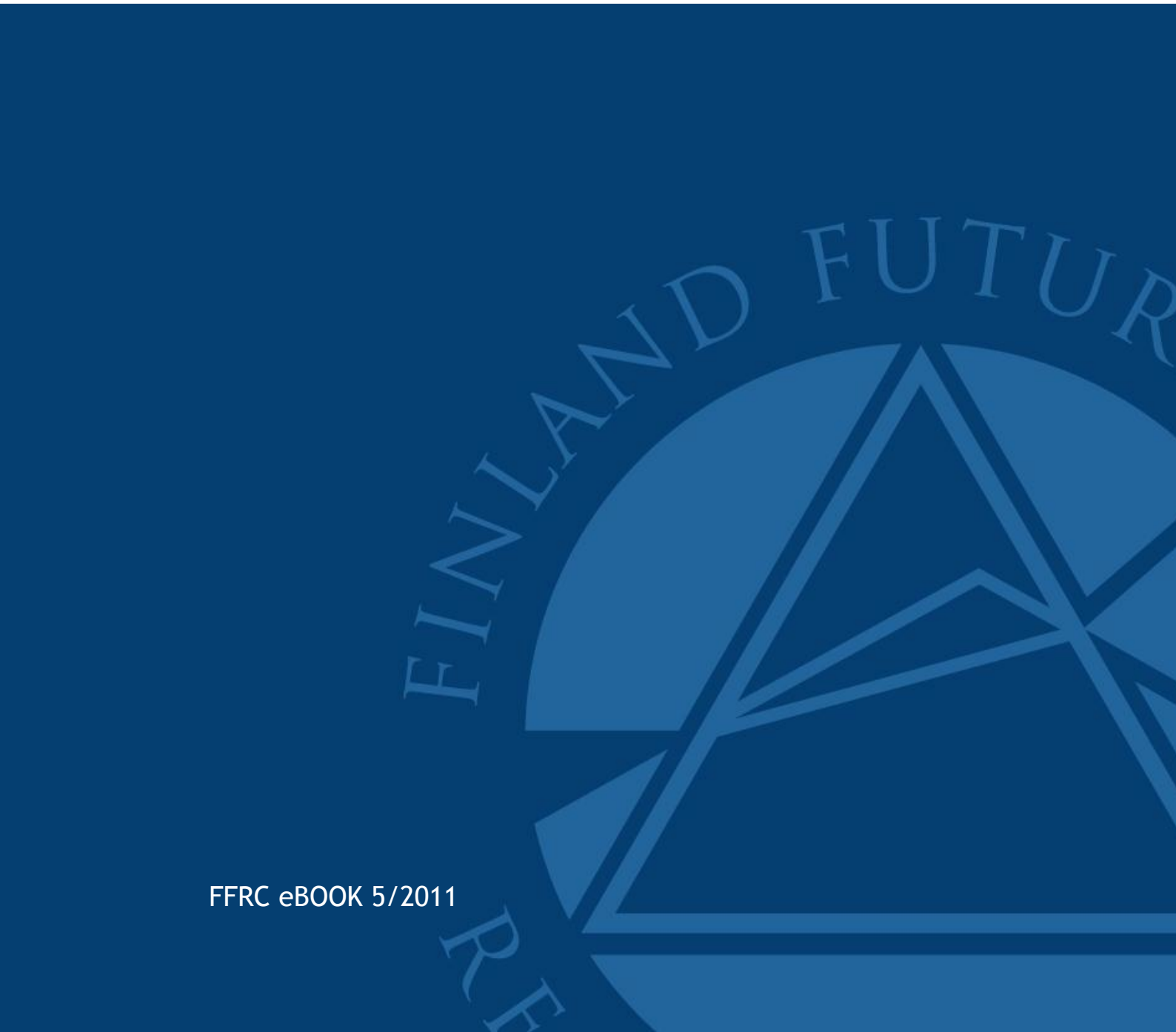
Burkhard Auffermann & Juha Kaskinen (editors)

SECURITY IN FUTURES – SECURITY IN CHANGE

Proceedings of the Conference “Security in Futures – Security in Change”, 3-4 June 2010, Turku, Finland



FFRC eBOOK 5/2011

Editors:

Burkhard Auffermann
Dr. phil., Senior Researcher
Finland Futures Research Centre, University of Turku
burkhard.auffermann@utu.fi

Juha Kaskinen
Ph.D., Director
Finland Futures Research Centre, University of Turku
juha.kaskinen@utu.fi

Layout Anne Arvonen & Jenni Elo

ISBN 978-952-249-063-6
ISSN 1797-132

Finland Futures Research Centre
University of Turku
Rehtorinpellonkatu 3, FI-20500 Turku
Korkeavuorenkatu 25 A 2, FI-00130 Helsinki
Pinninkatu 47, FI-33100 Tampere
Tel. +358 2 333 9530
Fax +358 2 481 4630
http://ffrc.utu.fi
tutu-info@utu.fi, firstname.lastname@utu.fi

CONTENTS

INTRODUCTION

The 12th Annual Conference of the Finland Futures Research Centre (FFRC) and the Finland Futures Academy was held 3–4 June 2010 in Turku, Finland. The conference was titled "Security in Futures – Security in Change". Five internationally recognized keynote lecturers, more than 40 workshop presentations in8 parallel workshops and more than 100 participants from all over the world brought new viewpoints and novel ideas.

By developing images of alternative futures, the goal of the conference was to give new viewpoints and novel ideas to decision-makers to assist them towards more feasible decisions to construct the world a better place. Security means that something is safe and protected – the absence of threats. Empirically, that is not possible and in consequence security is always a relative concept. Security is something that guarantees our lives to continue without fear of termination in physical and mental domains under a shield provided by the society.

Security, in general terms, can be understood as a political and analytical concept related to such policy fields as social, or domestic or internal security of a state or a society. In the context of external security, security is conventionally linked to the protection of the integrity of the society against external threats. Traditional conceptions of external security are primarily linked to the state, or a coalition of states, and, in most cases, military means are seen as the primary instruments of security building. However, this traditional understanding invited substantial criticism already during the Cold War when external military threat was considered the ultimate threat to the safety and integrity of a society. Alarmed by the prospects of the escalation of the arms race and the proliferation of nuclear weapons, proposals for new security thinking were presented in the context of 'common security' in the 1980s. During the 1990s, 'comprehensive security' and 'preventive security' were attempts to respond to the emerging security threats and challenges such as climate change, large scale poverty, human rights violations, and organized crime.

Security means that something is safe, sure and protected. *Security is something that guarantees our lives to continue without any fear of partial or total termination in physical and mental domains under a shield provided by trusted community.* Security analysis aims to delve deeply inside the inevitable change of security issues' revelation in a changing world compared to the immemorial human need to feel secure. Human activities and circulation are spreading more and more into the global production and business networks, information networks and ideological networks thus partly departing from the traditional nationally controlled context. Novel thinking and solutions are required to fulfil the immemorial human need to feel secure. The expansion of the reachable space, either physical or virtual, simultaneously with the feeling of the compression of perceived temporal axis, has led to a situation, where completely new kind of perceptions and activity patterns are combined with traditionally experienced phenomena. This new, mixed and broader world brings much more information into our vicinity about real and potential catastrophes, new kinds of technologies and new ways to encounter unknown people and their thinking and their ways to live. It also enables groups and individuals to demonstrate their

worldviews, aims and thoughts much more freely without social and legal restrains than it has been possible in traditionally organized physical world.

The traditionally experienced way of existence in the world will face new challenges. This changed situation might feel obscure, fuzzy and even weird or frightening, thus increasing and changing the revelation of the security demands towards community. At the same time, familiarity of traditionally experienced ways to interact with the world are gradually fainting away from own control. Assuring security gets new forms via the agony of inevitable change of the multi-actor, global interaction environment. To decrease the feeling and further on the realization of insecurity, the foreseen changes and the states of the futures shall be brought into the context with novel and innovative ideas of making the future more feasible. Bringing this information into publicity, security in the changing world will increase in the future while disagreements, wrong fears and empty wishes will settle outside the realistically reachable world of the future.

The conference aimed to look deeply into the inevitable changes of security issues. The traditional way we experience our existence in the world faces new challenges. The situation may feel obscure, fuzzy and even weird or frightening. Thus, it will increase and change the quality and quantity of security we demand from our communities. At the same time, awareness of the ways of interacting with the world is gradually slipping away from our own control. To decrease the feeling and, further on, the realization of insecurity, the foreseen changes and the states of the futures shall be brought closer to our everyday by introducing novel and innovative ideas of making the future more feasible. Novel thinking and solutions are required to fulfil the human need to feel secure and to build more reasonable security solutions for futures' world.

Joint sessions included the following keynote speeches: "The Future Role of the EU in European Security Politics" by Dr Teija Tiilikainen, Director of The Finnish Institute of International Affairs, Finland; "The Changing Futures of Social Security" by Professor Joakim Palme, Director of the Institute for Futures Studies, Sweden; "Emerging Technologies and Evolving Security Challenges in the Coming Decades" by Dr Yair Sharan, Director of The Interdisciplinary Center for Technology Analysis & Forecasting, Tel-Aviv University, Israel; "Climate Change, Resource Conflicts and Sustainable Peace: Addressing Future Security Challenges", by Propfessor Jürgen Scheffran, University of Hamburg, Germany; "Taming the Dragon: Risk, Chaos and the Loss of Security in the Age of Bifurcation" by Professor Markku Wilenius, Allianz Group, Germany & Finland Futures Research Centre, University of Turku, Finland. Furthermore, a panel discussion with Dr Teija Tiilikainen, Professor Joakim Palme, Professor Elina Pirjetanniemi (Åbo Academy University Turku), Professor Veikko Rouhiainen (VTT Tampere), and Professor Rauno Kuusisto (Finlande's Armed Forces, Riihimäki/Finland) was led by Dr Burkhard Auffermann, Senoir Researech Fellow, FFRC.

Workshops on the following aspects of security and safety were organized:

- International and Political Security (incl. Arms Races and Disarmament)
- Military and Defence (incl. Terrorism and Crime)
- Environment, Energy and Climate Change
- Security and Development
- Technology and ICT
- Business

- Culture (incl. Control and Surveillance)
- Theory and Methodology of Futures Studies (not only security-related).

Burkhard Auffermann & Juha Kaskinen

1. INTERNATIONAL AND POLITICAL SECURITY

THE COLLABORATION OF SECURITY ACTORS – ASPECTS FOR FUTURES RESEARCH

Vesa Valtonen
Major G.S. (PhD student)
Finnish Defence Forces

ABSTRACT - *This article presents aspects for futures research in security actors' collaboration. These aspects are based on recent research[1] dealing with the success factors in security actors' collaboration at the operational-tactical (collaboration practice) level. Along with the fundamentals of security actors' collaboration, a number of future implications were also discussed, which led to this article. The primary conclusion is that there is a clear need for comprehensive futures research at the operational-tactical scale regarding collaboration in security issues. In addition, certain constraints keep us focused on the present, our "comfort zone". This paper addresses these future aspects and presents a number of ideas for security- and collaboration-oriented futures research to come.*

Introduction

The changes in the overall security environment require ever-greater collaboration among security actors. The general requirement of keeping society secure and functional is hard to fulfil when the operational systems become more sophisticated, complex and interdependent. Only few actors can consider to be independent, e.g. in case of power failure. The need for reliable partners has also awakened an interest in the fundamentals of collaboration in security contexts. The primary question is: "What are the key elements for successful collaboration in general and in special contexts, such as the security environment?" In seeking a basis for daily ongoing collaboration, we may realize that the contexts, actors and even the united labour (Elliot 2007) itself are developing and changing rapidly in ways that are hard to foresee. When we are trying to create modern and robust security collaboration processes, we mainly react, which means that our actions are late. The collaboration processes should be thought through at least one step ahead. This requires Futures Research to observe the trends and signals and to be involved in shaping the possible futures.

This article approaches the possibilities of Futures Research to study security collaboration at the operational-tactical level, i.e. at the lowest echelon in practical collaboration in time-sensitive security situations, where a failure may lead to loss of human lives. For example, fire fighters, emergency units,

[1] Valtonen 2010, dissertation: *The Collaboration of Security Actors, Turvallisuustoimijoiden yhteistyö,* manuscript, under review.

police, military, and some other security actors operate in such conditions on a daily basis. At the other end, the operational level has to deal with challenges in leadership, information management, logistics and other support elements. A common feature is that you have to act fast, basing your actions on "good enough" knowledge to achieve your primary target (in the military, this means winning the battle, while in everyday life it usually means saving people's lives).[2] Collaboration in these environments most often involves voluntary organizations and private sector actors whose actions should be united for a common purpose. This is the short description of the operational environment that should be considered in the futures evaluations.

The referred research showed that collaboration among security actors has certain special features. Security collaboration requires trust, relevant capabilities and collaboration skills. In order to begin collaboration, a security partner has to show that it is reliable and has the necessary resources and certified capabilities. One example of an actual reliable capability is being able to demonstrate that you can handle secret information properly. Security information is often secret and only available to reliable partners. For this reason, it is difficult to use security information as a reference in the context of scientific research, where all publications should be public.

There are also other challenges in research on security collaboration. The most fundamental challenge is the definition of the terms, roles and actors themselves. In most cases, a terminological consensus has to be reached before addressing the subject. The terms *security* and *collaboration* have many meanings. In the Finnish language, the most fundamental dilemma is the two major roles and features of security. In English, there is a clear difference in the terms *security* and *safety*, but in Finnish they are combined in one word, "turvallisuus". Security, which refers to the more societal aspects of "turvallisuus", is mostly used and understood correctly, but some misunderstandings and difficulties still arise when safety matters are mixed with operational security level issues. That is only the tip of the iceberg of misunderstandings.

In collaboration, we might face problems that are quite similar yet not the same. Collaboration is not the only term describing united labour, even in English. In many security collaboration contexts, it is important to define the meaning of collaboration in detail (e.g. security information, administrative aspects, etc.). One way of approaching the terminological differences is to examine the aspects distinguishing the terms *networking, coordination, cooperation and collaboration*. Himmelman (1994, 2002) describes the common differences of definitions by comparing the interdependence of information and resources. From his point of view, the term *collaboration* is quite well suited to security collaboration.[3]

In some cases, the structure and the responsibilities in a collaboration context are so clear that proceeding to the subject does not require moderation phases (e.g. emergent daily situations). In rarer ad hoc situations, the whole operational system should be evaluated in a short period of time in order to enhance the collaboration of relevant actors.

Even when we share the common view of the environmental and terminological aspects, we may still have very different perspectives and objectives from the cultural point[4] of view. These constraints will

[2] Working hypothesis for paradigm of tactics (Valtonen 2008).
[3] In Himmelman's comparison, collaboration involves the highest degree of increased reliability and sharing of information and resources.
[4] This may include individual, organizational, ethical, etc. aspects.

mostly fade away in emergent time-sensitive situations, but if there is enough time to explore the fundamentals of collaboration, the features of power, profit, etc. will gain greater meaning. Successful collaboration between security actors at the operational-tactical level involves recognizing environmental (community) and human factor (individuals) aspects. That makes it a challenging target for futures research.

Material and Methods

The analyses in this article are based on the material that was produced by means of a Delphi Survey in the dissertation mentioned above (Valtonen 2010). In the dissertation, the main goal was to determine conceptual definitions and to find out the success factors within an operational-tactical collaboration context. In addition to the Delphi survey, the process included a discussion of future trends and aspects. In this article, the material on future-oriented answers was re-evaluated more profoundly in order to reveal possibilities for futures research concerning the collaboration of security actors.

The Delphi Method could be described in short as a structured information gathering and evaluation process, enabling experts to express their opinions anonymously (Turoff 2002, Linturi 2007). The method is very popular in futures research and numerous variants of the method have been used in different surveys. In Valtonen's Delphi survey, 21 experts (panellists) from different security branches (10 from public administration, 6 from voluntary services and 5 from business) took part in the process. Their expertise was verified before the survey in several exercises and interviews. Besides their expertise, the orientation and interests of the panellists were also discussed. The inquiry revealed that both pragmatic and future-oriented thinking are represented in their opinions. The Delphi process as a whole also turned out to be a learning process for both the participants and the researcher.

The re-evaluated, future-oriented Delphi results were discussed with reference to some recent domestic and international articles and writings. Operational-tactical level (practice) futures research on security collaboration has not been performed, especially in Finnish contexts (Kuusisto 2010).

Results

The main goal of the referred constitutive collaboration research was to determine conceptual definitions and to find out the success factors within an operational collaboration context. The research results were based on the analysis of the Delphi survey and action research findings from several security exercises and projects. The results were analyzed separately and jointly by triangulation. The conclusions proved that successful collaboration is based on functional interagency collaboration supported by compact-sized operational environments. All relevant actors will be involved and increase value through collaboration if they fulfil the security-related requirements (such as trust and professionalism). The major pitfalls in collaboration were recognized in information exchange and common situational awareness.

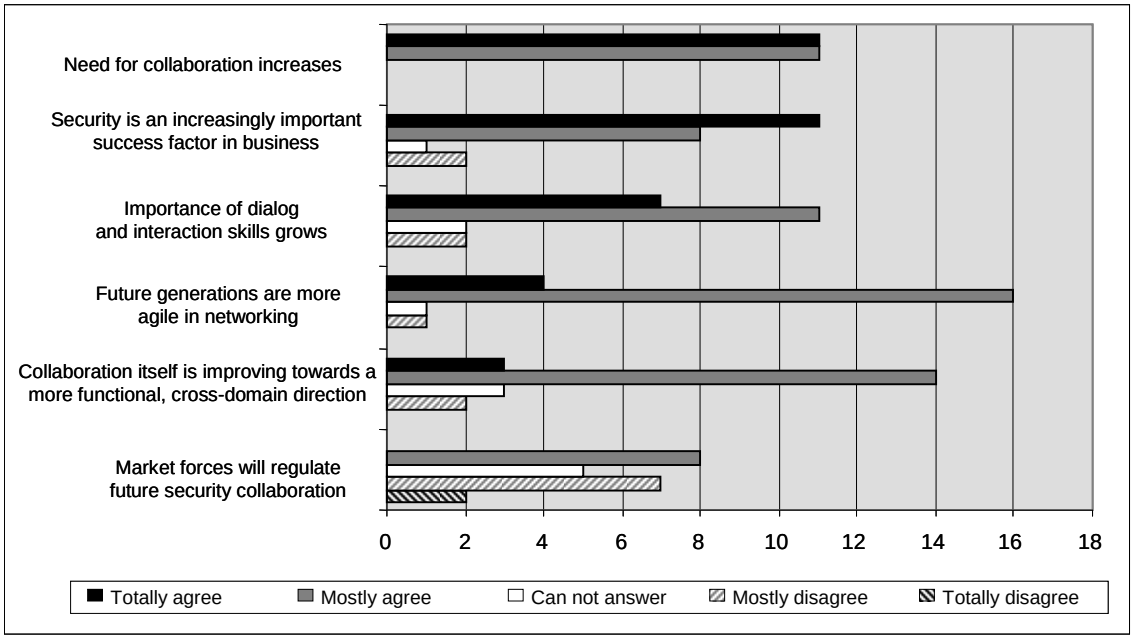
The Delphi survey was conducted in three iterative rounds. The future estimations were presented in the last round, so the only reflection was (in the sense of the Delphi technique) from the final call for comments on the analyzed results. In that phase, the panellists did not express any major disagreements

concerning the analysis. In summary, one can say that the futures estimation was conducted as a one-round Delphi survey.

The security experts' views on future development were quite moderate mainly because the actual study focused on the present. The mainstream viewpoint was that societal changes as a whole had the strongest influence on changes in security collaboration.

Six arguments reflecting future estimations were gathered from the first and second Delphi rounds. They are presented with the third-round estimations of their importance in Table 1.

Table 1. Estimations about Future Arguments.



The panellists mostly agreed with the presented arguments, yet there were many interpretations and reflections that may be seen as weak signals. The first arguments present mostly environmental aspects of possible futures. The panellists were most unanimous concerning the claim that *Need for collaboration increases*. They argued that the main causes are the evolving changes in the security environment and lack of resources. The second argument, *Security is an increasingly important success factor in business*, reflects the growing role played by the private sector in comprehensive security environments. On the other hand, it arises from a current phenomenon, as the agents have noticed that extensive security is required for profitable business. Some disagreements emphasized the difference in agencies and their environments – all business is not (at least not yet) security driven.

From the human factor point of view, the next arguments – *importance of dialog, interaction skills grows* and *future generations are more agile in networking* – were seen as a natural outcomes of human development and behaviour. The discussion dealt mostly with nuances of terms and their interpretations.

Although there was a degree of consensus on *Collaboration itself is improving towards a more functional, cross-domain direction*, only three experts were in full agreement. The panellists argued that cyclical development occurs over a longer time scale, which may be seen in forecasting as well. The pur-

pose of collaboration was also discussed in terms of whether the efficiency and quality of collaboration should be increased constantly or it is enough that it works.

The responses to the last argument, *Market forces will regulate future security collaboration*, were the most interesting from the researchers' perspective. The opinions of the panellists were scattered and the discussion raised the most interesting comments. Besides the terminological discussion, some weak signals were detected. The present world order – with its laws, order and authorities – was defended fervently. At the same time, the agile business world will shift its focus from quarterly performance towards ever-faster management, which has severe impacts for interagency and other security actor collaboration. The role of the authorities and both private and voluntary security actors will undergo changes in the future, yet the panellists considered that the traditional control of security by authorities will have significance. The private sector was seen as a growing actor in the comprehensive security area.

Additionally, the panellists were asked about their opinions on the most important trends in terms of comprehensive security. Their answers were quite moderately in line with the previous arguments. The main reason for this was the small role of the futures estimations in the whole Delphi process. Consequently, three trends were picked from the analysis of the Delphi results in the research report for this article. They were re-evaluated as follows:

Table 2. Trends from security actors' collaboration research and interpretations.

Rising Future Trends	What is it?	What produces it?
Need for collaboration rises	Complex systems and fewer actors have to collaborate	Joint services, authorities, processes, etc. (international)
Importance of security rises	Complex systems are vulnerable	Security attitude and culture develops
Individual influence rises	People may take part in security systems	Security knowledge increases, new innovation, thinking, etc.

