim of a natural or man-made disasters.
12: Arrangements on medical supplies, defence materiel and securing electricity transmission systems have been made under the auspices of Nordic co-operation. The Treaty of Lisbon provides the opportunity to deepen Nordic co-operation.
36: The role of public authorities in securing the welfare of citizens inevitably increases when normal economic activities are disturbed.
37: The premise of Finland's security of supply is the proper functioning of the single European market.
38: The ICT systems used by organisations and the population are reliable and secure.
38: Statutory basic security requirements are assigned to communication services and service infrastructure.
38: Compliance with regulations concerning system construction, maintenance and functioning is monitored.
41: It is ensured that society's vital functions relying on communications networks, communications services and other ICT systems are not paralysed because of functional disruptions and that services can be quickly recovered.
41: If need be, the authorities prepare to guide, regulate and categorise networks and their services as well as user groups according to their relative importance.
41: The competent ministry or government agency is given a role involving the entire state administration and the powers to negotiate with different service providers as to how services are secured for the various actors in state administration during disturbances in normal as well as in emergency conditions when service providers prioritise their production of services.

III. Sources of knowledge (The involved)

7. Expert: Who ought to be/is providing relevant knowledge and skills for the system?

2: Supported by the meeting of the heads of preparedness of the ministries, the Security and Defence Committee is responsible for the joint monitoring and development of the Strategy.
4: The Security and Defence Committee, supported by the meeting of the heads of preparedness of the ministries, is responsible for the joint monitoring of the Strategy in co-operation with the different authorities, the business community and organisations.
5: The Meeting of Permanent Secretaries and the Meeting of Heads of Preparedness are permanent co- operation bodies.
6: Because municipalities for the most part have the responsibility for organising basic services and other functions vital to society, their role in local administration is central to society's preparedness and management of disturbances.

6: As a result, the roles and responsibilities of supramunicipal organisations and external service providers in preparedness related matters must be defined and well-functioning co-operation procedures are to be established.
6-7: Apart from municipalities and their co-operation bodies, the actors of the regional state administration, parishes and religious communities, universities and other educational establishments and the units of the business community that contribute to the service production of the local government play a key role in regional preparedness and securing functions vital to society. Organisations, too, are important service providers and actors in building preparedness.
8: This requires, from the perspective of the business community, the possibility to efficiently provide products and services for the needs of the authorities on the commercial basis, which allows it to contribute also to societal discussion.
8: Some sectors such as telecommunications, transport, energy and financing are obligated to preparedness by legislation.
8: However, this can only be built on the recognition by the business community that the benefits of co-operation are worth the resources invested in it.
9: They produce and maintain resources and expertise that support the authorities and, in addition, implement education and communication that support and promote preparedness.
9: Various organisations run sports, cultural, youth and other societal activities, representing a significant segment of our civil society. The ability to recognise individual needs is one of the strengths of these organisations. They are often extensively networked, both nationally and internationally.
63: TPAK submits the results of the monitoring to the President of the Republic, the Government (the Cabinet Committee on Foreign and Security Policy) and the Parliament (in particular to the Defence Committee and Foreign Affairs Committee).
By informing parliamentary committees it is ensured that society's preparedness will be implemented in line with parliamentary guidelines.
In co-operation with the subordinate administration and co-operation partners, ministries draw up a report on a regular basis on the functioning of crisis preparedness and development needs to the Security and Defence Committee.

8. Expertise: What ought to be/are relevant new knowledge and skills for the system?

9: Security research which is based on national approach provides targeted information to support decision-making, identifies new threats and opportunities in a rapidly changing world and develops courses of action, instruments and systems for the management of various disturbances and crises.

9. Guarantor: What ought to be/are regarded as assurances of successful implementation?

2: For the basis of preparedness, preventing and combating threats and, further, for securing the functions vital to society the ministries are given the responsibility to develop, steer and monitor strategic tasks in accordance with the requirements of the security environment.
2: Also other parts of the public administration, in particular municipalities, and the business community and organisations play an important role in the implementation of the strategic tasks.
9: They produce and maintain resources and expertise that support the authorities and, in addition, implement education and communication that support and promote preparedness.
9: NGOs play an important role in, for example, search and rescue, air rescue operations and maritime search and rescue, civil defence and fire fighting, voluntary defence as well as organising first aid and psychological support.