The trends and their interpretations presented in Table 2 reflect the attitude and thinking of security actors. "What is it?" and "what produces it?" are quite optimistic and the light they shed is only one-sided. Those with a pragmatic mindset, which is quite common among security actors according to the research, would primarily view these trends as threats. The changes underlying the trends are due to increasing complexity (Rantapelkonen 2002, Keskinen 2004, Sivonen 2004). This raises the demand for collaboration and security when the systems are dependent on experts and specialists. The need for integrated services and changes in security thinking and attitudes reflects the present stage and development of the operational-tactical environment. Demographically people get older and fewer people live in a vast geographic area, which leads to a lack of security actors in large areas. The problem is that necessity-based integration proceeds slowly. The old administrative structures and other rudiments decrease the demand for flexible and more dynamic solutions. From the individual point of view, we may see positive development in participation in security discussions that may improve comprehensive security thinking. On the other hand, ill-minded people might have access to sensitive security information, and this must not be ruled out even in the most positive futures.

In the research, some weak signals were also discussed. They were summarized in two concepts: moulding of security attitudes and impacts of general securitization. Both of these are controversial phenomena and may have both negative and positive features. Security attitudes and efforts to ensure that everything is secure may once again result in an image of an Orwellian society, as the panellists stated. They might not be true weak signals, because some discussion has already taken place, mostly in blog writings (e.g. Virta 2008, Järvinen 2008). Beyond those presented, the re-evaluation of the Delphi answers revealed some other ideas that could be introduced as weak signals:

Hierarchy tends to steer thinking. For this reason, it is also important to separate different level phenomena in certain security issues. For the most part, the *learned truths* passed down from the top have a major influence on comprehending the real functions of systems. The political demand for generalizing security strategies may oversimplify practical level challenges within collaboration.

Trust is the key element for successful collaboration between security actors. It has two sides. Firstly, trust is the basis for mutual collaboration and sharing the most delicate security information. Secondly, the other element, which is here called the *hidden truth*, concerns the requirement of publishing research for public use. The most delicate, secret information may not be shared openly and therefore academic public research does not have the possibility to engage in scientific discussion on such issues.

Discussion and Conclusions

Futures security-related research has focused mostly on large-scale studies (strategic level environmental scanning). Global and continental security trends (e.g. DefMin 2007, Keskinen and Kuusisto 2007, Coker 2004) are also an important framework for operational-tactical level futures research, yet they tend to be quite general for small-scale (Robson 2005) futures studies. Technological forecasting (Kari et al. 2008a, 2008b) and mostly marginal security issues studies (e.g. Lintonen 2009, Rantapelkonen 2002) in one sense represent operational-tactical level futures research. Past futures research has yielded correct estimations in certain technological prognoses that have later proven to be guiding factors for even broader development (Haikara 1970, Toward the Year 2018, 1970). Nevertheless, the lack of comprehensive operational-tactical level futures studies is axiomatic.

It might be also relevant to raise the question whether level-based thinking is too limiting for futures studies. Does development progress through ever increasing levels, which may influence security integration? (Ahvenainen 2004) On the other hand, precision-targeted futures research might give some concrete ideas for system and process development. Along with collaboration integration level discussion, it is important to evaluate regional aspects that involve strongly cultural and environmental aspects (Nelson 2007).

The human factor is one crucial element for actual security collaboration. The development of collectiveness may be technologically driven. For example, network-based interaction develops rapidly. Networking may be seen to be quite random if the participants may act as anonymously, even as unpersons. This is not possible in collaboration between security actors. On the other hand, task-oriented security actors may develop unofficial networks, even with the opposite side, if the primary goal is achieved (Hyytiäinen 2010). Collectiveness may also result in the adoption of old-fashioned traditional processes that may be more robust when ultimate performance is required.

It is interesting that in the referred research the Delphi panellists were most unanimous about environmental and pedagogical development. Differences of opinion emerged when it was time to discuss competition for territories, finance, and power. Due to their focus on the present, the panellists favoured moderate and "sure" solutions. Futures thinking requires time and a certain attitude that liberates the person from present stage attitudes in order to seek future possibilities. That is why the presented one-round Delphi did not produce any such results that could be considered significant.

The research on security actors' collaboration at the operational-tactical level revealed fundamentals for successful collaboration and some ideas about the futures. The suggestions for futures studies in security actors' collaboration are presented in table 3.

Table 3. Suggestions for security actors' collaboration future studies.

Community	Individual
operational-tactical level environmental scanning – threat evaluation	individual scale scanning – threats in the sense of safety and security
future integration forms	meaning of networks and collaboration
SSM in collaboration and security	normative acting

Threats should not be excluded from any futures studies of security collaboration. They should be evaluated in terms of the community and from individual points of view. Both the terms and their meanings in the context of focusing on the common objects of futures study should be studied at the same time (Heinonen 2004). For example, safety and security matters ought to be specified, i.e. whether the focus is on tumbling on a slippery sidewalk or dealing with terrorists.

The common trend of integration in our societal scenarios is one important factor that should be evaluated at both the individual and community levels. Is integration creating new systems between security communities with their networks and active individuals?

Community-oriented future security collaboration issues are time and again facing discussion about who is the customer, actor, etc. One recommendable method for outlining the futures studies baselines is the Soft System Methodology (CATWOE, Rubin 2002; Checkland & Scholes 1999).

Comprehensive security collaboration in futures studies requires a cross-scientific approach to research. No expert can master all the methodologies of all disciplines (Nordlund 2004). Neither can we comprehend all the threats facing our systems and their interdependence. We tend to see collaboration as a tool for ongoing multidimensional challenges and engage in it only when it becomes unavoidable. Comprehensive futures study needs the participation of operational-tactical level experts who have a suitable knowledge on the matter. That may be understood as knowledge on threats, security processes, and practical possibilities without strong political orientation. Comprehensiveness means that systems work together and develop both independently and jointly towards the future we create for communities and individuals. At the operational-tactical level, a "good enough" approach might create a foundation for "secure enough".

References

Coker, Christopher (2004). *The Future of War. The Re-Enchantment of War in the Twenty-First Century*. Blackwell Publishing, Cornwall.

Elliot, Mark Alan (2007), *Stigmergic Collaboration. A Theoretical Framework for Mass Collaboration.* Dissertation. The Victorian College of Arts. The University of Melbourne.

Foreign Policy Association (1968). *Toward the Year 2018*. Translated into Finnish by Risto Varteva. (1970) Katse vuoteen 2020, Weilin+Göös, Tapiola.

Gordon, T., J. *The Delphi Method in Futures Research Methodology-V3.0. The Millennium Project* (eds. Glenn, J., C. and Gordon, T., J.). Available in http://www.millennium-project.org/millennium/FRM-V3.html (visited 26.10.2009)

Haikara, Kalevi, ed. (1970). *Suomi vuonna 2000*. Kustannusosakeyhtiö Otava, Helsinki.

Heinonen, Reijo E. (2004) *Mikä tulevaisuudessa takaa turvallisuutemme. Kohden kollektiivisen turvallisuuden käsitettä*. Futura 3/2004.

Himmelman, Arthur T. (1994), *Communities Working Collaboratively for a Change. Resolving Conflict: Strategies for Local Government*. Margaret Herrman, ed. Washington, D.C., International City/County Management Association, 1994, s. 27–47.

Himmelman, Arthur T. (2002), *Collaboration for change. Definitions, Decision-making Models, Roles and Collaboration Process Guide.*

http://depts.washington.edu/ccph/pdf_files/4achange.pdf (11.12.2009)

Hyytiäinen, Mika (2010). Personal interview, March 30th.

Järvinen, Petteri (2008). *Suomesta Euroopan turvallisin maa v. 2015 mennessä*. http://pjarvinen.blogspot.com/2008/05/suomesta-euroopan-turvallisin-maa-v.html (11.12.2009).

Kari, Mikko et al. (2008a). *Sotatekninen arvio ja ennuste 2025, Osa 1, Teknologian kehitys*. Edita Prima Oy. Helsinki. (Eng. Military technological estimation and forecast 2025, Part I, Technological development).

Kari, Mikko et al. (2008b). *Sotatekninen arvio ja ennuste 2025, Osa 2, Puolustusjärjestelmien kehitys*. Edita Prima Oy. Helsinki. (Eng. Military technological estimation and forecast 2025, Part II, Defence systems' development).

Keskinen, Auli (2004). *Kompleksisuudesta*. Futura 3/2004.

Keskinen Auli and Kuusisto, Rauno (2007). *Yhteiskunnallisten muutosten merkitys sodankäynnille - Globaalit skenaariot ja Suomen puolustusvoimien näkökulma 2030. Versio 2*. 28.3.2007. TLL IV Viranomaiskäyttö.

Kuusisto Rauno (2010). Personal interview, March 30th.

Lintonen, Tomi (2009). *Drugs 2020*. Ongoing Delphi study.

Linstone, Harold A. & Turoff, Murray, eds. (2002), *The Delphi Method. Techniques and Applications*. http://is.njit.edu/pubs/delphibook/index.html

Linturi, Hannu (2007). *Delfoin metamorfooseja*. Futura 1/2007.

Ministry of Defence (2007). *Predictions regarding international actors up to the year 2030*. Seminar 28th-28th Nov. 2007 in Helsinki.

Nelson, Ruben (2007). *Aligning (Alberta) with the 21st Century*. Futura 2/2007.

Nordlund, Göran (2004). *Ennustamisen vaikeudesta*. Futura 3/2004.

Rantapelkonen (2002). *Turvallisuus vuonna 2020*. Huhtinen, Aki-Mauri ed. (2002): Länsimaisen yhteiskunnan kriisinsietokyky 2020. Oy Edita Ab, Helsinki. (17-58).

Rekkedal, Nils Marius (2006). *Nykyaikainen sotataito*. Helsinki: Edita Prima Oy.

Robson, Colin (2001). *Käytännön toiminnan arviointi*. Tampere, Finland: Tammer-Paino Oy (English version: Small-Scale Evaluation. London: Sage Publications, 2000).

Rubin, Anita (2003). *Pehmeä systeemimetodologia tulevaisuudentutkimuksessa*. Kamppinen, Matti & Kuusi, Osmo & Söderlund, Sari (2003): Tulevaisuudentutkimus. Tammer-Paino Oy, Tampere, s. 171–203.

Sivonen, Hannu. *Tulevan ennakoiminen strategian tutkimuksen haasteena*. Futura 3/2004.

Valtonen, Vesa (2008). *Military Science and the Paradigm of Tactics: Exploring Finnish Inter-agency Cooperation*. Mutanen, Arto, ed. (2008): The Many Faces of Military Studies: A Search for Fundamental Questions. Edita Prima Oy, Helsinki.

Valtonen, Vesa (2010). *Turvallisuustoimijoiden yhteistyö operaatiotaidon ja taktiikan näkökulmasta*. (Dissertation, manuscript)

Virta, Sirpa (2008). *Turvallisuusutopia*. http://www.intermin.fi (12.2.2009)

THE FUTURE OF RESEARCH ON SAFETY AND SECURITY IN GERMANY - RESULTS FROM AN EXPLORATIVE DELPHI STUDY

Dr. Lars Gerhold
Freie Universität Berlin, Research Forum on Public Safety and Security

ABSTRACT - *This contribution presents the results of a qualitative, exploratively set up Delphi study. The achieved results supply an image of German research on safety and security from the perspective of all relevant disciplines as well as of its future challenges in the next 20 years. Based on developments relevant for safety and security and exemplary research topics, challenges are defined for the future of research on safety and security. In this context, this contribution will deal with the question of using different definitions of the term, alignment of research for different recipients and use of different research strategies and methods.*

Introduction and Background

Under the current conditions, safety and security as a personal value seems to be more endangered than ever. The effects and possible dangers of technological and natural developments can hardly be assessed, and terrorist attacks cannot be foreseen. To make safety and security possible never¬theless, research on safety and security has the task of finding and analysing vulnerabilities of society, and, in a best case scenario, to perform research for the protection of society (cf. Thoma, Drees & Leismann 2010, p.13[5]).

German research on safety and security is extremely heterogeneous and anchored in social sciences, humanities, technologies and natural sciences. At this point, only the beginnings of a comprehensive collection of different research lines and projects exist (cf. http://www.security researchmap.de). Nor does a summarising observation of current and future research questions exist. Inter- and transdisciplinary communication between the disciplinary approaches and actors only takes place rudimentarily (cf. Reichenbach et al. 2008). The research forum on public safety and security, founded in 2009 at the University Freie Universität Berlin, work on the challenge of combining interdisciplinary approaches from a scientific point of view by making the future of research on safety and security the object of research itself. The project therefore focuses on both aspects of the German term “Sicherheit”: security and safety. Safety means unintentional risks such as technical safety of a system like a nuclear power plant. Security means the protection of external threats like a terrorist attack (vgl. Beyerer et al. 2010, p.50).

[5] All citations were translated by the author.

The research project's task is examining developments of public safety and security from a scientific point of view and to offer a summarising evaluation, to synthesise the knowledge collected by interdisciplinary research under common questions, identifying research topics that will be relevant in future and contributing to structuring the field of research for answering these questions. The exploration study presented here was implemented to reach a first preliminary structure of the field of research on safety and security and its actors. It also serves as a basis for discussion for the starting workshop of the research project. The central questions of the study are:

- Which are the requirements, risks and dangers of the future from an interdisciplinary perspective of the security research in Germany (to the year 2030)?
- In which problem areas is there a special need for research and to whom is this need explicitly addressed?

Material and Methods

The qualitative exploration study represents the first methodical step of a long-term overall study. The aim is to develop the field of subjects from the point of view of German research on safety and security experts. The exploration study is accompanied by two other comprehensive studies. At the same time, scientists and politicians will answer questions on their assessment of the previous results in semi-structured expert interviews. Concurrently, a comprehensive Delphi study is to be performed. Its experts will include scientists from the area safety/security/uncertainty/risk as well as politicians as decision makers, police and rescue forces and a representative sample of the population as persons involved (cf. figure 1). In the end, all of the results are to be combined in a scenario process "Safety and security 2030".

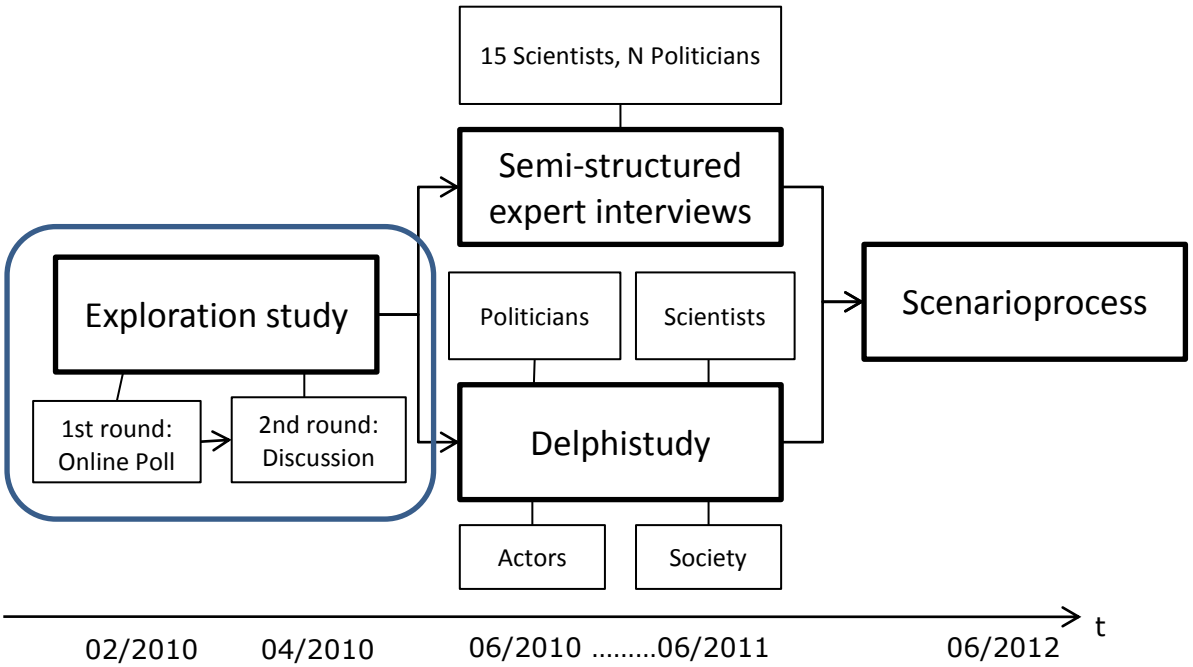


Figure 1. Overall Study Concept.

The study presented here is methodically structured as an open exploration. A conscious decision was made to not embed the study theoretically, e.g. in probabilistic or formal-analytic or social-constructivist theory concepts (cf. Gerhold 2009a, p.21 et seq., Taylor-Gooby & Zinn 2005, p.3 et seq.) to avoid narrowing the perspective of the observer.

The study is intended to be a two-round Delphi study[6] . The first round was a qualitative online survey, the second a group discussion during a workshop, in which participants from the online survey took part. The target of the first Delphi round was identifying future developments particularly important for research on safety and security in Germany. At the same time, the research topics that will be of interest during the next 20 years were to be determined. These two aspects formed the basis for the second round, in which the results from the first round were taken up again as basis for a discussion on the question of which implications this had for future German research on safety and security. According to the so-called classification type 1 of Häder (cf. 2009, p.36), the present study is a Delphi procedure for aggregation of ideas, characterised by open questions with the target of collecting ideas for the observation of problems. The criterion for success of the study according to the targets of aggregation of ideas is the number of ideas offered by the experts asked (cf. Häder 2009, p.31).

The experts asked should have as wide an expertise basis as possible. The experts selected are understood as function carriers and representatives of their organisational and institutional contexts rather than a person with subjective orientations and attitudes (cf. Meuser & Nagel 2002, p.72). Their technical expertise was verified when the participants were selected and confirmed later during the survey by way of self-assessment (so-called "subjective competence question", cf. Häder 2009, p.26). In total, 51 experts from the area of research on safety and security were invited to participate in the study; 27 experts from different disciplines of natural and social sciences, who perform research and work in the areas of safety and security, risk and danger, participated in the first round (response rate 53%)[7] . Participants were recruited based on their confirmation of participation in the starting workshop of the research forum on public safety and security, where the results of the first Delphi round were presented and discussed. Most of the persons asked were scientists (20 participants), 5 participants came from safety and security organisations, 2 participants are working for companies. All experts asked stated that their own competence in the area of (research on) safety and security was rather high or very high, and their average experience was 14.5 years. The experts' ages range from 30 to 69 years and the experts come from different disciplines (technology, natural sciences, law, social sciences, humanities, cultural sciences).

The results from the first Delphi round were introduced in a joint workshop with all persons participating in the survey and additional experts by way of an anonymised presentation of results. The discussion of the results regarding the research questions characterises the second round of the Delphi study with N=60. The experts' discussion was led, recorded and transcribed by the author.

---

[6] A Delphi study is a multi-stage process used for assessing future events and developments (cf. Cuhls 2009, p. 207et seq.; Häder 2009, p. 19et seq.).

[7] Since the study was a first exploration, it was not important to achieve a concrete number of participants (high N). For qualitative understanding, test persons are not selected according to criteria of statistical representativeness but according to whether or not they are suitable to expand knowledge of the object to be examined (cf. Glaser/Strauss 1967, p.45).

Analysis

The online survey data (1st round) and the group discussion (2nd round) were evaluated with the MAXQDA software in a structured content analysis according to Mayring (2000). Mayring personally describes the target of content structuring as "filtering certain topics, contents, aspects from the material and summarising them" (Mayring 2000, p.89).

After selection of the data material (all statements from the online survey and transcription of the group discussion), main categories where first determined deductively (see *Results*). In the course of the coding process[8] , the main categories were expanded inductively. Extraction of contents and assignment to categories from the text material is already an interpretative step characterised by the researcher (cf. Gläser & Laudel, p.201). The excerpts taken from the text are prepared, summarised and checked for redundancies and contradictions. This way, the text material is structured according to inductively developed categories: "The result of the analysis is a structured information basis summarising the empiric information on the cases to be reconstructed" (Gläser & Laudel, 2009, p.202). Main categories I and II are the main objects of the first round, main category III was subsumed from the two rounds (cf. *Results*).

Results

The analysis led to three main categories (cf. figure 2) to structure the data material. First, safety- and security-relevant developments from the points of view of the experts for the next 20 years were determined (I). The experts named different content-categories for future developments in different fields, such as health, society or technology. Based on this, examinations determined which research topics are going to become important in the next 20 years (II). The future developments were taken up to suggest exemplary research areas and topics such as technology development in the area of detection of hazardous substances or examination of self-help-capabilities of the population. The last area of results uses categories I and II as a starting point for debating the question of which factors will mainly characterise the future of German research on safety and security (III).

[8] Concretely, the coding process means that individual text sections, i.e. single sentences or whole paragraphs, are assigned to categories from the category system or new categories derived from the material (cf. Gerhold 2009a, p. 124). This procedure was described by Strauss und Corbin as "taking an observation, a sentence of a paragraph and assigning names to every single incident, any idea or any event included in it – for anything standing for a phenomenon or representing it" (Strauss & Corbin 1996, p. 45). According to this, codes or categories practically are pointers towards certain subjects in the text (cf. Kuckartz 2005, p. 64).

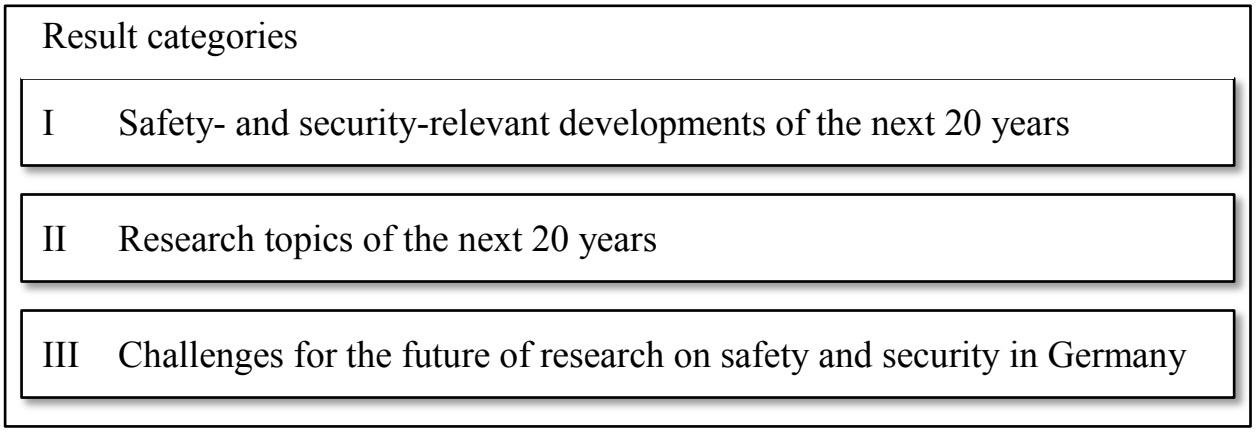


Figure 2. Categories of results of the exploration study.

I Identified Safety- and Security-Relevant Developments of the Next 20 Years

The category shows the safety- and security-relevant developments (i.P. of uncertainties, risks, threats, dangers, hazards) that will be important for the German research on safety and security over the next 20 years. This perspective is used to develop an orientation of the future that may present a range of possibilities for developments in the areas of society, political and environmental issues. However, this cannot be used to derive the probability of the described developments actually taking place or that the aspects named here all determine the future. Much rather, this is a section of the perspective of experts in research on safety and security[9] .

Figure 3 shows the presentation of results in a classified system of the answers of participants in the survey. The starting points for the categorical system are the themes for which contents are named; they are connected to each category as coded text excerpts. Therefore the classified system on the question of safety and security-relevant developments up to 2030 is based on the text material.

All in all, eight subject areas could be extracted from the data material; some were structured in subcategories again: 1.Governance/Politics/Globalisation, 2.Terrorism/Organised Crime, 3.Weather/Environmental Development, 4.Critical Infrastructures, 5.Health/Pandemic, 6.Economy, 7.Society and 8.Technology.

[9] However, it cannot be excluded that other safety- and security-relevant aspects that are not named here will determine future development. But according to the experts included in this study, it can still be assumed that the topics presented in the following will be of importance, even though these assessements require additional empiric and theoretic foundations.

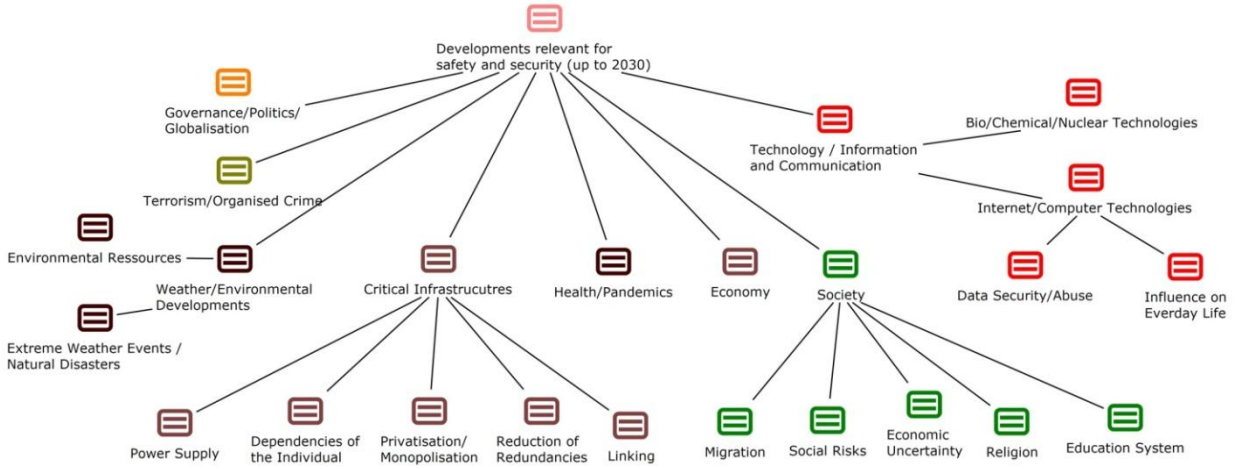


Figure 3. Systematic presentation of identified safety- and security-relevant developments over the next 20 years.

1. **Governance/Politics/Globalisation**

   The category of governance/politics/globalisation combines political processes such as risks that may result from globalisation processes, e.g. interlinking global developments, which, due to their growing complexity, may lead to political inability of act. This may lead nationally in alignment problems between the Federal republic and its states when dealing with major incidents or internationally in the coordination of procedures in crisis management. The data material also brought up the question of proportionality of national and European politics as a security-relevant topic of the future. Connected to this is the basic question of the state's ability to overcome future challenges.

2. **Terrorism/Organised Crime**

   The subject area of terrorism is mainly characterised by descriptions of the topic in the data material (e.g. terrorism in the sense of bombs, poison, etc.) and emphasis on connected effects, such as threats to national and international societies and their large cities. It was also mentioned that reaction to terrorist acts requires new strategies, e.g. regarding the treatment of injured persons or retention of resources to be deployed. Furthermore not only terrorism, but also organised crime is named as safety- and security-relevant for the next 20 years.

3. **Weather/Environmental Development**

   This category has two central aspects. On the one hand, climate change in general and its possible effects, e.g. on migration, biodiversity and agriculture, were named. The second important aspect is related to the first and refers to extreme weather events and natural disasters (such as floods, earthquakes). A participant in the survey expressly indicates the danger of different projections of local, national and international events. Risk assessments may turn out to be too "mild" and the events appearing as being more intense than expected. On the other hand, a period with few events is also possible, which would make political adjustment measures more difficult.

4. **Critical Infrastructures**

The vulnerability of critical infrastructures is another category of developments important for the future with many facets as determined by the experts. Among others, this includes questions of power supply as well as general dependency of every individual on critical infrastructures. Both are closely linked to interconnections resulting in a great impact of outages. Increased vulnerability is also seen in the reduction of supply redundancies, which also refers to monopolisation of certain infrastructures.

5. **Health/Pandemic**
   The category of health/pandemic combines pandemics and the connected health hazards, as well as food safety, as future safety- and security-relevant topics.
6. **Economy**
   The (global) development and the connected “non-universalisability" of the Western growth and wealth model is described by this category. Riots are named as a possible result of risky developments in the financial markets.
7. **Society**
   Social developments relevant for research on safety and security were particularly differentiated. First, some indications of the participants in the survey cover the area of migration; in the text material, this refers to possible aspects such as general conflicts, depopulated and uneducated zones, as well as accelerated mobility. Furthermore, religion is named as a potential conflict without any more differentiated information being given. The participants in the survey also assign education as a facet of social development both to the question of safety and children’s rights in education systems, as well as to the change of the traditional educational institutions by learning based on communication technologies. The subcategory of economic insecurity mainly focuses on distribution conflicts, precarious economic situations and the widening gap between poor and rich, as well as possible consequences such as riots. The aspect of social risks includes a wide range of problems. Social processes such as social exclusion and progressing individualisation, loss of trust and a lack of perspective in the population, changes in identity formation processes, erosion of social security systems and the importance of subjective perception processes are named as safety- and security-relevant topics for the future.
8. **Technology**
   The subject field technology is divided into two central areas. On the one hand, dangers resulting from developments in the areas of biologic, chemistry and nuclear technologies (including, e.g. the consequences of genetic engineering) are named. On the other hand, internet and communications technologies and computer technologies are dealt with. The second aspect refers to the increasing penetration of different areas of life by information and communications technologies and the connected questions of data security, espionage (e.g. movement and consumer profiles) and sabotage as future topics.

All in all, developments relevant for research on safety and security (and therefore for society, politics and economy) are to be expected in different subject areas during the next 20 years. Focusing on singular subjects in scientific research or the political debate therefore does not seem suitable, in particular since many different cross-links – which are not examined or presented here – may exist between the subjects. At the same time, many “typical” or “expected” subjects are named, which also can be found

in the area of scientific (cf. e.g. Lange, Ohly, Reichertz 2009; Gerhold 2009b) as well as political (cf. Reichenbach et al. 2008) and social discourse (cf. R+V 2007). This includes terrorism and organised crime, climate and environmental development, technology and health issues. This may be considered proof that consulted experts agree with and confirm the socially, politically and scientifically discussed subject areas. Apart from this, however, social questions also make it possible to find "newer" differentiations, which were previously given little consideration in the debate of safety and security. These include topics such as social exclusion, lack of perspectives, subjective fiction of safety and security or education system issues. While these are also dealt with and discussed by science, they are, however, not always included in the area of research on safety and security.

II Important Research Topics during the next 20 Years

After dealing with the issue of future developments, the question of which research subjects and fields would result for research on safety and security during the next 20 years from the developments named was analysed. The indicated research subjects mainly were found in the subject areas of the first question, but also added by the subject of risk/crisis management/ communication.

In the scope of this contribution, only some thinkable research topics can be named as examples: Regarding the aspect of governance and politics, possible future research topics that were named include, for example, flexibility of the political security architecture in case of spontaneous incidents and threats situations, and a better linking of safety- and security-relevant facilities. For the subject field of technology, research subjects e.g. in the areas of detection of hazardous substances or consequences of comprehensive networking of information and communications technologies are focussed on. In the area of critical infrastructures, ideas are phrased that focus on securing and warranting the function of critical infrastructures (prevention, downtime precautions, logistics, actors), e.g. using research for ensuring power supply or development research on evacuation plans in traffic networks. In the area of environmental research, suggestions are made for the examination of extreme weather events; in the area of biology, the expansion of research on epidemics and other biological threats were named. In particular regarding the subject area of "society", the data material gives a lot of research subjects. The starting point is a general vote for prioritising social-scientific research in the context of safety and security research, e.g. using topics such as social developments, economisation and security of society. Here, the data material includes the question of development and creation of a culture of risk and security in a society. The question of self-help capability and -willingness is also asked and ways for facilitating this to turn the population into an "actor" in cases of crisis or disaster are considered. Other ideas are targeted on research on subjective wishes and ideal conceptions on the safety and security of the population.

In addition to the previous topics, the data material also indicates that the research area of risk and crisis management (including the connected communications processes) as a transectional theme has to accompany and/or complement the research projects.

Until now, the survey's results show a very heterogeneous image of possible research topics (category II). Together with the listing of developments that will be relevant in future (category I), the question of what this heterogeneity of requirements of future developments and possible research subjects means for the future of research on safety and security in Germany must be addressed now. How does research

on safety and security have to be positioned to comply with the general developments while also effectively dealing with the named research subjects?

III Challenges for the Future of Research on Safety and Security in Germany

The above presented results were discussed with the experts in a workshop event. Including the data from the online survey, the content analysis of the discourse returned four aspects particularly relevant for future research on safety and security in its conceptual alignment:

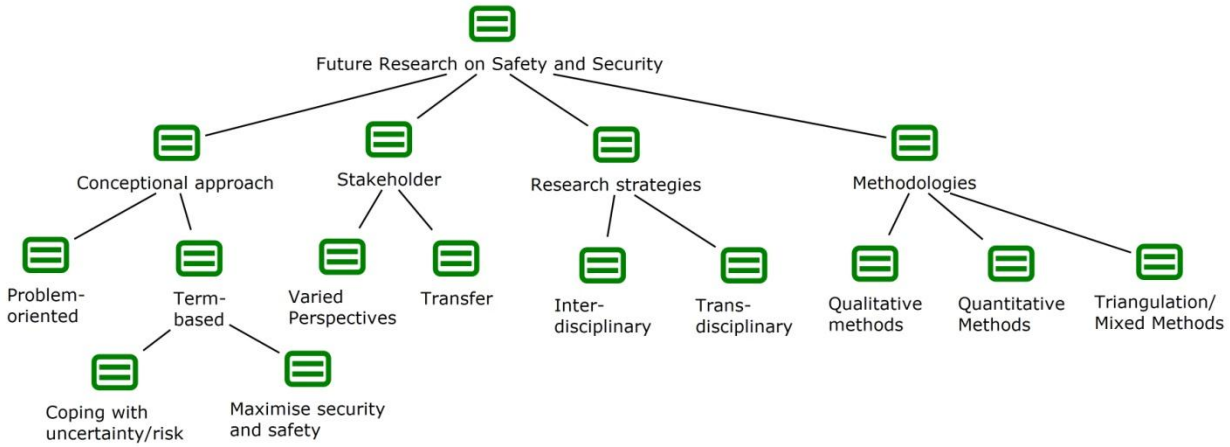


Figure 4. Challenges of Future Research on Safety and Security in Germany.

1. **Conceptual Approach**

   The "conceptual approach" category brings out two different approaches for research on safety and security. Firstly, the experts suggested a problem-oriented approach for future research. It is aligned with concrete vital problem situations relevant for public safety and security. The starting point for research would, in this case, be an explicit object or theme, such as protecting critical infrastructures. However, this approach presents a hierarchy problem. Which questions are particularly urgent, on which things can the different actors in science and politics agree?

   The second conceptual approach is looking for a more epistemological approach in which the terms relating to security are to be determined first. The differences of terminology conceptions of the term "security" must be taken up and discussed comprehensively. Regarding this, experts speak of a subject range of security as "coping with uncertainty and risk" on the one hand and security as "maximising security and safety" on the other hand. The first understanding refers to the conceptualisation of security as a "wicked problem". Where security is understood as a wicked problem (cf. Conklin 2005, p.7f.), it is understood to be indefinable, complex, linked and non-linear, so that the problem is impossible or, in the very least, highly difficult to solve. This understanding is along the lines of the social-scientific approaches (cf. e.g. Bechmann 1993, Bonß 1995) of not seeing security as the single target dimension, but rather as learning to deal with unavoidable, indefinable or unpredictable uncertainties. Furthermore, different references in the data material emphasise the subjectivity of perspective that, e.g., security and uncertainty are social constructs and security means a subject's ability to act even in spite of danger and threats.

This confirms that research on safety and security must also to be understood as research on uncertainty, which in turn is a special challenge for the interdisciplinary exchange between researchers.

The second understanding refers to security as an order problem (cf. Bonß 1996, p.169f.). This understanding defines clear criteria that can be determined and would enable, e.g., quantifying the problem areas. In this understanding the presence of security is understood in the sense of "objective" absence of risks and danger (cf. e.g. Grünbuch 2008; Thoma, Drees & Leismann 2010). According to this, technological, political and social developments follow after the paradigm of establishing security. This also includes the concept of "protection". The protection aspect can be inherent to the preceding understanding of absence of danger, but this is no prerequisite, since the absence of risk and danger does not have to be due to protective mechanisms.

Both understandings are not mutually exclusive, but lead to different manners of thinking and action both from a political and a research point of view; therefore, they need to be discussed before performing studies or funding schemes.

2. **Stakeholders**

   The category of stakeholder poses a challenge for research on safety and security regarding addressees, users and actors. Future research on safety and security must be aware of the different perspectives of political and social actors, know them and use them in research if research is to be accepted by these actors. This is aligned with the wish of designing knowledge transfer according to these groups and to work out knowledge accordingly. Therefore, the actual complexity may have to be reduced to make it possible to communicate research results.

3. **Research Strategies**

   The text material repeatedly describes holistic strategies such as interdisciplinary and transdisciplinary strategies as an idealised form of research. Interdisciplinary research is, e.g. illustrated in the combination of research in natural science, social science and law or the combination of social sciences and technology research strategies. Transdisciplinary approaches may be pursued via cooperation of public and private actors in the area of safety and security (regional, national, international). In general, the content suggestions show that the different disciplinary approaches do, in fact, overlap, but that the overlapping is too few to cover the future needs.

4. **Methodologies**

   In addition to general research strategies, the data material clearly shows that future research on safety and security must make use of a comprehensive range of methods. Apart from the rather quantitative methods such as modelling, morphology and prognostics, qualitative procedures such as group discussions and projection methods are named. A combination of methods or theories seems to be particularly important here (cf. Flick 1999). A possible model for exemplary implementation would be principally combining technically-oriented research with accom¬panying social-science research.

Discussion and Conclusions

In the light of the categories discussed here, the perspective of the experts in this survey comes to the following image for the future of German research on safety and security:

Safety- and security-relevant developments are to be expected in many different political, social and economic areas. However, they cannot be determined in advance in a way that we could tell now which subject areas, such as terrorism, technological developments, pandemics or social risks, will be particularly most important in future. Therefore, there is no singular important safety and security topic of the future. Research on safety and security is extremely heterogeneous and will continue to draw on the whole range of disciplines of science and to be implemented in different research topics. This also means that there cannot be one homogenous research strategy on safety and security. This is combined with the fact that research on safety and security needs to open up to a terminology discourse that will be able to productively link and expand the difference between the perspectives of "research on safety and security" in the sense of absence of danger and in the sense of coping with uncertainty. Research on safety and security also needs to be designed as research on uncertainty.

Future research on safety and security also needs to be intensely inter- and transdisciplinary to meet the requirements of complex problem situations. For this, all actors need to be linked and included in research. Social questions in particular will gain importance in future, e.g. in exchange with technical questions, and need to be dealt with under consideration of the respective methods or method combinations.

The insights of this exploration study can only serve to phrase the conceptual framework for future research on safety and security in Germany. It also does not yet include the scientific dialogue regarding research on safety and security that takes place within the disciplines. Nevertheless, it draws an image of the requirements of current and future research on safety and security as it was phrased by the experts themselves. This image is the starting point for other, concrete questions that are to be discussed in further studies:

Which conditions need to be met for successfully combining different disciplinary approaches for the research on safety and security and how can the disciplines learn from each other? How does an exchange between politics, science, economy and society have to be organised for targeted and successful results? How does the different understanding of terms influence the scientific discourse and the discourse between science, politics and public? Which methods and which combinations of methods will lead to the target in which contexts and for which research questions?

References

Bechmann, G. (Eds.). (1993): *Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung*. Opladen: Westdeutscher Verlag.

Beyerer, J.; Geisler, G.; Dahlem, A., Winzer, P. (2009): Sicherheit: Systemanalyse und –design. In: Winzer, P.; Schnieder, E.; Bach, F.-H.. Sicherheitsforschung – Chancen und Perspektiven. Berlin: Springer/Acatech, p.39-72.

Bonß, W. (1995). *Vom Risiko: Unsicherheit und Ungewissheit in der Moderne*. Hamburg: Hamburger Edition.

Bonß, W. (1996). Die Rückkehr der Unsicherheit. Zur gesellschaftstheoretischen Bedeutung des Risikobegriffs. In: Banse, G. (Ed.), *Risikoforschung zwischen Disziplinarität und Inter-disziplinarität. Von der Illusion der Sicherheit zum Umgang mit Unsicherheit*, p.165-184. Berlin: edition sigma.

Bundesministerium für Bildung und Forschung (2007): *Forschung für die zivile Sicherheit. Programm der Bundesregierung*. Berlin: BMBF.

Conklin, J. (2005). *Dialogue Mapping: Building Shared Understanding for Wicked Problems*. Wiley: Chichester.

Cuhls, K. (2009): Delphi-Befragungen in der Zukunftsforschung. In: Popp, R.; Schüll, E. (Eds.): *Zukunftsforschung und Zukunftsgestaltung. Beiträge aus Wissenschaft und Praxis,* p.207-222. Springer: Berlin.

Flick, U. (2004). *Triangulation*. Wiesbaden: VS Verlag.

Gerhold, L. (2009a): *Umgang mit makrosozialer Unsicherheit. Zur individuellen Wahrnehmung und Bewertung gesellschaftlich-politischer Phänomene*. Lengerich: Pabst Science Publisher.

Gerhold, L. (2009b): Für eine Subjektorientierung in der Zukunftsforschung. In: Popp, R; Schüll, E. (Eds.): *Zukunftsforschung und Zukunftsgestaltung: Beiträge aus Wissenschaft und Praxis*, p.235-244. Berlin: Springer.

Glaser, B. G.; Strauss, A. L. (1967): *The discovery of grounded theory: Strategies for qualitative research*. Chicago: Aldine.

Gläser, J.; Laudel, G. (2009): *Experteninterviews und qualitative Inhaltsanalyse*. 3. Auflage. Wiesbaden: VS.

Häder, M. (2009): *Delphi-Befragungen. Ein Arbeitsbuch*. 2. Auflage. Wiesbaden: VS-Verlag.

Kosow, H.; Gaßner, R. (2008): *Methoden der Zukunfts- und Szenarioanalyse. Überblick, Bewertung und Auswahlkriterien*. WerkstattBericht Nr. 103. Berlin: IZT - Institut für Zukunftsstudien und Technologiebewertung.

Kuckartz, U. (2005): *Einführung in die computergestützte Analyse qualitativer Daten*. Wiesbaden: VS Verlag.

Lange, H.-J.; Ohly, H.p.; Reichertz, J. (2009): *Auf der Suche nach neuer Sicherheit. Fakten, Theorien und Folgen*. 2. Auflage. Wiesbaden: VS-Verlag.

Mayring, P. (2000): *Qualitative Inhaltsanalyse. Grundlagen und Techniken* (7. Auflage). Weinheim: Beltz DSV.

Meuser, M.; Nagel, U. (2002): ExpertInneninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion. In: Bogner, A.; Littig, B.; Menz, W. (Eds.). *Das Experteninterview. Theorie, Methode, Anwendung*. Opladen: Leske und Budrich, p.71-93.

R+V Versicherung (2007): *Studie: Die Ängste der Deutschen 2007: Angst vor Terrorismus steigt spürbar an*. Infocenter der R+V Versicherung. Verfügbar unter: http://www.ruv.de/de/-presse/download/pdf/aengste_der_deutschen_2007/20070906_aengste2007_terror.pdf. retrieved 10.02.2008.

Reichenbach, G.; Göbel, R.; Wolff, H.; von Neuforn, S. (Eds.) (2008): *Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland. Szenarien und Leitfragen*. Berlin: ProPress.

Strauss, A. & Corbin, J. (1996): *Grounded Theory: Grundlagen qualitativer Forschung*. Weinheim: PVU.

Taylor-Gooby, P.; Zinn, J. (2005): *Social contexts and responses to risk network (SCARR). Current Directions in Risk Research: Reinvigorating the Social?* Working Paper 2005/8 Verfügbar unter: http://www.britsoc.co.uk/user_doc/05BSAConfTaylorGoobyPeter.pdf retrieved 01.11.2006.

Thoma, K.; Drees, B.; Leismann, T. (2010): Zukunftstechnologien in der Sicherheitsforschung. In: Winzer, P.; Schnieder, E.; Bach, F.-H.. *Sicherheitsforschung – Chancen und Perspektiven*. Berlin: Springer/Acatech, p.13-38.