9: Various organisations run sports, cultural, youth and other societal activities, representing a significant segment of our civil society. The ability to recognise individual needs is one of the strengths of these organisations. They are often extensively networked, both nationally and internationally.
38: The ICT systems used by organisations and the population are reliable and secure.
38: Statutory basic security requirements are assigned to communication services and service infrastructure.
38: Compliance with regulations concerning system construction, maintenance and functioning is monitored.
41: Compliance with regulations concerning system construction, maintenance and functioning is monitored.
41: If need be, the authorities prepare to guide, regulate and categorise networks and their services as well as user groups according to their relative importance.
41: The competent ministry or government agency is given a role involving the entire state administration and the powers to negotiate with different service providers as to how services are secured for the various actors in state administration during disturbances in normal as well as in emergency conditions when service providers prioritise their production of services.

B. List of YTS writers and commentators

Security Strategy for Society (YTS) writing group (Secretariat of the Security and Defence Committee [TPAK], 2009, n.p.).

- Bank of Finland, Veli-Matti Lumiala
- Defence Command, Pekka Toveri
- Ministry for Foreign Affairs of Finland, Johanna Kotkajärvi
- Ministry of Agriculture and Forestry, Vesa Kiskola
- Ministry of Agriculture and Forestry, Timo Tolvi
- Ministry of Defence, Tiina Tarvainen
- Ministry of Defence, Petteri Tervonen
- Ministry of Education, Joni Hiitola
- Ministry of Education, Kirsti Kupiainen
- Ministry of Education, Heikki Rosti
- Ministry of Employment and the Economy, Kari Mäkinen
- Ministry of Finance, Marko Synkkänen
- Ministry of Justice, Olli Muttilainen
- Ministry of Justice, Ari Pajuniemi
- Ministry of Social Affairs and Health, Olli Haikala
- Ministry of the Environment, Jyri Juslén
- Ministry of the Interior, Olli Lampinen
- Ministry of Transport and Communications, Rauli Parmes
- National Emergency Supply Agency, Hannu Pelttari
- Prime Minister's Office, Hannu Mäntyvaara
- Secretariat of the Security and Defence Committee, Aapo Cederberg
- Secretariat of the Security and Defence Committee, Matti Piispanen
- Secretariat of the Security and Defence Committee, Eeva Warro
- Secretariat of the Security and Defence Committee, Tero Ylitalo
- The Finnish Border Guard, Hannu Tervo

- The Social Insurance Institution of Finland, Matti Tuomi
- The Social Insurance Institution of Finland, Jukka I. Hänninen

List provided by TPAK secretariat of non-governmental organisations (NGOs) who participated on the December 9th 2009 NGO seminar (TPAK , 2009, n.p.).

- Allianssi ry
- Autoliitto
- Electronic Frontier Finland ry
- Elintarviketeollisuus ry
- Iholiitto ry
- Kadettikunta ry
- Kuurojen Liitto ry
- Maa- ja metsätaloustuottajain Keskusliitto MTK
- Maanpuolustuskorkeakoulu
- Maanpuolustusnaisten Liitto ry
- Millog Oy
- MPK
- Naisten Valmiusliitto ry
- SPEK
- SPR
- Suomen Humanitaarisen Oikeuden Seura
- Suomen Kotiseutuliitto
- Suomen Kylätoiminta
- Suomen Lentopelastusseura SLPS ry
- Suomen Mielenterveysseura
- Suomen Naisjärjestöjen Keskusliitto ry
- Suomen Radioamatööriliitto ry
- Suomen Rauhanturvaajaliitto ry
- Suomen Reserviupseeriliitto ry
- Suomen Tiepalvelumiehet
- Vantaan nuorisopalvelut

List provided by TPAK secretariat of authorities, entities and organisations that were requested to comment on the preliminary YTS text (TPAK, 2010, p. 2).

- The Office of the President of the Republic of Finland
- Ministries (12)
- National Emergency Supply Agency
- The Social Insurance Institution of Finland (KELA)
- Bank of Finland
- Association of Finnish Local and Regional Authorities
- The National Defence Training Association of Finland (MPK)
- Scientific Advisory Board for Defence
- Finnish Red Cross (SPR)
- National Rescue Association (SPEK)