2. TECHNOLOGY AND ICT

STRAW PROJECT: A EUROPEAN TECHNOLOGY ACTIVE WATCH ON SECURITY TECHNOLOGIES

Aljosa Pasic[a], Raimondo Iemma[b] & Christian Blobner[c]& Elsa Prieto[d]
[a] Atos Origin SAE, Atos Research & Innovation
[b] Fondazione Rosselli
[c] Fraunhofer, Institute for Factory Operation and Automation
[c] Atos Origin SAE, Atos Research & Innovation

ABSTRACT *– The project STRAW (Security Technology Active Watch) believes one of the greatest challenges of the Security environment will be the need for detecting, accessing and controlling relevant information (especially threats and possible countermeasures). Therefore it proposes a proof-of-concept of a European Technology Watch based on the active participation of the security community and the usage of semantic and Web2.0 tools.*

Introduction and Background

Most definitions of Technology Watch describe it as a set of activities or processes to systematically capture, analyze, disseminate and exploit useful technical information. Active Technology Watch (ATW) is incorporating a number of mechanisms (automation, dynamicity) in these activities, both on collection and on delivery side, in order to make scientific or technical innovation susceptible to emerging and future opportunities or threats and to detect, at an early stage, and prospectively shape, scientific or technological breakthroughs.

It is however closely related to trends and events of potential socio-economic importance, which may require action at decision-making level and in this sense it is sometimes confused with similar actions and processes such as Competitive Intelligence, Commercial Watch, Competition Watch, Surrounding Watch or Technology Foresight. However, although there might be some overlapping, there are many differences between them: for example, ATW focuses on the search and capturing of relevant information to make decisions, while Competitive Intelligence has also emphasis on creating new information.

The area of Technology Foresight and its methodology and mechanisms are also rather different: they focus on the projection of plausible prospective evolution of technologies or even technology markets in a short, medium or long term future. The target group is another differentiating factor: future visions are mainly used as support for identifying strategic research directions and therefore targets strategic decision makers, while ATW offers an important complement to these studies and targets more tactical and operational decision-making levels.

Active, yet Trustworthy

Everybody would agree that we can hardly trust a single vendor when s/he speaks about her/his magnificent products. But can we trust industry analyst or online search engines to deliver only fair and objective results for ATW? Since they update their results and reports frequently it seems like a good source of fresh information to feed ATW. Sometimes we take it for granted that they offer unbiased information, although we know there is an issue of paid placement or advertising links that appear in most search results these days and most industry analyst reports.

Another source of information for Active Research Watch is expert's opinion. The larger a group of uncorrelated expert from different communities is, the more unbiased the information theoretically will it be. However, it is both more complex and more costly to implement, especially when it comes to cross-country expert communities and information collection. Automated questionnaire processing certainly helps, but there are various problems, such as expertise limitations, that can lead to complete disagreement when it comes to information inclusion in ATW. In the story of the blind men and an elephant that originated in India, a group of blind men touch an elephant to learn what it is like. Each one touches a different part, but only one part, such as the side or the leg. They then compare notes on what they felt, and learn they are in complete disagreement. In a similar way, different communities or groups of experts may view same technology differently depending upon their perspective, suggesting that we often have to deal with half-truths.

Our experience with Lookout service in Atos Origin (Atos Origin 2010) shows that end-users have often more divergent and nuanced views than the analysts. However, an aggregate of perceptions in different communities (user, provider, consultants, research…) is very interesting. ATW within a particular cross-cutting segment of several markets such as security is particularly difficult. There are several attempts to design new analyst business models (Information Week 2006) based on blogs, open source licensing concepts, loosely federated analysts, social networking etc, but this does not eliminate the possibility of relationship or correlation between analysts, vendors and information providers, such as in the case of paid bloggers. Other open questions, both for ATW and analysts are including balance between qualitative vs. quantitative information research, survey transparency, technology expertise versus geographical coverage, etc

Even though it is not new, an additional point that is gaining strength is the dual use of technology. This concept refers to tools or techniques, developed originally for military or related purposes, which are capable of civil application. In spite of the inevitable controversy about the real motivation for this technology transfer, it is also true that the benefits can be countless. Therefore an ATW can help identifying synergies and establishing suitable communication channels between both fields.

STRAW (Security Active Technology Watch) is a coordination and support action project funded under the Security Research theme (FP7-SEC-2007-7.0-01 "Technology Watch") that aims at providing a European Service of Technology Watch on Security Technologies. Potentially, it will serve various communities from European end users to technology providers and system integrators. Although it can be used to alert European companies to possible emerging threats from disruptive technologies, STRAW sustainability will be driven, but also constrained, by a number of specific factors that are covered in this paper. Before we focus on these drivers and constraints, we will briefly present STRAW technology watch phases and main achievements.

Material and Methods

Information Gathering

The Information Gathering tasks represents the first step of the STRAW activity. Roughly speaking, it comprised the following actions:

1. the exploration of the Security concept and its associated elements;
2. the review of the existing taxonomies and classifications of the Security domain, including:
   a. the 2006 European Security Research Advisory Board report (ESRAB 2006);
   b. the European Security Research and Innovation Forum working group structure (ESRIF 2010);
   c. the STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities (STACCATO) taxonomy (ASD-Project STACCATO 2006);
   d. the U.S. National Strategy Homeland Security (White House 2010)
3. the adoption of a taxonomy of Security missions for STRAW (Project STRAW 2008)

The mission capabilities to include in STRAW were identified as a subset of the STACCATO taxonomy. The selection of missions reflected the interest and expertise of partner organisations and the professional profiles of the STRAW experts' panel members. The main rational of this choice was based on the fact that the STACCATO taxonomy provides a classification of the whole Security field, a detailed and up-to-date classification of missions and technology, being sufficiently extendable and flexible to allow for future changes in the Security areas. As well, the challenge in this phase is the compromise between an in-depth analysis of each mission and a broad coverage of the multi-faceted Security outlook.

Generally speaking, in information gathering phase, STRAW is combining "hard" methods such as literature study etc, with "soft" methods, such as interviews, expert panels, questionnaires, workshops etc. The outcome is a broad input of varying precision and bias.

STRAW also adopted STACCATO recommendations for a Technology Watch at European level (ASD-Project STACCATO 2006) in terms of:

- heterogeneity of the stakeholders involved (per category, country, Security field);
- maximisation of the participation;
- built on existing networks.
- product life cycle assessment;
- technological progress and maturity monitoring;
- threats assessment;
- interaction between Users and the other Security players;
- evaluation of the matching of the Security priorities identified by three categories of Security players: academia, industry (technology providers) and end users (including administration and also public at general);

The information collection activity represents the “front end” of the project. The involvement of Security actors in STRAW can be affected by several barriers, mainly related with the strategic importance of information (especially when related with underpinning technologies and new products), whose disclosure and sharing is likely to be critical. The effort produced by STRAW was therefore aimed at creating an attractive and easily joinable environment to bring together the different security groups and communities and to promote their participation. It is worth to mention that STRAW does not aspire at creating another security community, but recognizes the need for a model of one security community driven by high endorsement. In this sense, STRAW is a tool that allows the exchange of information and contributes to strengthen the security network in general.

In virtue of their permanent nature, both the tangible (automated online interface) and intangible (theoretical framework) assets are probably to be considered as the main achievements of the information gathering process. Together with the “back end” tools designed in the framework of the other tasks, those assets are meant to sustain the STRAW extent even beyond its temporal boundaries.

Knowledge discovery and representation

The objective of this second phase is to update a structured representation of the security concepts underlying the contents of the large and very rapidly increasing set of documents that represent knowledge in the technical domains related to security research. The purpose of the representation, in the form of taxonomy and ontology, is to be able to use natural language processing tools to perform computer-aided identification and classification of existing documents concerned with security research.

Significantly different terminologies were developed by different communities to describe the same aspects of security research. The terminologies became entrenched through usage at annual conferences, in books, journals, research reports, standards, industrial handbooks and manuals, patents, etc. In many cases the definitions themselves have multiple versions that depend on a given author’s preference.

The use of several synonyms or near-synonyms that lack well-defined distinctions is a source of continuing confusion that leads to re-inventions and plagiarism, impairs the transfer of research results to practical use and blocks the recognition of related documents. The current security research in Europe requires that past and current work as well as new technology have to be classified on the basis of a single ontology and thus made accessible to the technology watch processes such as analysis or packaging.

Today the purely manual process of ontology building for security research concepts is reaching its limits. The complementary solution is to augment the human effort by the use of automatic natural language processing tools that have been developed by computer linguists. Therefore STRAW considered computer-aided building of consensus ontology. Much progress has been made in the development of computer tools for human language processing. Such tools have been developed for the extraction of term candidates from a corpus (set of texts). A thesaurus (list of important terms with related terms for each entry) is constructed from the candidates. The ontology for a given domain is a data model that represents those terms and their relationships. Automatic indexation of the texts is carried out using the thesaurus, followed by clustering analysis using statistical and linguistic techniques. A measure of similarity between texts is computed that serves as a basis for automatic classification.

Taxonomy mix

Terminology extraction (TE) plays an important role in building lexical resources and is currently applied widely in many fields. There are several approaches for terminology extraction: linguistic, statistic and hybrid (Pennacchiotti 2005). Terminology extraction systems based on linguistic approaches have a higher than 70% coverage in term extraction. Statistical term extraction approaches, when given a big annotated training corpus, can perform almost as well.

The streams of documents from a variety of sources are pre-processed filtering information based on its level of interest according to criteria to be defined at the start of the task.

Once filtered, the information is processed to:

- Index and classify all documents and relevant information,
- Extract pertinent concepts and
- Arrange this information in a document base.

In STRAW the information is processed by a structured repository (Taxonomy Mix Output) combining classification nomenclature, classification criteria and extracted concepts according to the three defined categories of Security stakeholders (academia, industry and administration).This configuration is constructed taking into account the final use of the information, expressed by use cases of end users of the application.

Different indices and labels link documents and stored information to an operational repository, thus enabling experts to access information (based on nomenclature classification and knowledge base concepts). The documentary base will contain every document acquired from external site. All documents and information from every source will be processed automatically for abstraction, indexing, categorization and extraction.

Ultimately STRAW administrators will be able to employ various analysis tools for work on documents or structured data. They will be able to expand the operational knowledge base by adding either new concepts or new documents. A nomenclature tree has been defined for classification according to headings and for use by any automatic categorization function. Classification is representative of a theme or a concept.

The nomenclature classification structure is independent of the structure of the knowledge base, thus making it possible to adapt nomenclature to specific groups of user (user targeting or information packaging) and their needs.

Depending on the relevance of terms with respect to the security research domain we discovered several different levels of granularity. Leaf mapping, for example, means to map single terms to single concept in the ontology. This can be considered as a one-to-one mapping. In addition we identified the following kinds of mappings: manually introduced synonyms, ontology enrichment etc

Ontology structuring

Two steps are composing the Ontology structuring:

1. Ontology structuring (classes & subclasses definition): it defines the first elements of the Ontology: classes and subclasses.

2. Ontology structuring (named relations definition/directions/inferences): it defines relations among classes and subclasses. The pertinence of the map is validated by trying to answer the use cases following the structure of the ontology that has been defined.

In the example: "What issues and needs are most relevant for the administration in a given security area?", we need to check that there are direct relations between "users" and "Security area"; "Issues and needs" and "Security area" and finally between "Users" and "Issues and needs".

Settlement of the ontology

Once the structure of the ontology is set, it is possible to settle or fill the ontology with an integrated development environment (IDE) editor.

The additional settlement of the ontology is based on three sources of information:

- End users/research stakeholders/technology providers questionnaires. This is so far the main input to the STRAW system. Defined in the framework of the Information Collection activity, questionnaires try to combine a bottom-up approach (from technologies to security areas) with a top-down approach (from needs to technologies) according to the perspectives of the three categories of participants: academia, providers and end users.
  A top-down approach in STRAW is essentially breaking down EU security research priorities, capabilities etc. to gain insight into concepts, technology readiness levels and other issues. In a top-down approach an overview of the mission or capability is first formulated, specifying but not detailing any sublevels, which is usually done in sequence. A bottom-up approach in STRAW is bringing together researchers opinion about trends, sources, gaps etc to enhance initial assumptions.
- Outcomes of a crawling process in a subset of ICT-related security webpages. As a proof-of-concept, the goal of this task was to prove its feasibility. Therefore a limited scope was covered.
- State of the art documents submitted by experts.

It is important to notice that while in project SeNTRE (Foundation pour la recherché stratégique) a Mission and Scenario Analysis is consisting of an Initial Mission Analysis, Definition, Taxonomy and Standards and a Final Mission Analysis, the STACCATO final report (ASD-Project STACCATO 2006) proposes a methodology for European Technology Watch (ETW) aiming at both helping clarify the European Security Industry Structure, and identifying market growth potentials and deficient industry factor. This was also taken into account in the ontology settlement. Furthermore, the ontology settlement reflects the selected mission capabilities mentioned in the former chapter as means to outline the focus area of the technology watch for each mission. It is the project's belief that the inclusion of these criteria will improve the strength of the technology watch and consequently its impact.

Processing and packaging

The processing tools characterize and index information that can be extracted with a search engine. With these two components, a packaging process extracts information, pre-segments and customizes it for

each segment. Organizing ATW outputs is not a trivial task. With the increasing number of documents, it is becoming crucial to automate processes such as packaging and delivery of specific document to specific target groups. Clustering is a solution for organizing large amount of documents and it represents a quick way to acquire relevant document sets. For a particular document, search results would be documents from the same cluster that the given document belongs to.

A major delivery of the project will be the concept development for a Web2.0 (Wikipedia 2010) based information repository and online network for the security community. For this the STRAW consortium consciously follows the community approach, as laid out by the various Web2.0 applications that emerged in the last couple of years.

STRAW will develop a prototype external information repository based on the ever more popular Wiki technology (MediaWiki 2010), enabling community actors, such as researchers, technology providers and users of security technology, to actively come together and share information. The external information repository will be STRAW's major interface for the external stakeholders and the STRAW community to interact with the consortium and among each other.

The main objective for the external information repository will be the efficient and effective provision of information on security technologies. The wiki's advantage is the possibility of a continuous updating of information by users, so that ideally, the information displayed is always up-to-date. An active community, however, is the most important prerequisite for this advantage to manifest. STRAW will contribute to the foundation of a constant exchange between the security environment actors by pointing out major principles, which have to be considered in this very special environment. The project's concept for an active community will contribute to an increased interlinking of individual actors, an increased exchange of information and a more efficient allocation of resources.

Results

The result of the previous activity is a proof of concept of an active technology tool to monitor what is relevant in the Security domain in terms of knowledge, experience and stakeholders, and to deliver this information to the right audience at the right time. This is supported by a search engine and an own wiki (STRAWiki) that are available online at the project webpage (http://www.straw-project.eu/). This tool not only eases the information exchange, but also promotes the involvement of the different Security communities. In fact it is the Security community (or communities) who can make this solution active by taking up the STRAW results.

Discussion and Conclusions

Possible future directions

Although the sustainability of STRAW service is guaranteed at the moment (Project STRAW 2010), we envisage that STRAW has to continuously evolve and expand. In this chapter we briefly mention two ideas for the future work.

- *Technology Watch and Disruptive*. InnovationTechnology innovations can be thought either as evolutionary or as revolutionary. Evolutionary innovation is critical to sustaining and enhancing shares of mainstream security markets, and focuses on improving existing products and services to meet ever more demanding customer requirements. Because evolutionary innovations maintain the existing and mainstream markets and improve the performance of products and services in directions that customer's desire, the uncertainty is relatively low. Technology Watch of revolutionary innovation is much more difficult, as it is often not easy to identify. The term 'disruptive innovation' has been used to describe innovation that is of highly revolutionary or discontinuous nature, in which customers are provided with products or services which were not available to them before. A disruptive innovation methodology, such as DISRUPT-IT from Atos Origin (Information Society Technologies 2001) represents one way to identify offering that can displace some or all of an established market. We argue that the next generation of Active technology Watch, based on tools such as opinion mining and collective intelligence, would and should be included in disruptive innovation methodology.
- *Technology Watch and Network Analysis*. For the assessment of emerging and existing networks and research communities as well as participants within the community, network analysis methodology is needed. Science, research and technological development for security are capability-driven, and although experience from the military domain provides a good starting point in capability-based research, it is necessary to adapt it significantly to address the specificity of the security sector and related communities. The different capabilities (tools, processes, skills, and behaviours) will often need to be implemented across many areas, in dynamically changing context and across Europe. These also span before mentioned technology lifecycle, but also supply chain, change management etc.

Conclusions

STRAW approach to active technology watch is based on a collaborative process across various cross-country communities which strength its independence and transparency. STRAW is therefore emphasising the need to make technology watch a collaborative and unbiased process. This includes involvement of a large heterogeneous group of contributors and interested parties as well as fast, flexible and practical procedures.

Inputs from previous security research are highly welcomed, but they are not sufficient. Product development and engineering leads to innovation and competitively of European security industry, and is therefore equally important for technology watch. Here, the main problems arise with confidentiality of product development and research plans. We tried to address this problem with a mix of top-down and bottom-up approaches. This strategy can be described as a "seed" model, whereby individual experts or research communities propose topics that later can grow in complexity and completeness, hopefully attracting attention of product development teams. STRAW mix of top-down and bottom-up approaches for security research knowledge ordering is therefore one of the most important project strengths.

Technology watch is a sensitive business and market actors might oppose the conclusions of STRAW. In addition, the Security Technology market is very hard to delineate and we can expect criticism or dis-

agreements. Besides segmentation and positioning, we also expect conflicts related to the technology readiness and maturity. However, the prime objective of sustainable STRAW active technology watch service has to be trustworthiness and independence, both in regards to limiting possible biases in its findings, and in the comprehensiveness of its results. Only if those criteria are met can it be expected that the objectives have been achieved.

Management of expert's feedback and overall take up is crucial for the STRAW sustainability. A future development might consider mechanism needed to monitor the adoption and use of STRAW as well as its evolution.

Disruptive technologies can grow rapidly, replacing less efficient precursors, and can create new services and markets. However, it is also essential to identify what new weaknesses/security gaps these technologies may introduce into society, in order to be able take action as soon as possible to mitigate possible dangers. The future extensions of ATW could include or should link to information on the nature of risk, threats, impact etc. Although this is currently not part of STRAW, the service such as assessment on contextual technology investments, or risk assessments for innovative technologies, could be also provided. The related challenges are EU-wide stimulation of the research in specific directions, detecting priorities, establishing competitiveness maps etc.

References

ASD - Project STACCATO (2006). Deliverable *D 1.2.2. STACCATO Final Taxonomy*. http://www.asd-europe.org/site/fileadmin/user_upload/STACCATO_final_taxonomy.pdf retrieved 30.2010 retrieved 30.2010

ASD - Project STACCATO (2006). *Deliverable 2.2.1. Final recommendations towards a methodology for technology watch at EU level*. http://www.asd-europe.org/site/fileadmin/user_upload/STACCATO_final_recommendations.pdf retrieved 30.2010 retrieved 30.2010

Atos Origin (2010). *Lookout Service*, http://lookout.atosconsulting.com/ retrieved 30.2010

European Security Research Advisory Board (ESRAB) (2006). *Meeting the challenge: the European Security Research Agenda. A report from the European Security Research Advisory Board*. http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf retrieved 30.2010

European Security Research and Innovation Forum (ESRIF) (2010). *Home page*. http://www.esrif.eu retrieved 30.2010

Foundation pour la Recherche Statégique (2004). *Security Network for Technological Research in Europe (SeNTRE)*. http://www.frstrategie.org/specifique/activitesEuropeennes/SeNTRE.pdf retrieved 30.2010

Information Society Tecnologies (2001). *IST Project Fact Sheet (Project DISRUPT-IT):* http://cordis.europa.eu/fetch?ACTION=D&CALLER=PROJ_IST&QM_EP_RCN_A=61140 retrieved 30.2010

Information Week (2006) - Greenemeier, L. Blog-Based Analysts Shake Up IT Research.. http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=188100576 retrieved 30.2010

MediaWiki (2010). *Homepage*. http://www.mediawiki.org/wiki/MediaWiki retrieved 30.2010

Pennacchiotti M. et al (2005). *Terminology extraction: an analysis of linguistic and statistical approaches*. http://www.marcopennacchiotti.com/pro/publications/SFSC_2005.pdf retrieved 30.2010

Project STRAW (2008). D1.1 - *Technology watch list*. http://www.straw-project.eu/?q=content/repository retrieved 30.2010

Project STRAW (2010) D3.3 - *STRAW Sustainability Plan*. Not published yet.

White House (2010). *Homeland Security*. http://www.whitehouse.gov/issues/homeland-security/ retrieved 30.2010

Wikipedia (2010). *Web2.0*. http://en.wikipedia.org/wiki/Web_2.0 retrieved 30.2010

TACKLING THE GROWING COMPLEXITY IN INFORMATION SYSTEMS

Rauli Puuperä & Kimmo Halunen
Oulu University Secure Programming Group, Computer Science and Engineering Laboratory, University of Oulu

ABSTRACT – *Complexity is one of the most emerging threats to critical infrastructure. This growing complexity brings about more and more problems and vulnerabilities to the systems that have at the same time become a part of our daily lives. These systems are many times beyond the comprehension of the very people who are supposed to maintain them. Finding suitable methods and tools for managing this complexity and discovering the hidden dependencies and vulnerabilities is of utmost importance. The traditional methods for studying these systems are not suitable in the future for managing the rapidly increasing complexity. Thus a new approach more akin to the empirical study of the laws of physics and nature than to the engineering driven methods of today is needed. This means that we should more try to study the problems in information systems as phenomena to be understood rather than singular problems to be solved with yet another tweak in some of the underlying protocols, software or devices. This would in our opinion lead into a better future development of devices, software and technology in general.*

Introduction

The 21st century has brought about the rapid growth of information systems. This growth has been very notable in the developed countries and nowadays almost everyone needs information systems and the services of the Internet daily. The pervasiveness of these systems has become an increasingly difficult problem from security perspective as can be seen from the rise of cybercrime, malicious programs and from the growing impact that failures in the network and information systems cause to individuals, organizations and even societies.

One of the main issues affecting the security and functioning of modern information systems is the complexity of the networks, communications and software that enable the functionality that many rely on. This complexity has made it virtually impossible to have a thorough understanding of the network of information systems. Even when some parts of the system are very well understood and documented, the interaction of that system with other systems might be misunderstood or forgotten.

Especially the use of these systems in critical infrastructure has brought these issues into surface. As the name suggests, critical infrastructure consist of the services, facilities and goods, which are essential to the functioning of some organization or government. The question at the heart of this discussion is how we can manage the growing complexity in the future. Will the growing complexity lead to a situation

where the systems actually do more harm than good or will the positive effects always outweigh the negatives? In this paper, we will try to show some scenarios and the ramifications of these scenarios.

We will also describe some of the methods that we have found effective in tackling some parts of the problem of complexity. These methods approach the problems in information systems more like scientific phenomena to be understood and explained than the conventional engineering approach of finding a problem and fixing it. Our testing methods use some ideas from genetics and other natural sciences in order to better tackle the problems. We also use a method for finding hidden dependencies in order to quickly gain a visual and more thorough understanding of the phenomenon under scrutiny.

The paper is organized in the following way. The second section defines the key concepts and the research topic in detail. In the third section, we describe four scenarios of growing complexity and its effects. In the fourth section we discuss some of the existing methods for tackling the complexity and their effectiveness in the proposed scenarios. We conclude with sections for discussion and conclusions, where we take another look at the future and propose some research topics.

Complexity and information systems

In order to have a meaningful discussion on the topic we need to define some basic concepts. First of all by an *information system* we mean any system, which contains information and which is accessed by either other information systems or individuals. Thus our view of an information system is quite large. Of course the main focus of our research and discussion is on the modern information systems. However, even a system with stone blocks and runes inscribed on them can be considered as an information system.

One notoriously ambiguous term often used is *complexity*. Complexity is usually a property of a system that is so complicated that its functionality can not be merely described as the functions of its parts. Also in computer science complexity is usually used to describe computational complexity, i.e., the amount of simple, atomical computational steps it takes to complete a run of some algorithm. We would like to add to this by also considering the usability complexity, especially in the context of information systems and processes. This complexity does not necessarily grow as the complexity of a system grows. A good example of this phenomenon is the library. Only a few decades back the index of books available for the customers of libraries were only available as paper cards that were filed in a (usually enormous) cabinet by some order (alphabetical, Dewey decimal etc.). The only way to use this information system to find the books one wanted to obtain was to go to the library and go through the index cards. Nowadays, most libraries have even more books available than before, but the usability of the indexing system has improved enormously. The database containing the information on the books is in digital form and usually even accessible from the Internet. This has lead to a decrease in the usability complexity as the customers can now access library databases from their own computers and search the database with a multitude of search terms.

Information systems are nowadays almost ubiquitous as computers and the internet have become the tools through which many people work, do business and spend their leisure time with. This has lead also to the situation, where the understanding of these systems or the great systems, which contain all these different information systems has become almost impossible. It is certainly not enough to know the inner workings of a single part of these systems be it a single microprocessor, computer or even a

large network of computers. Thus problems in any (even a small) part of this system can have ramifications on the system as a whole.

This pervasive nature of information systems in our society has lead to the description of our current society as *the information society* (or knowledge society (Mettler, 2005)). The emerging trends in this type of society are the increase in less tangible goods and services such as virtual realities and games. This also means that new information and new ways to utilize, disseminate and analyze information have the most value in this type of society. The role of information systems is very central in this society whereas before these systems were merely tools for the manufacturing industries. The nature of information society has lead to the situation where almost the whole infrastructure is somehow dependent on well-functioning information systems. This is also true for critical infrastructure.

Information systems are much more than just the sum of the individual parts. This also means that these are much more complex than the parts as the interactive nature of modern information society means that the different parts and systems interact with each other. This growing complexity of information systems causes problems in many ways. Whenever the information system malfunctions, finding the cause of the problem is also difficult and sometimes impossible. Maintaining and administering a complex information system is hard and time consuming and every time a new part (service, a piece of hardware, an user interface, etc.) is added to the system the overall complexity grows more than the complexity of the new part. Complex systems also tend to be more vulnerable to attacks as they may contain functionality and dependencies, which are unknown and/or undocumented. These may lead to nasty surprises and the systems may exhibit chaotic behavior, which can be hard to understand (Gordon, 2008).

Probable scenarios

In this section we describe four scenarios for the future development of information systems. We identify two directions of complexity growth and use these to develop our scenarios.

We have identified two major directions in which the complexity of modern information systems is increasing. First direction is the *spreading* of information systems in such a way that they cover more areas of the society as a whole as well as more areas of each individual's life. It is worth noting that the old Internet addressing scheme IPv4 (RFC 791) has already basically run out of distinct addresses for each device and/or individual in the network. This problem is to be tackled with the new IPv6 scheme (RFC 2460), which supports an enormous amount of possible unique addresses for network devices. However, the new system has been very slowly adopted as the technology of the internet usually requires a lot of backward compatibility. In any case, there will be more and more devices joining the network and communicating with other devices and/or individuals.

The other direction of growing complexity is *depth* by which we mean that the information systems are a part of and control more and more the critical parts of societies and individuals lives. Online banking is a very good example in the individual perspective as nowadays almost all banking services are available to customers online. Societies are dependent on the fast and accurate transmission of data between different government agencies and especially the availability of information systems is very critical.

In the scenarios we have a few underlying assumptions. First of all, as is common in futurology, we leave out the possibility of a global disaster that effectively shatters the modern society. Secondly, and more particular to our paper, we assume that the amount of new information (and links between the existing information) grows at an increasing rate. We will also refrain from considering the role of artificial intelligence in our scenarios. This is because the development and effects of AI are very unpredictable. In the light of historical development, we find these assumptions quite reasonable.

Table 1. The four scenarios

		Spreading	
		Contained	**Uncontained**
Depth	**Contained**	*Harmonious growth*	*Wild spreading*
	Uncontained	*Deepening impact*	*Complexity explosion*

The first scenario is labeled *harmonious growth*. This means that even though information systems continue to spread and to dig deeper into the society, there are regulations, mechanisms and techniques which help to contain, understand and cope with the issues. There would still be incidents on critical infrastructure, but these would be exceptions. Furthermore, the impact of these incidents could be dampened and the normal routines of society would not be much disrupted. Also the individuals could enjoy the level of privacy that they choose to exhibit. The growth of information could be effectively utilized and it would not become just noisy chatter where one is hard pressed to find relevant and meaningful information. Thus, innovation and advances in science and technology could become easier and progress could be made a lot faster in many key areas of science and technology.

The second scenario is *wild spreading*. This means that the spreading of information systems continues and there are very few mechanisms to limit it and to cope with the complexity that this brings to the society. In an extreme case this means that every toaster, milk carton and piece of clothing is somehow constantly communicating via different channels with other devices. The benefits of remotely controlling some household appliances are already today well understood. On the other hand, this wild spreading causes an enormous toll on the communication and information infrastructure. If this constant chatter of mostly irrelevant (to the society as a whole) information can not be distinguished from

the useful information, the increase in information does not lead into useful actions as people and devices alike struggle to find the needle of relevant information among the haystack of all information. However, the deepening effects of complexity in information systems have been either limited or techniques for handling and understanding the effects of this have been formed. Thus, the effects on the physical routines of the society and to the most important parts of individuals' lives are limited. The spreading of information systems will make it ever harder and harder to find relevant information and this may lead to the situation where organizations and governments wish to limit the information systems in such a way that the amount becomes manageable. Thus, the internet would be partitioned into different domains with little interaction between them.

In the third scenario, *deepening impact*, the spreading of information systems can be contained and coped with by new methods, regulations and techniques. However, the information systems penetrate ever deeper into the lives of individuals and into the fabric of society. This deepening leads into trouble, when these information systems are compromised or when they fail. Even though these incidents may be relatively infrequent in nature, the damage done to individual people, organizations, companies and governments grows all the time. On the other hand, the society requires its participants to use these systems as these have become the norm in commerce and interaction. It may also lead to oppressive behavior from governments and organizations towards the individual. The systems that have a deep impact in the lives of individuals could e under constant monitoring and thus privacy could be lost.

The final scenario we propose is called *complexity explosion*. In this scenario, complexity continues to spread and also reaches more deeply into the critical infrastructure and everyday life of ordinary people. Also the mechanisms and techniques of coping with this growth fail to provide more safeguards and more effective measures to prevent and recover from failures of the information systems. This means that the failures in information systems become more frequent and disrupt the everyday routines of the society. Because the deep effect of these failures there might be loss of life and economic disturbances. Also civil unrest may ensue. It is very likely that criminals and other unscrupulous individuals and organizations would take advantage of this state of affairs and try to use the vulnerable nature of the information systems and society to their own purposes. In addition, this complexity explosion could eventually lead into situation where adding more devices and services to the information system actually makes it very likely less useful for the users. This very negative consequence could lead into a stagnant state, where innovation in the information systems stops altogether.

As can be seen, these four scenarios are not a complete list of possible future development on information society and information systems. As the world at large is not a homogenous entity we might expect some or all of these scenarios in different parts of the world and/or at different times. Table 1 demonstrates the relationship between our directions of complexity and the scenarios we presented above.

Methodology for tackling complexity

In this section we describe two methods that we have utilized to tackle some of the problems arising from the complexity of information systems. One of our methods is a software testing method that infers a model for the input data from one or several sources and applies this model and some mutations in

order to generate test data. The other method we have applied is an information gathering and visualization tool that can be used to provide insight on information systems.

In all the possible scenarios presented in the previous section complexity of information systems grows, in one way or another. Since the growth is inevitable we must develop new methods for handling the situation. Complexity of information systems is already a significant problem. Even if we look at a single program it is very complex in the sense that it depends on multiple protocols, file formats, external libraries, etc. The role of software in information systems has been increasing with the same rate as its complexity. A good example of this is vulnerability research. Vulnerability research is a discipline of finding faults in computer programs. In the old days, a vulnerability researcher could read the specification of a protocol that the system under test used and generate test cases based on that information. Today this kind of approach is still feasible but it is becoming more and more costly. New protocol specifications tend to be long and labyrinthine, e.g., ISO/IEC 29500:2008 Part 1 consists of 5560 pages (ISO 29500, 2008).

One approach to address this situation is to use some sort of model to find faults. We can build a model based on partial knowledge. For example we can use the behavior of the system, on the data the system handles, etc., as the basis for testing. In the PROTOS GENOME project we have developed methods of generating useful test cases based on some sample data. So instead of trying to understand the protocol in use completely, we observe some network traffic and use that knowledge as the basis of testing. Thus we employ the idea that we should study to understand instead of studying to solve some specific problem.

On a larger scale in computer networks protocol dependencies are causing a number of problems. Protocols can contain other protocols that can contain other protocols and so on. This matryoshka principle of protocols yields a situation where protocols are highly dependent of each other. These interdependencies have caused serious problems in the past (OUSPG, 2002). These dependencies in most cases are not obvious as Eronen and Laakso have pointed out (Eronen & Laakso, 2005). Thus material has to be collected from multiple sources and to map the dependencies in this collected material in some visual way. In our MATINE method, we gather information on dependencies on a certain subject and enter it to a database. We use a Graphingwiki tool introduced by Eronen & Röning (Eronen & Röning, 2006) to draw graphs to gain more insight on the dependencies.

Both of the above examples demonstrate how we can cope with growing complexity. Of course the understanding every detail of the whole system would give us a better result but in these cases it would be so time consuming that it is not possible. The world of information systems is in a state where we need to form better theories of how these systems behave. It might even be possible to aspire for a unified theory as the physicists do in physics.

In general as information systems get more complex the amount information we need to possess in order to understand the inner workings of the system grows dramatically. In physics in most cases, we do not need to understand all details of a physical phenomenon to understand it. For example if we consider a small weight attached to a spring we can calculate how high the spring will bounce even if we do not take to account the atomic properties of the metal that the spring is made of. The same goes for information systems. If we want to understand a complex system, we must take a step back and try to understand the whole instead of the individual parts.

Conclusions and Future Work

All in all future will bring us more complex information systems. Whether or not the society can cope with this growing complexity and its implications will define many aspects of future development. Because the directions in which complexity may grow are not mutually exclusive we have to be able to take into account many variables when trying to understand modern information systems. However, this is in our opinion the only way to succeed in this task as by focusing on only singular events or parts of the system will not result in a desirable outcome. This does not mean that there should be no efforts to improve the hardware, software and protocols, which are the building blocks of our information systems. Nevertheless, in order to make the most out of these improvements it is necessary to understand the whole of information systems and information society. Especially in critical infrastructure this understanding should span all the levels of the organizations that form the infrastructure.

As we have stated in this paper understanding the complexity and its implications is crucial for the further development of the information society. We have developed some methods that can be utilized in a small scale to provide more thorough understanding and to test the robustness of modern information systems. Unfortunately, even our methods are not comprehensive enough. The model based fuzzing techniques can not find all the flaws in software and there is no time for one to test all protocols and software and different combinations of these. Thus the advances should be made in the design phase and this requires a shift in the mental model of software, hardware and protocol developers. This is a very slow process and it needs lots of support from different actors to be successful. Our method for finding hidden dependencies works fairly well and can be applied at many different levels of abstraction. However, combining the information in all these levels of abstraction can be a very difficult task and trying to filter only the relevant information from each level has been a very difficult task. Furthermore, this become quite computationally intensive as the size of the system under scrutiny grows and we still lack some of the tools needed to automate many of the more laborious phases of the method.

References

Bishop, Peter (2008) *Teaching Systems Thinking*. Futures Research Quarterly, Summer 2008, 7-38.

Eronen, Juhani - Laakso, Marko (2005) *A Case for Protocol Dependency. IWCIP '05: Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection, 22-32, IEEE Computer Society.*

Eronen, Juhani - Röning, Juha (2006) *Graphingwiki - a semantic wiki extension for visualising and inferring protocol dependency. Proceedings of the First Semantic Wiki Workshop, 1-15.*

Gordon, Theodore Jay (2008) *Recognition and Management of Systems in Chaos.* Futures Research Quarterly, Summer 2008, 39-50.

Internet Engineering Task Force (1980) *RFC 791 - Internet Protocol version 4.* http://tools.ietf.org/html/rfc791 retrieved 29.4.2010.

Internet Engineering Task Force (1998) RFC 2460 - Internet Protocol version 6. http://tools.ietf.org/html/rfc791 retrieved 29.4.2010.

International Organisation for Standardization (2008) ISO/IEC 29500:2008 Part 1. http://www.iso.org/iso/pressrelease.htm?refid=Ref1181 retrieved 29.4.2010.

Mettler, Peter H. (2005) *The Coming Global Knowledge Society: How to Analyze and Shape its Future?*. Futures Research Quarterly, Spring 2005, 51-68.

Oulu University Secure Programming Group (2010) *PROTOS Protocol Genome Project*. https://www.ee.oulu.fi/research/ouspg/genome retrieved 29.4.2010.

Oulu University Secure Programming Group (2002) *PROTOS Test Suite c06-snmpv1*. https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c06-snmpv1 retrieved 29.4.2010.

Viide, Joachim - Helin, Aki - Laakso, Marko - Pietikäinen, Pekka - Seppänen, Mika - Halunen, Kimmo - Puuperä, Rauli - Röning, Juha (2008) *Experiences with model inference assisted fuzzing*. *WOOT'08: Proceedings of the 2nd conference on USENIX Workshop on offensive technologies, 1-6, USENIX Association.*

AN EVALUATION OF VOIP COVERT CHANNELS IN AN SBC SETTING

Christian Wieser & Juha Röning
OUSPG, Infotech Oulu and Department of Electrical and Information Engineering, FIN-90014 University of Oulu, Finland

ABSTRACT – *Voice over Internet became popular in recent years, shifting the classical telephony system towards the Internet age. At the same time this shift poses new challenges in several areas, one of them found in security. A Session Boarder Controller is acting as a gatekeeper at the borders of trust. We were evaluating such a device for covert channels. Such covert channels were found them in the control and the media exchange protocol implementations. All of the channels have a considerable bandwidth, making their exploitation rewarding for any culprit.*

Introduction and Background

In the past, the Public Switched Telephone Network (PSTN) was used primarily for the transmission of voice, with the transport of data accounting only for a fraction of the volume. During the last ten years we have seen data traffic growing at a fast rate. In 1999, there was an equal amount of voice and data traffic and by 2002 the volume of data traffic was a magnitude higher. Internet operators were looking for new markets and found Internet telephony. Internet telephony is also known as Voice over Internet Protocol (VoIP). Traditionally, the PSTN was under close scrutiny by regulatory bodies, whereas the same regulations have not been applied to VoIP. Initially research was conducted in the area of improved quality and new services. Security was not an overriding issue. Due to frequently found vulnerabilities – for example described in (Wieser & Laakso & Schulzrinne 2004) and (Wieser Christian & Takenen & Röning 2006) – and their exploitation, security has become more relevant.

VoIP transmissions, which utilize standardized protocols, establish two logical channels: the control channel and the media exchange channel, each reflected by its own set of standards. Describing the control channel is for example: Session Initiation Protocol (SIP) (IETF 2001), H.323 (ITU 2006) and MGCP (IETF 2000). The actual transmission of encoded voice and/or video is then done on the media exchange channel implemented typically via the Protocol for Real-Time Applications (RTP) (IETF 2003).

One functional element to improve security in VoIP systems is the Session Boarder Controller. Such an SBC could be considered a session policing controller, an element that provides a multitude of functions, including an application layer firewall. SBCs are located at trust boundaries.

The term covert channel was introduced by Butler Lampson (Lampson 1973). It is a channel that exists parasitic in a legitimate channel and is generally hard to prevent. The goal of this paper is to describe software and tests to demonstrate the existence of these covert channels in VoIP systems and answers

the question if an SBC detects and counters the utilization of such a channel to transmit arbitrary binary data.

The layout of this paper is as follows: In the next section, we reference relevant previous work, after which we describe the test setup. Then the test cases and their results are presented. An analysis of the results and their discussion finish this paper.

This work profits from earlier work done in the area of VoIP security and covert channel detection. Thermos and Takanen (Thermos & Takanen 2007) wrote the reference literature on VoIP security. Their work describes threats, vulnerabilities and countermeasures in a comprehensive manner. The SIP RFC proposes a generic threat model and gives recommendations for a safe deployment of SIP. Neither work included covert channels. These are described for example in the DoD's "The Orange Book" (Department of Defence 1985). Such covert channels in VoIP are described by W. Mazurczyk and Lubacz (Mazurczyk & Lubacz 2008) and Takahashi and Lee (Takahashi & Lee 2007). Their work concentrates on establishing and detecting VoIP covert channels.

Test Setup

The test network for the following experiments is depicted in Figure 1. The SBC is acting as application layer firewall between the public Internet and a private network. In each network, one computer is acting as endpoint. A management network connects all parts to a single host, from which the experiment is conducted. All parts are connected by a 100 MBit/s IEEE 802.3 network, with a measured upper speed of 11 MBytes/s.

We have tested a SIP SBC with the latest firmware and configured it to work as expected. The user agents are registered with valid user accounts at the SBC. We do not reveal the SBC's vendor, because we have not communicated the results with them, because we did not test any other SBC, singling them out should be considered unethically.

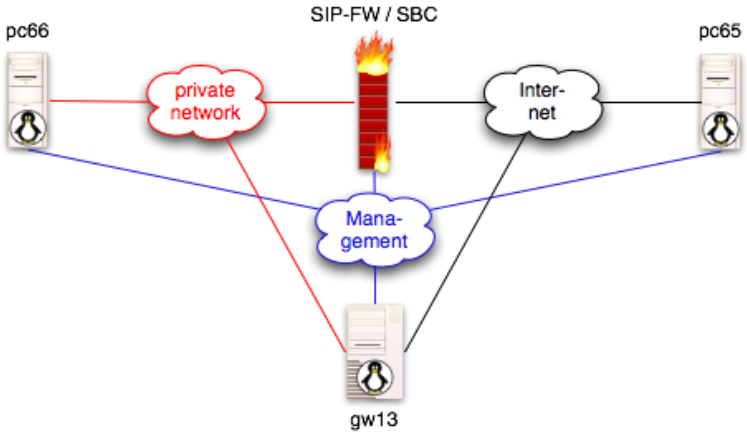


Figure 1. The test network setup.

Test Program

We adapted the Shtoom (Divmod 2003) SIP user agent for our purpose. The reason we used this specific program had been: The license permitted us to utilize it, the program worked satisfactorily and the program structure allowed us an easy adaption. We used UDP as transport protocol for SIP and RTP.

Test cases

We have separated our test cases into two groups: We try to find and assess hidden channels in the SIP control channel. Later, we evaluate the media exchange channel RTP.

The correctness of any communication in a covert channel was ascertained with an MD5 checksum of the transmitted data. All reported test cases have matching checksums.

Covert channels in SIP

We tried to find covert channels by forging SIP header fields. Initial tests used the From and To display name fields. Binary data was MIME encoding and passed the SBC unaltered. In a next step, we found out the maximum header field size of the From and To display name fields listed them in Table 1. By continuously calling, we also found the maximum throughput of the channel.

Table 1. Maximum SIP header field length and throughput

Field	Size	Throughput
Fom display name	546 bytes	2150 bytes/s
To display name	518 bytes	1768 bytes/s

Because we kept the SIP-URIs constant, the call was directed to the desired callee.

Covert channels in RTP

During the successive tests, a call was established again through the SBC and the RTP media exchange was carrying the covert channel. On the control channel we announced the usage of the G.711 codec. I accordance to the AV Profile (IETF 1996), the default interval should be 20 ms, which leads to a RTP payload of 160 bytes.

Ascertain maximum RTP payload size

At first, we tried to see if the SBC checked the RTP payload. We send random data in the RTP payload, which the SBC passed. We then changed the payload length and adapted the RTP header fields accord-

ingly. We achieved a maximum payload size of 1456 bytes, which is together with the header fields of RTP, UDP, IP and Ethernet the maximum size of an Ethernet frame. Split UDP packets were silently dropped by the SBC.

RTP packets send faster than interval time

The default interval time of PCMU is according to the profile is 20ms. We tested, if the SBC checked any of the RTP timing. The results are found in Table 2. We utilized the maximum payload length found in the previous experiment.

Table 2 RTP interval time and throughput

RTP sending Interval	Throughput
20 ms	71935 bytes/s
15 ms	93929 bytes/s
10 ms	13882 bytes/s

RTP header nonobservance

In the final test, we wanted to find if the SBC checks for any of the RTP header fields and simply send random data on the previously agreed media channel. The SBC allowed the data stream to pass. With no delay between send packets and the maximum Ethernet packet length we achieved a constant throughput of 569 Kbytes/s.

Analysis of the test results

The goal of this test setup was to detect covert channels in VoIP network with an SBC. In this test setup such were found in the SIP and RTP implementation. The SBC was not successfully evaluating packets for covert channels. Notably the RTP test cases showed the existence of a high bandwidth channel. It seems the firewall is merely opening a connection between the networks, routing the packets and is not checking the content of the passing RTP packet. The SBC did not log any anomalous condition. The bandwidth of any channel is considered high by “The Orange Book”, as it is over 100 bits/s.

Discussion and further work

With the above results, we try to give context to them. One limitation of your work: we could test only one SBC. We aim to extend our work to include a more complete picture of several different SBCs. Our expectation nevertheless is, that we find covert channels in all further SBCs. Reason being that voice and video has a natural variance, and so has data send in the control channel.

Even if the throughput by advanced detection (as proposed for example in (Takahasi Takahiro & Lee Wenke 2007)) might be reduced, we have a wide range of choices to adapt the channel encoding: using

steganographic methods, or switch to a timing based covert channel. Another limitation of this attack is: we have to manipulate the locally running VoIP software.

Can we estimate the relevance? Today, our web browsers allow us to connect to a plethora of information sources. Why are then such covert channels of any relevance? We can think of obvious reasons: stealthy and bidirectional communication and network neutrality. We could open communication without the notice of the SBC and transferred data in both directions. Due to the implicit end-to-end character of any telephone conversation, a successful attacker is able to initiate data transfers on any side of the SBC. By comparison, we typically do not allow users to run their own web servers on their local computers for good reasons. Covert channels might be increasingly relevant in a non net neutral setup, in which specific network traffic is discriminated. If a VoIP call receives better quality of service, these techniques will become popular.

Acknowledgement

We would like to express our appreciation to Infotech Oulu for providing support during this research.

References

Wieser Christian – Laakso Marko – Schulzrinne Henning (2004) SIP Robustness Testing for Large-Scale Use. *SOQUA/TECOS*.

Wieser Christian – Takenen Ari – Röning Juha (2006) Security analysis and experiments for Voice over IP RTP media streams. *SSI 2006*.

IETF (2001) *SIP: Session Initiation Protocol*. http://www.ietf.org/rfc/rfc3261.txt retrieved 29.4.2010.

ITU (2006) *Recommendation H.323*, Jun. 2006, Geneva, Switzerland.

IETF (2000) *Media Gateway Control Protocol Architecture and Requirements*. http://www.rfc-editor.org/rfc/rfc2805.txt retrieved 29.4.2010

IETF (2003) *RTP: A Transport Protocol for Real-Time Applications*. http://www.rfc-editor.org/rfc/rfc3550.txt retrieved 29.4.2010.

Lampson Butler W. (1973) *A note on the confinement problem*, Communications for the ACM, 16(10).

Thermos Peter – Takanen Ari (2007). *Securing VoIP network*. Addison Wesley.

Department of Defence (1985). *Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD (The Orange Book) edition.

Mazurczyk Wojciech - Lubacz Jozef (2008). Analysis of a procedure for inserting steganographic data into VoIP calls. http://arxiv.org/pdf/0806.1034v2 retrieved 29.4.2010.

Takahasi Takahiro – Lee Wenke (2007). An Assessment of VoIP Covert Channel Threats *SecureComm*.

Divmod.org (2003) *Shtoom*. http://divmod.org/trac/wiki/ShtoomProject/ retrieved 29.4.2010.

IETF (1996). *RTP Profile for Audio and Video Conferences with Minimal Control* http://www.rfc-editor.org/rfc/rfc1890.txt retrieved 29.4.2010.

SIMULATING INFORMATION SECURITY WITH KEY-CHALLENGE PETRI NETS

Simo Huopio[a], Pekka Wartiainen[b] & Anneli Heimbürger[b]
[a]FDF Research Centre, P.O. Box 10, FI-11311 Riihimäki, Finland
[b]University of Jyväskylä, P.O. Box 35, FI-40014 University of Jyväskylä, Finland

ABSTRACT - *The increased complexity in the networks, measured by the number of connected devices, offered services, and the variations in access options, has made even the basic network planning a challenge without suitable tools. The same trend makes the security evaluation of the chosen infrastructure and policies a significant challenge. Modelling any real systems security properties requires scalability, efficiency and ease of application to be practical. Based on a method introduced earlier, Key-Challenge Petri Net (KCPN), a hierarchical model of complex systems can be constructed for evaluation of information security. In this paper we describe a novel application of simulating the KCPN model with a case study of a realistic network and discuss about the experiences from preliminary simulations.*

Introduction

Administrators of complex computer networks would get a lot more insight to their work if they had a reliable model of the security properties in hand. The model could be used e.g. in testing different strategies for protecting the network and visualizing the results. In order to accomplish this, the model should be complete and realistic, and there should be good tools to simulate it.

Modelling information security properties on the communication networks can be done on many abstraction levels. On a detailed level, one can for example create a detailed attack graph regarding the target system which provides accurate view to the present state against all known attacks. On this detailed level, modelling any larger part of networked system becomes easily too complex to be analyzed or visualized (Sheyner et al. 2002, 273). On a more abstract level, information security can be viewed as an access control system. This approach can be too general and abstract to provide any real value.

The Key-Challenge Petri Net (KCPN) model, as introduced by Kiviharju et al. in (Kiviharju et al. 2009, 190-206) provides possibility to choose the practical abstraction level suitable to the purpose by having multiple hierarchy levels. With the KCPN model it is possible to have a simple network topology view on top modelling the whole network behaviour under attack, but still at the same time the model is capable of simulating even the internal details of a single workstation, such as a web browser or a device driver. The KCPN model is also planned to be flexible enough to be able to model the modern social engineering attacks like Phishing, or attacks using USB drives, which have been hard to incorporate in the traditional models.

The KCPN model does not yet have support from the available simulator tools. In this paper we address that by describing the application of simulating the KCPN model in a Stochastic Activity Network (SAN) simulator. The implementation approach is discussed and the details are narrated with the help of a use case.

The remaining paper is organized as follows. Next two sections introduce the KCPN model and discuss the related work in information security simulation. *Description of the simulation environment* introduces the simulator tool we chose for implementation. In the following two sections an example use case is discussed along with details how the KCPN model is implemented on top of the simulator. Before conclusions, there is a chapter for *preliminary results*, in which we describe how the model behaved in our initial simulations.

KCPN model

The Key-Challenge Petri Net (KCPN) model introduced in (Kiviharju et al. 2009, 190-206) was specifically built for modelling network security. It was based on case of generalization of stochastic Petri nets, called Hierarchical Coloured Stochastic Activity Networks (HCSAN) (Azgomi & Movaghar 2004, 297-308), defined originally for the modelling and analysis of distributed real-time systems. The concept of key challenges was adapted from Key-Challenge Graphs (Chinchani et al. 2005, 108-117).

The KCPN model has many good features needed for comprehensive network security modelling and simulation. It uses variable abstraction level, which is powerful in expressing even complex networks, and in the same time reasonable for simulation. The model uses hierarchy for scalability for simulation and precision, and to give the researcher straightforward views to different abstraction levels. Built into the model there is also a way of monitoring the basic security attributes - confidentiality, integrity and availability - for all needed entities.

Figure 1. A KCPN graph consisting of two places.

Figure 1 shows simplified version of a KCPN graph. Entities with information or capability that can be acquired are presented as places on the graph, like u and v on this graph. A place can be, for example on a network topology level (TL), a database server or a computer system. On the TL, one place can represent a large number of computers with identical characteristics of the device, running software and reachability. Using this method the complexity of the model can be reduced significantly (Ingols et al. 2006, 121-130).

Each place can also have a colour and security attributes. The colour denotes the ownership of the place i.e. whether it is originally at an attacker's possession, a neutral place or owned by the defender. The security attributes are Confidentiality, Integrity and Availability (CIA). The colours and security attributes are used in making rules for monitoring the state of an attack. For example, an attacker success-

fully entering the defender's place with an availability attribute set and monitored, is equivalent of a successful Denial-of-Service (DoS) attack.

Each piece of information or capability that is in the place is presented as a key. A key could be, for example, a password stored on a computer or the knowledge of the local network structure. The edge between the places presents the channel of access between the entities. The security measure that protects the access represented by the edge is denoted by a combination of an input gate, an activity and an output gate.

The input gate, IG_{uv} in Figure 1, has a logical expression involving mandatory keys for entering the activity. If the attacker has the needed keys, his token can pass the challenge with minimal cost of resources, which can be for example time or computing power. Having the required keys equals the situation where attacker has for example knowledge of server software version, suitable configuration and working security exploit. If the key requirement is not met, the cost of entering is significant, equalling brute forcing a security measure or waiting if a suitable exploit is found.

Activity, *IA* in Figure 1, fires the token(s) to the next place in the graph as it has passed the input gate. Activities can have more than one input, and more than one alternate output. Output gate, OG_{uv} in Figure 1, holds the keys of next place v that the attacker receives after successfully entering. The gates and the activity are defined as macros in KCPN, following the HCSAN definition.

Each of the abstraction level has similar structure as the main graph, including places, activities, input and output gates. The lower abstraction level graphs are fully contained within the places of its parent abstraction level. As an example, the more detailed abstraction level of a place denoting a server cluster of TL is usually a graph incorporating the major attack categories and their phases to this particular server type. On this abstraction level, a place can be an intermediate step in attacking the system, for example the act of scanning the local network for vulnerable software versions. These layers of lower abstraction are called Attack Action Levels (AAL) within the KCPN.

Definitive description and formal structure of KCPN is presented in (Kiviharju et al. 2009, 190-206).

Simulation of the Information Security Models

Information security modelling and simulation has been performed from a number of viewpoints (Saunders 2002). The most popular approach is to generate an attack graph in which attacker's actions, network states, and vulnerabilities are represented with nodes and arcs. The most relevant work for our simulation are the previously presented KCPN model (Kiviharju et al. 2009, 190-206) and simulation scenarios of a network in the area of information security.

Simulation tools for modelling cyber attacks to a network have been developed a lot because there are various positive arguments for using a simulator instead of performing tests in the real world. Building the model in the simulator is often more affordable and the results are produced faster. The downsides are that the results are not as accurate, and modelling of human behaviour is difficult with the network tools.

Simulation of information security in networks has various approaches. Some tools like Opnet (Opnet 2010) are designed for analyzing the safety of the network. This kind of software is also good also for performance testing of the network but they do not necessarily include verified and validated attacking models.

Simulation can be also approached from a distributed point of view where the simulator such as NetSim (McGrath et al. 2002) can be used to organize security exercises. These events provide reliable results for certain attack types and they are a good practice to test the defence methods in reality. Unfortunately, this kind of software usually lacks modelling capabilities.

Another type of network security simulator is a client-server based solution. One example of the type is MAADNET (Carver et al. 2002), which is a network simulator for educational purposes. The idea is that the user creates a network architecture and sends it to the server for evaluation. The server analyzes the network and evaluates it with attributes like preservation of confidentiality, integrity and availability. The success of the attack depends on attributes such as the type of the attack and the skill level of the attacker. Still the problem for almost all of modelling and simulation types is that there is only a limited number of attributes related to human behaviour.

Description of Simulation environment

A tool named Möbius (Möbius 2010) was chosen for simulating the KCPN model. Möbius is a software tool for modelling the behaviour of complex systems. It was originally developed for studying the reliability, availability, and performance of computer and network systems. In addition to the original applications, it is now used for a broad range of discrete-event systems, from biochemical reactions within genes to the effects of malicious attackers on secure computer systems.

Möbius is a versatile tool for modelling Petri nets and it's variations like hierarchical and stochastic Petri nets. The only significant limitation is that pure coloured (CPN) and timed Petri nets (TPN) are not supported. Different Petri nets are implemented through stochastic activity network (SAN) models (Sanders 2009) which use an extended notation of the standard Petri net. Besides the standard Petri net objects the SAN model includes input and output gates and extended places. Extended places are places which are not constricted to count tokens but can be extended with customized variables and structures. Möbius doesn't support CPN but extended places can be used to compensate colouring in the model. For this reason it is possible to implement the KCPN model with Möbius despite the lack of CPN support.

Möbius has a highly modular structure. The researcher can create function libraries and use them in Möbius. The application programming interface (API) of the function library has full support for C++ programming language. The source code of the library needs to be compiled with a separate compiler, after which the header and the object file are linked to Möbius. This freedom of expansion gives almost unlimited possibilities to implement more features to the model at hand.

The graphical user interface of the Möbius is straightforward. It consists of multiple windows and each window represents one graphical layout of a SAN graph with simulator-related controls. The main controls are used for linking several SAN models to each other and managing the simulation. The Möbius has also good possibilities for compilation of statistics (called Reward in Möbius) because it is possible to add as many variables as required, by defining them in separate code. There are not any special built in tools for the analysis of the results except the calculation of mean and mean's confidence interval of the added variable. However with the API calls, the user can print out to the log file the marking of a place during the simulation and analyze results afterwards with external tools.

Möbius runs well on modern PC hardware. Supported operating systems are Windows, Mac OSX, and Ubuntu Linux (Sanders 2009). Möbius has an ability to distribute calculations of simulation over the network to other computers which can be useful in cases when the size of the model is significant. Function libraries can also be ported between different platforms by compiling them again in the new system.

Case study

As a case study, an imaginary moderate size company network was drawn for modelling purposes. The network (Figure 2) has two subnets: demilitarized zone (DMZ) and inner private network (Intranet) both of which are separated from the Internet and each other by a firewall. There is a cluster of extranet servers in the DMZ. In the intranet there are a number of workstations which are able to connect to the intranet web server but not directly to the project database server. The access to the Project Database is possible only through the company Intranet Web pages. The company firewall has been set up with a policy of blocking all inbound connections from the Internet.

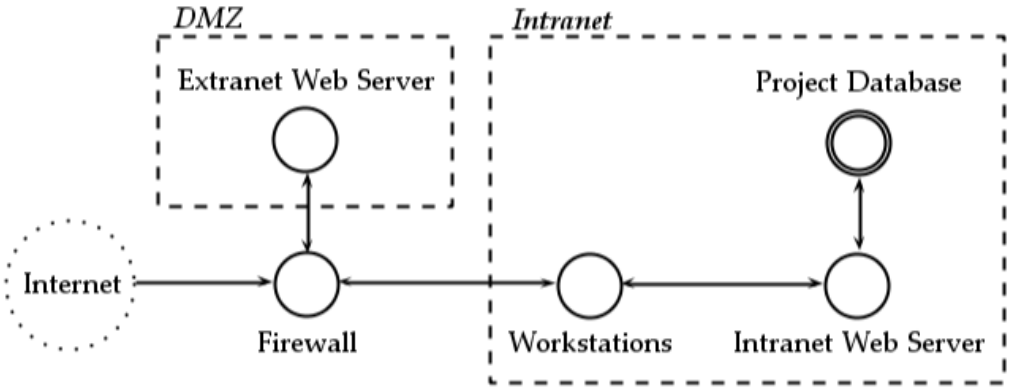


Figure 2. The example network of our case study.

In our simulated case, each device of the network is intentionally associated with several exploitable vulnerabilities in order to enable multiple non-trivial attack scenarios.

The attacker's goal is first to break into the intranet and then gain access to confidential information of company's profit report on the database server. One possible sequence of action to reach these goals would go as follows (Figure 3); Attacker scans all the visible computers that are visible from the Internet and he finds out the extranet servers and their configuration. Exploiting an unpatched vulnerability in the web server he gains login access to it, and with a local privilege escalation exploit he gains full access to the server. From the server databases the attacker finds contact and login information of some of the company employers. Using this knowledge he sends infected PDF files to a number of employers. When unsuspecting employer opens the malicious email attachment, the attacker gains remote control of one of the workstations. The attacker has now reached his first goal of breaking in the company intranet, and immediately begins scanning the internal network topology. Within, he uses similar techniques to first gain control of the intranet web server, and eventually of the protected database server.

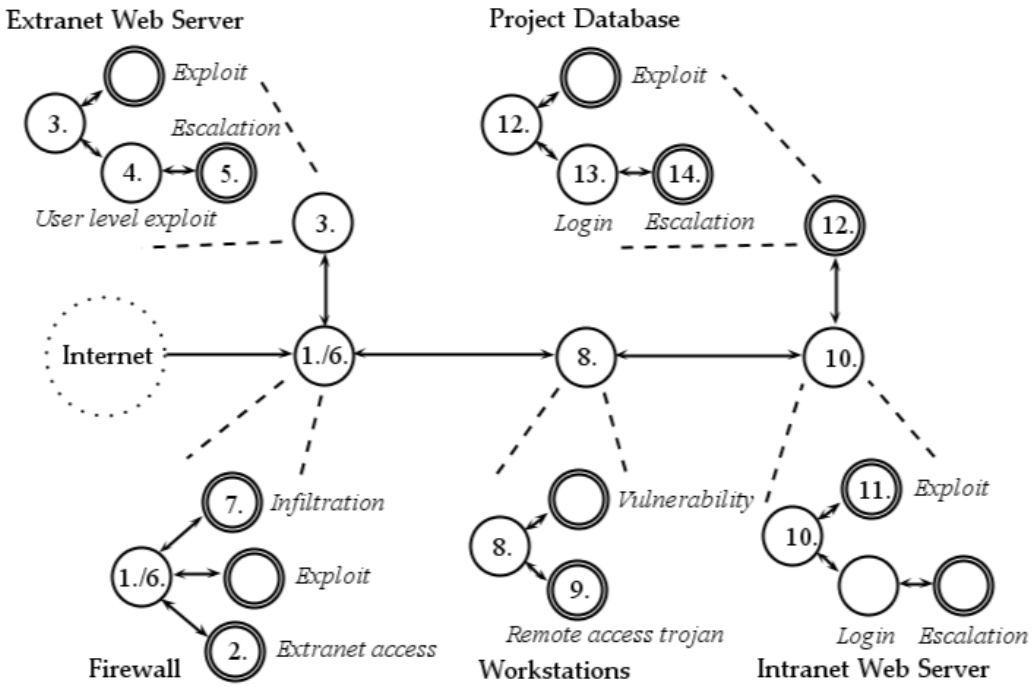


Figure 3. An example attack scenario.

Modelling the example network, its security policy and vulnerabilities revolves around choosing how the properties and attacker knowledge is projected to the keys, and how they are placed within the network. In this case there are, for example, following keys; Knowledge of the extranet server vulnerability is a key, which is acquired when the company network is scanned. Knowledge of how to exploit that vulnerability is another key, which the attacker has in his knowledge or not. Further on, knowledge of a company employer email address is a key, and possession of knowledge how to infect and use the PDF files for the attack is another, and so on. Without these last two keys, the attacker would have to use some brute force attack to the company firewall, or do further research to gain knowledge of the email attacks, both of the activities which would consume lots of time and other resources.

The result of this modelling work is the KCPN model of the network. Further details of the structure of the model and how it is implemented with Möbius is given on the next chapter.

Implementation of KCPN Model

As mentioned earlier Möbius has support for many Petri net formats. For implementing the KCPN model, the SAN file format is used. In the notation of SAN, Möbius is using an extended representation of Petri net. In practice this means that in addition to places, transitions and edges, the input and output gates are defined. The input and output gates are placed on both sides of a transition on graphical layout of SAN file.

The input and output gates have a key role in the implementation process. In the KCPN model the attacker's keys are checked in the input gate and new keys the attacker gains when entering a new place are given in the output gate leading to that place. Technically the input gate has two code fields: one for Input Predicate and the other for Input Function. The functionality itself is defined with C++ code in-

serted in the code fields. The Input Function will be run if the condition in Input Predicate is true. The output gate has only one code field for Output Function. The Output Function will be run after the transition fires the token and before the token reaches the next place.

The input and output gates are also managing the other variables necessary for the KCPN model simulation like costs and probabilities. All of the variables are implemented in the extended places of SAN. Each place is modelled as separate C++ class using inheritance. For example in our case the firewall class is inherited from the device class which is inherited from the abstract place class. The place class contains general structures about the model like placeholders for keys and probabilities. The device class inheriting the place adds the definition of the state and version of the device. Furthermore, the firewall class has all of the previous attributes as well as the type and filtering rules as new additions.

The model parameters are saved in C++ data structures (struct) as doubles and integer lists. Some of these variables are used for the colouring of the HCSAN model (Azgomi & Movaghar 2004, 297-308). For example when the attacker begins the attack towards a workstation the token is being moved to the place called workstations. In this implementation only one type of tokens are present, the attackers, but the places can still be in control of the defender or the attacker. This ownership, or colour, of the place is declared as a state attribute denoting the number of attacker tokens present.

The places which have security attributes assigned are specifically monitored. When the attacker successfully enters a place with any of the security attributes set, the simulator logs the event and checks if the success criteria for the whole attack is met. The success criteria is usually the violation of security attributes in one or multiple places. The other possible reason for ending the simulation is the attacker running out of resources.

In addition to extended places, the other important part of the HCSAN model (Azgomi & Movaghar 2004, 297-308) and also KCPN is the hierarchy. The concept the token moving in the graph hierarchy had to be built manually because the chosen method of joining the graphs would conflict with the way of Möbius running all SAN graphs simultaneously. In practice e.g. in the output gate on the topology level a permission to start running the attack action graph of the next place can be given i.e. when the token is moved to the workstation the sub graph of the workstation is run. After the sub graph is finished successfully the token can continue on the topology level to the next input gate.

In the implementation of the case only two levels were used (Figure 4). The topology level (TL) presents the topology of the network and the second level is the attack action level (AAL) where the attacking methods are described. In our case, every place on the topology level corresponds to one attack action graph. In the real network there might be many devices that share the same kind of software and services like workstations. For example the *workstations* place (Figure 2), which describes many physical workstations, has a *workstation* attack action graph (Figure 4). In this case the attack action graph of the workstation represents two possible attacking methods: to use an exploit or login with a proper user account.

On the attack action level every attack method like a Trojan horse or an exploit has a list of required keys. If the attacker has all of the keys on the list of the attack method, the probability of successful attack will be significantly greater and the costs of resources are lower than without. Still it is possible to use an attack method without any keys e.g. by brute force but the cost is much higher. The attacker gains control of the device when the token manages through the attack action graph. After successful attack

the keys belonging to the last place of the attack action graph are given to attacker in the last output gate, and the permission to continue will be given to the upper level.

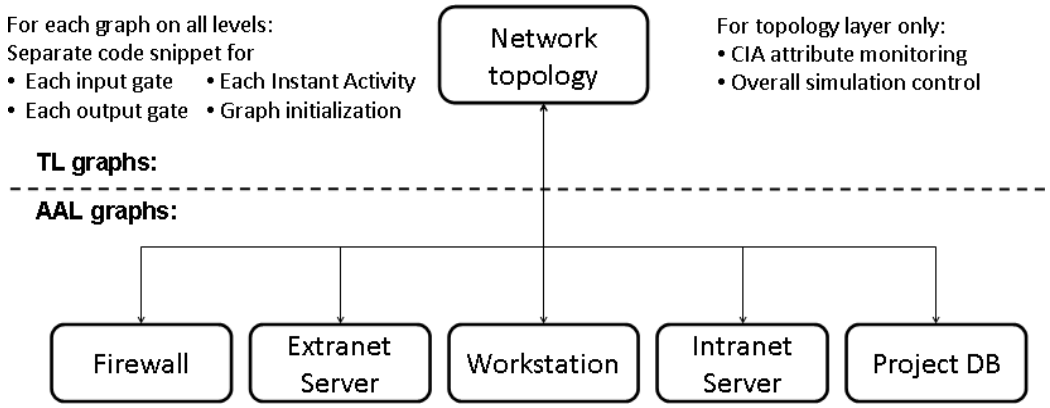


Figure 4. The hierarchical implementation of our case study.

If more detailed simulation of the behavior of the vulnerable devices is wanted, the KCPN model allows using further hierarchy levels, both AAL and TL. (Kiviharju et al. 2009, 190-206). In this example only two levels were used, but e.g. on the third level attack methods of same type could be separated. For example Trojan horse on the second level could be separated to remote access, data theft and keystroke logging Trojans. Optimal use of the multiple hierarchy levels brings simplicity for the graphical layout of the graph, and at the same time enables very detailed results on a chosen focus area to be provided if required.

Preliminary Results

The main goal of our work was to implement the KCPN model into the simulator. Some test simulations were also run but their results are just suggestive. In this chapter we present and discuss the preliminary results.

For this implementation we used very basic set of input parameters. Every device had at least two vulnerabilities and in some devices multiple steps were needed for gaining complete control. The time spent in every attacking step was chosen randomly from the interval which was defined by the vulnerability in use. The total time of breaking the device was affected by a success probability of each attack method.

The attack success probability without the required keys was categorically set to a low figure, usually less than one percent in a resource unit. It means that the attacker has to try to research and brute force trough the security protection of the device and in every step the resources is spent. In cases where the attacker had all the required keys the probabilities of success were set close to 100% in a resource unit. It is to be noted that the resources were spent only on the attack action level of the model, as the token movements on the topology levels are considered practically instantaneous compared to the usually interactive and slower paced attack actions.

Determining the realistic parameter values and keys for the device- and attack libraries is one of the biggest challenges in the implementation work. For this simulation test he parameter values were chosen

by using expert opinions and educated guesses. The model validation with the real world network data and parameter tuning would be the next natural step of the KCPN simulation implementation work.

Figure 5 shows the ratio of the attack success plotted against the resources available for the attack. The initial results seem to be in line with expectations: The model is stable in the simulation and the success trend is believable. It can be seen from the figure that to a certain threshold the amount of resources available to the attacker is the limiting factor to success. Considering the amount of unpatched vulnerabilities present, it was no surprise that the success ratio approaches 100% quickly.

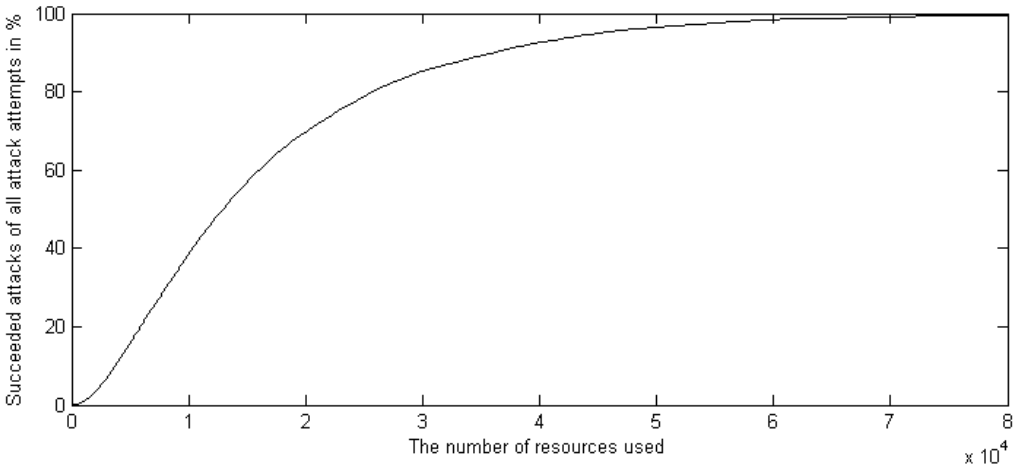


Figure 5. Total number of successful attacks as for used resources.

Naturally, a single run of simulation does not include a lot of valuable data, especially when the model validation is incomplete. The real value of simulating a model, even an abstract one, would come from variating the configuration of the network and the resources and skill level of the attacker and seeking the optimal defense strategies in different threat scenarios.

Conclusions

We have accomplished a basic implementation of the KCPN model to a simulator environment. As the main goal of the implementation process was to use Möbius simulator to produce the preliminary result, the work was a success. Möbius was proven as a versatile simulation tool for working with the KCPN models. One significant factor of the success was the flexible and well designed C++ interface within the simulator. In the resulting implementation the model behaved in a stable and predictable way and therefore proves to be a good basis for validation work and more detailed analysis of the model behaviour.

In the present setup the creation of new scenarios is very laborious and slow. The interactive editor forces the user to enter the source code in small snippets separately for each gate and place of each graph. For managing large models, integrated support for creating and using libraries of different places and their internal sub graphs would be needed. Now the challenge was managed to a degree with disciplined source code management and commenting. The fact that Möbius doesn't provide or link to a proper Integrated Development Environment (IDE) or a debugger makes working with larger models

even harder. The only help available for code verification are the debug printouts and the simulation logs.

For the more practical use of the simulator, more advanced means of importing a new model to the simulator are needed. Even if the libraries would be in place for the needed device types, the lack of a proper graphical network topology editor or an import tool in Möbius would make the creation of any larger model a significant effort. As Möbius is able to read the SAN graphs from a file, the investigations continue whether this could be used for creating an import functionality of our own.

Despite the lack of debugger and import feature, simulating the KCPN model in Möbius provides a lot of freedom to the researcher in variability and scalability for modelling information security attacks. The next step in our work is to make more realistic and complex scenarios and validate and balance the chosen parameterization approach with a real reference system The KCPN model makes modelling very complex attacks possible with the inherent scalability via hierarchy and the unique usage of key challenges. This could enable a realistic simulation of Botnet DDoS attacks, Phishing and other emerging Internet threats.

Another interesting development path could be developing the model implementation from the defender's point of view and creating some interaction between the attacker and defender. The behaviour of the attacker can be made more human with parameters like skill level and the style of attack. Even some chosen technologies from the artificial intelligence research could be used to enhance the simulation of how attacker discovers new vulnerabilities and makes choices during his attack.

References

Azgomi, Mohammad Abdollahi - Movaghar, Ali (2004) *Coloured Stochastic Activity Networks: Definitions and Behaviour*. 20th Annual UK Performance Engineering Workshop (UKPEW'04).

Carver, Curt - Surdu, John - Hill, John - Ragsdale, Daniel - Lathrop, Scott - Presby, Timothy (2002) *Military Academy Attack/Defense Network*. 3rd annual IEEE Information Assurance Workshop.

Chinchani, Ramkumar - Iyer, Anusha - Ngo, Hung - Upadhyaya, Shambhu (2005) *Towards a Theory of Insider Threat Assessment*. International Conference on Dependable Systems and Networks.

Ingols, Kyle - Lippmann, Richard – Piwowarski, Keith (2006) *Practical Attack Graph Generation for Network Defence*. 22nd Annual Computer Security Applications Conference (ACSAC'06).

Kiviharju, Mikko – Venäläinen, Teijo – Kinnunen, Suna (2009) *Towards Modelling Information Security wit Key-Challenge Petri Nets*. Lecture Notes in Computer Science, Proc. of NORDSEC, Vol. 5838/2009.

McGrath, Dennis - Hill, Doug - Hunt, Amy - Ryan, Mark - Smith, Timothy (2004) *NetSim: A Distributed Network Simulation to Support Cyber Exercises*. Huntsville Simulation Conference.

Möbius. http://www.mobius.illinois.edu retrieved 31.3.2010.

Opnet. http://www.opnet.com retrieved 12.4.2010.

Sanders, William (2009) *Möbius manual*, version 2.3, University of Illinois.

Saunders, John (2002) *Simulation Approaches in Information Security Education*. Proc. of 6th National Colloquium for Information System Security Education.

Sheyner, Oleg - Haines, Joshua - Jha, Somesh - Lippmann, Richard - Wing, Jeannette (2002) *Automated Generation and Analysis of Attack Graphs*. IEEE Computer Society, Proc. of the IEEE Symposium on Security and Privacy.

3. BUSINESS

ORGANISATIONAL SECURITY: FROM EXPERT KNOWLEDGE CONSTRUCT TO A BODY OF KNOWLEDGE

David J. Brooks
Security Research Centre (SECAU) from Edith Cowan University
d.brooks@ecu.edu.au

ABSTRACT - *Security is capricious in nature, with many practising domains and heterogeneous occupations. In addition, security can only be defined by its applied context. Such diffusion leads to a need to develop and present a consensual body of knowledge for the practising domain of Organisational Security; one domain of many parts of security. Organisational security may be considered, in part, that which provides security services and functions as a commodity within either public or commercial enterprises. There have been studies that have put forward a number of organisational security bodies of knowledge; however, there is still restricted consensus that is needed if we are to understand the future of organisational security.*

This study considered existing body of knowledge studies and puts forward a body of knowledge framework for organisational security, with integrated knowledge categories. In addition, further analysis was applied to this framework using a psychometric multidimensional scaling (MDS) knowledge mapping technique. The psychometric MDS mapping technique allowed implicit expert understanding of the framework and knowledge categories to be measured and interpretations made. Interpretations lead to an adjustment to the initial organisational security framework, resulting in a body of knowledge that better reflects organisational security experts' view of their practising domain and considered Security Science.

Introduction

The security industry is one of Australia's fastest growing sectors, generating revenues of approximately $4.5 billion per year and employing over 150,000 security personnel (Australian Security Industry Association, 2008). In a recent study, census figures for a ten-year period from 1996 to 2006 demonstrated that while the Australian population increased by 12 percent and the police workforce by 15 percent, the number of security providers grew by 41 percent (Prenzler, 2009, p. 3). However, *security providers* included many security occupations that would suggest that such comparison lacked some validity, an issue raised by Prenzler (2009, p. 4) which resulted in a more conservative figure of 26 percent.

Security has strong parallels with Defence, as they both provide protection; nevertheless, there are "disturbing differences" between these industries (Tate, 1997, p. iii). Defence, as with other related industries, are often considered to be *security*. An example may be the parallelism demonstrated through police and military organisations, with increasing convergence in their response to national security challenges (Ferguson, 2004). Such diverse and multidimensional approach to security cannot support the definition of security (Morley & Vogel, 1993), as ASIS International stated, "every time we think we've got the definition of the security field nailed, somebody … starts taking some of the nails away" (2003, p. 10).

Such diversity results in difficulty in providing a single encompassing definition for the many applied domains and heterogeneous occupations of security. Security cannot be considered singular in concept definition, as definition is dependent on applied context (Brooks, 2009b). A lack of concise understanding of security is becoming more significant, as the many practising domains of security such as public security, private security, national security, and private military security converge in the current social and political environment. As Zedner states "scholars have tended to think about security within their immediate discipline and in detachment from one another" (2009, p. 3).

Significance of the Study

There is an ever increasing reliance by both private and public sectors on private security, as public policing no longer has a monopoly on such services (Bradley & Sedgwick, 2009, p. 468), although it is as important to be able to provide an understanding and demarcation of security domains. However, there has been limited research in presenting an understanding of organisational security body of knowledge, with publications primarily by ASIS International (2003; 2009) and others (D.J. Brooks, 2009b; Hesse & Smith, 2001; Talbot & Jakeman, 2008). Therefore, the study provides a better understanding of a part of security, namely *organisational security*, its body of knowledge and its practicing knowledge categories. Organisational security is a multi-disciplined field and the identification of discrete knowledge categories could assist in better understanding a part of security.

Purpose of the study

The purpose of this study was gain a better understanding of one part of the multidimensional domain of security, in particular, the group who provides a significant portion of applied security within our society. The study addressed a number of discrete objectives, namely:

1. What knowledge categories are most relevant for the practising domain of organisational security?
2. Can a singular body of knowledge framework be developed for the practising domain of organisational security?

Material and Methods

The study design was divided into two discrete phases (Figure 1). The first phase critiqued existing body of knowledge studies to develop an integrated framework of organisational security. The second phase tested this integrated framework using psychometric multidimensional scaling (MDS) knowledge mapping and from this analysis, produced a final integrated framework.

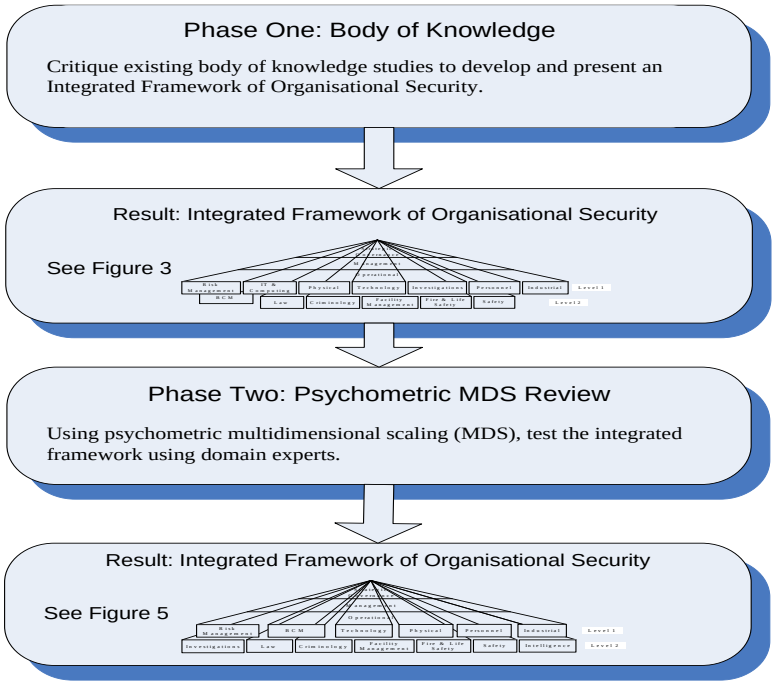


Figure 1. Study design.

The second phase of the study, namely the psychometric multidimensional scaling (MDS) knowledge mapping, used a web based survey instrument embedded with a number of security knowledge categories. Non-probabilistic peer selected expert participants (n=27) made up the study's sampling group. In general, the participants consisted of people operating in private or public organisations at a managerial or executive level within their corporation's security group or were academics researching the security industry. Participants selected, on a sliding scale, how similar or dissimilar they considered *pairs* of knowledge categories (Figure 2). Data were extracted from the completed survey's, summed and inserted into Excel, considered the *source document*. At this point, validity and reliability measures were applied on the source data and multidimensional scaling analysis applied.

when compared to			Similar	1	2	3	4	5	6	7	8	9	10	Dissimilar
Security		Security management												
Security		Physical security												
Security		Security technology												
Security		ICT												

Figure 2. Sample of the MDS survey instrument.

The underlying theory of the study used interpretative analysis, where existing security body of knowledge studies were considered and expanded. In addition, psychometric multidimensional scaling (MDS) knowledge mapping technique (D. J Brooks, 2009a) was incorporated, presenting a spatial experts' representation of organisational security knowledge structure.

Knowledge categories

Knowledge may commence with object and pattern recognition; nevertheless, this does not provide an appropriate explanation to define knowledge. Knowledge is constructed and built on previous experience by using and expanding existing ideas (Novak & Gowin, 1984). Therefore, it can be stated that as new knowledge is gained, change in understanding existing theories may be achieved. Nevertheless knowledge is integral to memory structure, concerned with how the memory may organise, store and retrieve such knowledge. As a person is exposed to information in their everyday life, concurrent knowledge has to be economised and abstracted into what are defined *knowledge categories*.

These knowledge categories are developed and maintained within long-term memory; however, there is a cognitive balance between the number and effectiveness of such categories. Categories need to be *informative*, based to a degree on the natural world, economic and cohesive (Eysenck & Keane, 2002), and organised (Kellogg, 2003). Similar objects are grouped together within a conceptual category and these groupings are generally a product of the learner's environment.

Multidimensional scaling

Multidimensional scaling (MDS) is a statistical technique within the area of multivariate data analysis, "attracting worldwide interest" (Cohen, Manion, & Morrison, 2002, p. 369) and has been used in many other similar studies (Cox & Cox, 2000). MDS operates by reducing complex dimensional data and presenting such data as a spatial representation, allowing hidden data structure formation. MDS commences with a set of objects that are paired and their dissimilarities measured, with configurations of points sought in dimensional space and each point representing as an object. MDS calculates a dimensional space configuration where the points match, as close as possible, to the paired dissimilarities. Dimensional representation demonstrates object proximity, with proximity being how similar or dissimilar objects actually are or perceived to be (Cox & Cox, 2000; Kruskal & Wish, 1978). Such a technique results in a spatial representation of knowledge concept clusters (Trochim, Cook, & Setze, 1994).

Phase One: Organisational Security Body of Knowledge

The study critiqued existing body of knowledge studies that focused on what could be considered organisational security. These studies included an introductory course in organisational security (Nalla, 2001), Integrated Framework of Organisational Security (D.J. Brooks, 2009b), Security Risk Management Body of Knowledge (Talbot & Jakeman, 2008) and ASIS International Symposiums (ASIS International, 2009).

Nalla (2001) explores the core components of an introductory course in organisational security, where nine security topics were ranked important (Table 1) drawn from benchmarking security text-

books, security professional's interviews and proceedings of the ASIS first academic/practitioner symposium. The study emphasised, to a lesser degree, the consensus on the conceptual and methodological components of security education such as fire safety, workplace violence and workplace drug use. However, this study is considered too narrow in approach and lacking core and relevant knowledge categories put forward by others, such as Brooks (2008; 2009b), ASIS International (2009), and Talbot and Jakeman (2008).

Table 1. *Components of an introductory survey course in organisational security. (Nalla, 2001, p. 49)*

Component's description	
Physical security and asset protection	Access control management
Emergency and incident management	Risk assessment and management
Personnel security	Investigations
Legal issues	Information security
Computer security	

Brooks (2008; 2009b) investigated and critiqued 104 security related undergraduate security courses from Australia, South Africa, United Kingdom and United States. From this critique, seven courses were selected for in-depth course content analysis using Linguistic Inquiry and Word Count (Pennebaker, Francis, & Booth, 2001). This analysis resulted in 2001 security concepts being extracted, with the 14 more implicit concepts considered knowledge categories (Table 2). In addition, this study used other related body of knowledge studies (American Society for Industrial Security, 2002; Bazzina, 2006) to support and valid these security related knowledge categories.

Table 2. *Organisational security knowledge categories. (D. J. Brooks, 2008, p. 19)*

Security categories description		
Criminology	Business continuity management	Fire science
Facility management	Industrial security	Information &computer
Investigations	Physical security	Security principles
Risk management	Safety	Security law
Security management	Security technology	

From the 14 knowledge categories (Table 2) a proposed *integrated framework of organisational security* (Figure 3) was developed. The framework considered the breadth of organisational security, opposing many past studies that have presented a narrow approach to the diverse role of organisational security, such as Kooi and Hinduja (2008). Such breadth was supported by Yates (2007) when he stated that traditional security categorisation does not consider the large range of security related functions, including business continuity, emergency response, information security and risk management. As the integrated framework indicates, Level 1 security knowledge categories comprises of risk management, IT

and computing, physical security, security technology, investigations, personnel and industrial security. Business continuity management may be considered a subordinate concept or risk mitigation strategy of risk management. Level 2 was considered an allied or supporting disciplines or practising domains.

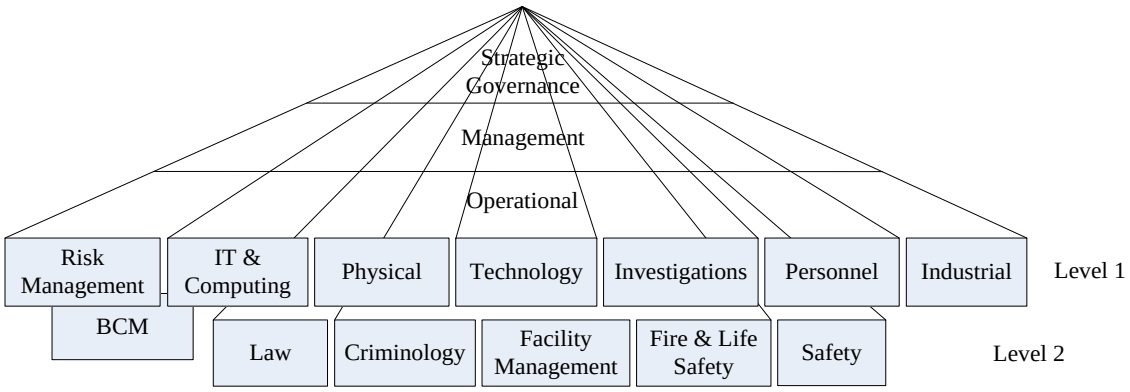


Figure 3. Proposed integrated framework of organisational security. (D.J. Brooks, 2009b).

Note: BCM = Business Continuity Management, comprising of crisis, emergency and business recovery

ASIS International (2009) academic/practitioner symposium continues to develop a security body of knowledge. The most recent 2009 symposium attempted to gain an understanding of the security body of knowledge, understand what disciplines security may extract its knowledge categories from, what knowledge categories are core, how can these knowledge categories be used and to consider if consistency and consensus can be gained? In addition, a list of 18 knowledge categories was put forward as the symposium's security model (Table 3).

Table 3. ASIS International Symposium security model. (ASIS International, 2009)

Security model		
Physical security	Personnel security	Information security systems
Investigations	Loss prevention	Risk management
Legal aspects	Emergency/continuity planning	Fire protection
Crisis management	Disaster management	Counterterrorism
Competitive intelligence	Executive protection	Violence in the workplace
Crime prevention	CPTED	Security architecture & engineering

Phase one has put forward the most current studies into organisational security bodies of knowledge. Such studies assist our understanding of this security domain; however, further analysis had to be applied to consider underlying knowledge categories and their interrelationships.

Phase Two: Expert Knowledge Structure

Phase two tested the security knowledge categories and integrated framework in an attempt to measure how relevant these were according to security experts. The study analysis and following interpretation of the source data resulted in a spatial multidimensional scaling (MDS) map of the participating experts' knowledge structure (Figure 4). There were some interesting aspects to the spatial locality of some of the organisational security knowledge categories, such as *investigations*, the cluster of technology categories, the relationship of *risk management* and *business continuity management*, and locality of *industrial security*. What was expected was the central locality of *security*, being the most abstract and ordinate knowledge category

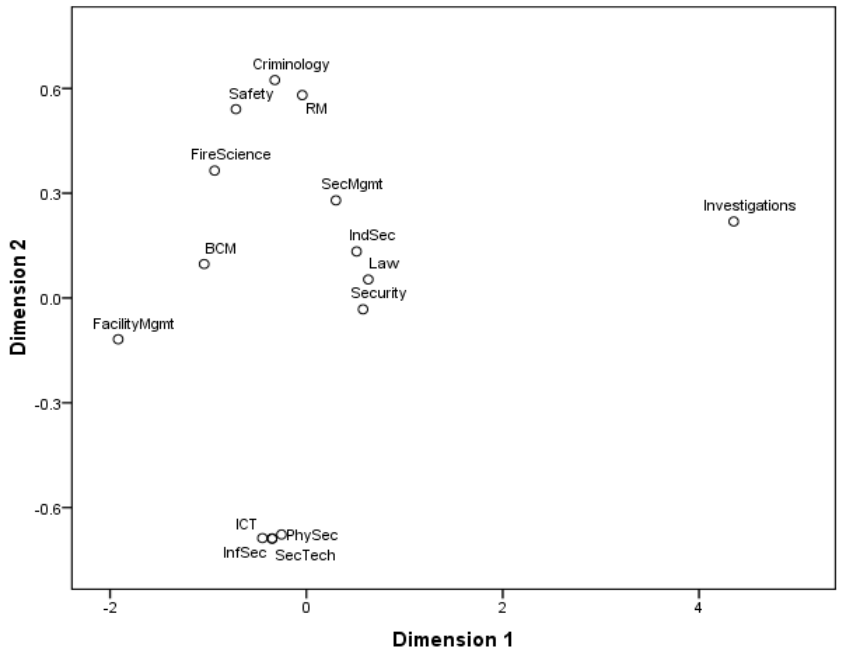


Figure 4. *MDS expert knowledge structure of organisational security. (SSTRESS1=0.222; 0.992 Cronbach Alpha).*

When considering Figure 4, the categories of *security* and *security management* were both located relatively central in respect to the other knowledge categories, indicating more abstract and central ideas. In addition, the categories of *law* and *industrial security* were located between these two categories. Why *law* was located in such a locality would require greater research, perhaps with greater in-depth interviews with the expert participants. However, it is postulated that law may be spatially located at this point because it is a fundamental principle by which society and its members exists, and is therefore a foundation for security. Nevertheless, the locality of industrial security appeared to indicate that this category was not clearly understood in respect to definition, supported by such comments from the participating experts.

The technology categories of *physical security, security technology, ICT* and *information security* were spatially clustered, indicating similarity of concepts and that these functions are closely related.

Nevertheless, it was proposed that *information security* was not necessarily a technology category, related more to *security management* as a procedural function. As Talbot and Jakeman (2008) states, the knowledge category *information* and *computer* should be divided into two discrete categories, namely *information security* and *information communications technology* (ICT); however, according to the MDS knowledge structure these were viewed as similar categories and should perhaps remain as one knowledge category.

Investigations was found to be an outlier, relatively separated from the other knowledge categories. Based on this locality, it could be suggested that investigations is not a significant knowledge category of organisational security. Finally, Figure 3 put forward that *risk management* and *business continuity management* (BCM) would be similar and therefore clustered. Nevertheless MDS placed these two categories relatively apart from each other, indicating that these categories as quite discrete functions (Table 3).

Table 3. Interpretations of MDS knowledge structure.

Knowledge category	MDS interpretation
Security	Central location due to its ordinate position
Security & security management	Only some degree of cluster, indicating discrete categories
Industrial security	Located between security and security management, indicating no clear category definition
Investigations	Spatial outlier, indicating that this is not a core category
Physical, ICT, information security & security technology	All concepts clustered, indicating a common knowledge category
Information security	Clustered with technology, indicating that this should be integrated with Computing & Information Technology
Risk Management & BCM	Spatial separation, indicating distinct functions

Integrated Framework of Organisational Security

Reflecting from the interpretations of the MDS knowledge structure of organisational security (Figure 4), the integrated framework of organisational security (Figure 3) was adjusted. Adjustments to the framework included the relocation of *business continuity management* to Level 1 and *investigations* to Level 2. The categories of *security technology* and *information technology and computing* were integrated into a single category of *security technology*. From discussions with the participating experts, it was suggested that *security intelligence* should be included as a supporting organisational security category. Adjustments to Figure 4 resulted in the final integrated framework of organisational security (Figure 5), considered *Security Science*.

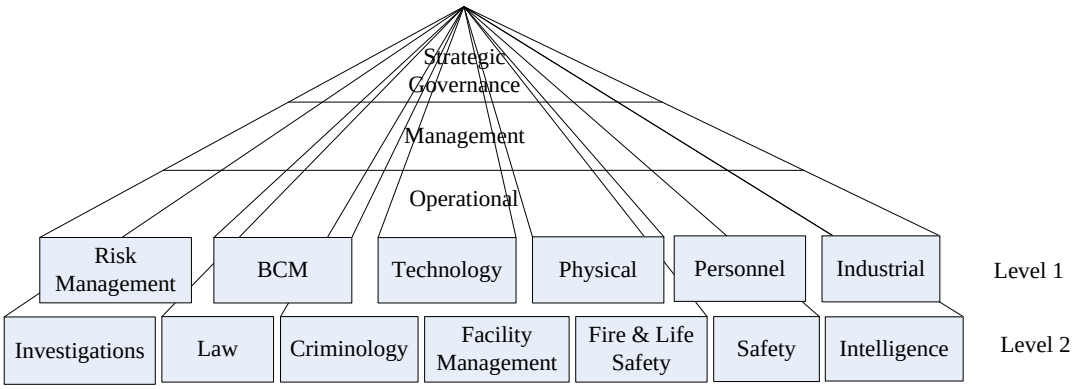


Figure 5. Integrated framework of organisational security or Security Science.

Notes: BCM = Business Continuity Management; Technology = security technology, information technology and computing

The ASIS International body of knowledge (ASIS International, 2009) security model (Table 3) further supported the inclusion of many of the study's defined categories and to some degree, the integrated framework of organisational security (Figure 5). For example, Business Continuity Management (BCM) encompasses the security model's categories of emergency/continuity planning, crisis management and disaster management categories. Therefore, from the 18 proposed categories from the ASIS International security model, five categories are presented in Level 1 and three are in Level 2. Nevertheless, it is argued that the ASIA International security model categories such as crime prevention through environmental design (CPTED), crime prevention and counter-terrorism are tasks or functions embedded within the prescribed knowledge categories.

Conclusion

There is still future study required in gaining consensus in knowledge category definition and an organisational security body of knowledge; however, it could be suggested that both are required to achieve the other. Continued research with similar studies being completed by such groups as ASIS International and the development of national and international standards will ultimately result in such common understanding. In addition, organisational security has to have a clear understanding of its operating boundaries, from which further consensus in a body of knowledge will be achieved. There are many overlapping and defuse security domains that interact, interrelate and have independencies with organisational security, such as public policing, national security, military security and private security, to name a few.

Security is diverse and multidimensional in nature and practice. Such diffusion results in the need to define various operational parts of security, achieved to some degree through a body of knowledge. The study put forward an integrated body of knowledge framework of organisational security (Figure 5), developed from core security knowledge categories and with integration from previous body of knowledge studies. The study used multidimensional scaling (MDS) to present a spatial knowledge structure of the participating security experts. Such a knowledge structure allowed the implicit expert understanding of

the security categories to be analysed, displayed and interpretations made, resulting in a number of category interrelationships.

There will be a degree of overlap between the knowledge categories, as they are not hierarchical or applied in isolation. The study considered the need to present a practical and industry focused organisational security consensual body of knowledge, considered *Security Science*. It is suggested that the study outcomes could further improve the comprehension of the practising domain of organisational security and support the advancement of this security profession. Nevertheless, the diversity of organisational security mandates interdisciplinary studies to sum competencies under each knowledge category.

References

American Society for Industrial Security. (2002). *Proceedings of the 2002 academic/practitioner symposium*. The University of Cincinnati, Ohio: ASIS International.

ASIS International. (2003). *Proceedings of the 2003 academic/practitioner symposium*. The University of Maryland, Maryland: ASIS International.

ASIS International. (2009). Security body of knowledge (BoK): substantive considerations. Unpublished ASIS International Academic/Practitioner Symposium 2009, ASIS International.

Australian Security Industry Association. (2008). Security industry overview. Retrieved 2 September, 2008, from http://www.asial.com.au/default.asp?page=%2Fconsumer+information%2Fsecurity+industry+overview

Bazzina, M. (2006). *Security standards and support systems report: A collaborative project between the Commonwealth Attorney-General's Department and Standards Australia*. Sydney: Standards Australia International Ltd.

Bradley, T., & Sedgwick, C. (2009). Policing beyond the police: A "first cut" study of private security in New Zealand. *Policing and Society*, 19(4), 468-492.

Brooks, D. J. (2008). Defining the science of security through knowledge categorisation. *Acta Criminologica, CRIMSA Conference Special Edition 2008*, 1, 12-23.

Brooks, D. J. (2009a). *Key concepts in security risk management: A psychometric concept map approach to understanding*. Saarbrucken: VDM Verlag.

Brooks, D. J. (2009b). What is security: Definition through knowledge categorisation. *Security Journal, DOI 101057/sj.2008.18*, 1-15.

Cohen, L., Manion, L., & Morrison, K. (2002). *Research methods in education* (5th ed. ed.). London: RoutledgeFalmer.

Cox, T. F., & Cox, M. A. A. (2000). *Multidimensional scaling: Monographs on statistics and applied probability* (2nd ed. ed. Vol. 88). Boca Raton: Chapman & Hall/CRC.

Eysenck, M. W., & Keane, M. T. (2002). *Cognitive psychology: A student's handbook* (4th ed.). New York: Psychology Press Ltd.

Ferguson, G. (2004, August). Homeland security: Emerging technologies: Policing conference returns to Adelaide. *Australian Defence Magazine,* 12, p. 54.

Hesse, L., & Smith, C. L. (2001). Core curriculum in security science. *Proceedings of the 5th Australian Security Research Symposium* pp. 87-104).

Perth, Western Australia.

Kellogg, R. T. (2003). *Cognitive psychology* (2nd ed. ed.). Thousand Oaks: Sage Publications.

Kooi, B., & Hinduja, S. (2008). Teaching security courses experientially. *Journal of Criminal Justice Education,* 19(2), 290-307.

Kruskal, J. B., & Wish, M. (1978). *Multidimensional scaling* (Vol. 07). London: Sage Publications.

Morley, H. N., & Vogel, R. E. (1993). The higher education dilemma for the private security professional: Delivery methodologies and core curriculum from the practitioner's perspective. *Security Journal, 4(3)*, 122-127.

Nalla, M. K. (2001). Designing an introductory survey course in private security. *Journal of Criminal Justice Education*, 12(1), 35-52.

Novak, J.D., & Gowin, D. B. (1984). *Learning how to learn*. Cambridge: Cambridge University Press.

Pennebaker, J. W., Francis, M. E., & Booth, R. J. (2001). *Linguistic inquiry and word count (LIWC2001)*. Mahwah, NJ: Erlbaum Publishers.

Prenzler, T., Earle, K., Sarre, R. (2009). Private security in Australia: trends and key characteristics. Trends and Issues in Crime and Criminal Justice, no. 374 [Electronic Version]. Retrieved 11 August 2009, from http://www.aic.gov.au/publications/tandi/tandi374.html

Talbot, J., & Jakeman, M. (2008). *SRMBOK: security risk management body of knowledge*. Carlton South: Risk Management Institution of Australasia Ltd.

Tate, P. W. (1997). *Report on the security industry training: Case study of an emerging industry*. Perth: Western Australian Department of Training. Western Australian Government Publishing.

Trochim, W. M., Cook, J. A., & Setze, R. J. (1994). Using concept mapping to develop a conceptual framework of staff's views of a supported employment program for individuals with severe mental illness. *Journal of Consulting and Clinical Psychology*, 62(4), 766-775.

Yates, A. (2007). *The future of private security*. Canberra: Australian Homeland Security Research Centre.

Zedner, L. (2009). *Security: Keys ideas in criminology*. London: Routledge.

INSIGHTS INTO THE DEVELOPMENT OF THE SECURITY BUSINESS: TOWARDS INCREASING SERVICE ORIENTATION

Reeta Hammarén[a], Arto Kangas[a], Anna Multanen[a], Mervi Murtonen[b], Arto Rajala[a], Risto Rajala[c] and Mika Westerlund[a1]
[a]Aalto University, School of Economics, Department of Marketing and Management
[b]VTT Technical Research Centre of Finland
[c]Aalto University, School of Economics, Department of Business Technology

ABSTRACT *– The security industry provides us with novel and interesting examples to analyze the service orientation of companies providing business-to-business security services. Our study draws on a qualitative research approach to investigate the manifestation of service orientation in security companies. The study reveals that although the dominant business logic in the security industry has previously relied on product-oriented offerings, many firms increasingly emphasize service-dominant logic over product-dominant logic in their security solution business. Such service orientation spans over several aspects of the business models of the security firms and goes far beyond their offerings.*

Introduction and Background

Security business has its origins in services. Already a century ago, night watchmen and security guards were protecting the safety of the citizens in the cities of central Europe. In addition, in-house security officers were common in industrial companies of that time (de Waard, 1999.) In today's highly competitive business environment, we are witnessing the re-birth of services, and industrial firms including security companies are increasingly integrating services into their product offerings. This trend is spurred by factors related to economic considerations (higher margins, incremental and more stable revenues offered by services), customer expectations (customers' increasingly complex needs and wants, and higher requirements) and intense competition (Gebauer 2009; Oliva and Kallenberg 2003). Especially, Homburg et al. (2003) argue that in today's competitive landscape one of the few ways left for firms to differentiate from competitors is by offering value-added services.

As suggested by Vandermerwe and Sada (1988) modern companies are increasingly offering fuller market packages or "bundles" of customer-focused combinations of goods, services, support, self-service, and knowledge. This movement is termed the "servitization" of business. One of the main motives driving companies towards servitization is that it leads to new relationships between them and

[1] The authors' names are in alphabetical order

their customers. Oliva and Kallenberg (2003) stress that recent studies almost unanimously recommend product manufacturers to integrate services into their product offerings, and Jacob and Ulaga (2008) support the view that industrial manufacturers are developing value-adding services in order to sustain competitiveness and long-term growth. On the other hand, Nijssen et al. (2006) point out that in new service development the company's willingness to cannibalize organizational routines and prior investments is more important than the R&D-related strengths. This indicates that companies need to unlearn from the traditional R&D capabilities and develop a new mindset to gain success in more service-oriented business.

The augmented service orientation in firms is seen as an indication of the so-called service dominant logic. Lusch et al. (2007) signify that the primary focus in service dominant logic is on the exchange of specialized competences between the service supplier and the customer. In this vein, the service-oriented view of business is customer- and market-driven. This means that a service-oriented company is constantly learning from customers and adapting to their dynamic needs. However, service orientation has been mainly studied at the level of employees among the service staff (e.g. Cran 1994) and prior investigation into service orientation at the level of organizations especially in the b-to-b setting (Homburg et al. 2002) is almost exiguous.

Previously, security has been studied within several research streams. These include, e.g., criminology (Armitage and Pease 2007), sociology (Zedner 2003), international political studies (Wolfers 1952; Baldwin 1997), economics (Brück et al. 2008) and technological studies (Rouhiainen 2009). Thus, security environment, as well as preconditions and solutions for organizational security are well covered in an extant literature, but a thorough analysis of a supplier–customer relationship in business-to-business security services seems to be lacking in current research. One of the few studies that take the customer perspective on security is that of Ian Loader's (1999) who studies the consumerism of public and private security services. In spite of its absence in extant academic debate, privatized security is one of the most fast growing businesses in Europe and security services are under active development worldwide (de Waard 1999). This has also caused criticism against the ever-spreading "securitization" and the replacement of public policing with private security services (see e.g. Zedner 2003). In the light of all these notions, security services are presented as an interesting and current research topic.

This study strives to fill the aforementioned research needs by investigating *how the service orientation is manifested in the security firms' business models*. We take a service research approach to security and focus our study on business-to-business security services and the service orientation of the security suppliers. We focus our study on private security industry that aims at preserving the security of persons, information and property using both manpower, alarming and surveillance technologies (de Waard 1999). As the relationships between business models and service operations in security companies have not yet been fully revealed, a qualitative research approach, built on a thorough literature review and rich data was an obvious choice for this study. Rather than testing a pre-determined hypothesis, we aim at generating new descriptions and categorizations for the private security business from the perspective of service research. The data were collected through semi-structured interviews with the managers in these companies. In addition, we analyzed an extensive set of secondary material on security service business.

This paper is structured as follows: First, we introduce the concept of organizational service orientation as the focus of the research and the business model of a firm as the level of analysis. We use these concepts in our investigation of transition towards increased service orientation in the security industry. Then, we present the research setting, methodology and the empirical findings. Finally, we discuss the findings and conclude the paper with suggestions for further research.

Service orientation as the focus of research

The service dominant view on strategic management has gained ground in diverse business fields. In their seminal paper on the service-dominant business logic (SDL), Vargo and Lusch (2004) advocate the shift towards increasing service orientation in contemporary business. According to them, goods-dominant logic has been the prevalent logic in the markets, but over the past decade increasing competition has forced industrial manufacturers to adapt a more service-oriented perspective to business. While the traditional goods centered view is based on the exchange of tangible goods, the service-dominant logic focuses on intangible resources and co-creation of value (Vargo and Lusch 2004; Lusch et al. 2007). Hence, the dominant logic of doing business is shifting away from the exchange of manufactured goods towards the exchange of intangible aspects such as professional know-how and specialized skills. Moreover, Vargo and Lusch (2004) underscore that value is co-created by service providers and customers rather than received from the use of tangible outputs. Prior studies suggest that the service-oriented view is a business strategy that can be adapted to any market offerings (Vargo and Lusch 2008), even in the business-to-business context (Homburg et al. 2002).

Academic literature by and large lacks an exact definition of organizational service orientation. One of the few exceptions is provided by Homburg et al. (2002), who conceptualize the service orientation of an industrial firm's strategy in terms of two dimensions: (1) the number of services offered, and (2) how strongly these services are communicated to customers. Much of the academic literature on service orientation focuses, without more precisely defining the concept, on analyzing the extent of service orientation in firm's business strategy (Gebauer 2009; Antioco et al. 2008; Lytle et al. 1998; Berthon et al. 1999). For example, Gebauer (2009) categorizes manufacturing companies into those with high service orientation and those with low service orientation. According to Gebauer (ibid.), the former group heavily emphasizes services in their business strategy and operation, whereas the latter group focuses the role of product in their value propositions and receives their profits and revenues mostly from the product offerings.

Service orientation is intertwined with the company's business model. In concordance with Hombug et al. (2002), Rajala (2009) suggests that an organization's service orientation can be determined upon the extent to which (1) the firm's marketing strategy emphasizes the importance of customer service, (2) the firm's solutions are sold as services, (3) services constitute a source of competitive advantage in the firm's business, (4) the firm responds to customer needs through service, (5) the organization structure supports the realization of service, (6) the organization culture is service-centered, and (7) the company's information systems support the service activity. Furthermore, Hombug et al. (2002) stress that the realization of service orientation in business necessitates a number of other organization-related factors, such as the human resource management. All these measures of service orientation actually comprise the business model elements of the firm. Thus, we argue that the shift towards increasing service orien-

tation should be analyzed through the framework of firm's business model as it covers the crucial aspects of company's every-day business and manifests the realization of its business strategy.

Business model as the level of analysis

Business model offers a viable concept for the analysis of service orientation at the firm level. This is because firms promoting service orientation in their business embody changes far more than merely accentuating the share and role of services in the company's offering or value proposition. That is, the change towards more service-oriented business necessitates changes on all aspects of the firm's business model. This is consistent with the notion of Oliva and Kallenberg (2003), who state that "*not only are new capabilities, metrics and incentives needed, but also the emphasis of the business model changes from transaction- to relationship-based*". Also other authors (e.g., Homburg et al. 2002) state that increasing firm's service orientation requires changes in several organizational factors.

The concept of the business model of a firm has reached a position as a strategy-based (Rajala and Westerlund 2007) "thought-focusing device", a pertinent notion in the managerial vocabulary (Shafer et al. 2005; Tikkanen et al. 2005). It includes the key components of a company's every-day business, and embodies the fundamental processes of value creation and value capture underlying the business (Möller et al. 2008; Chesbrough 2007). Although the two concepts – business model and strategy – are sometimes used interchangeably, it should be noted that business model is not the same as strategy (Shafer et al. 2005; Magretta 2002). Instead, business model is a reflection and a result of the strategy, and a way to implement it. In other words, business model is a conceptual and theoretical layer between firm's strategy and operations (Rajala and Westerlund 2007). We also argue that a clearly defined business model can help the company to create 'mindsets' and foresight in order to cope with future (cf. Naisbitt 2006).

Following the conventions of the previous literature that often defines business model through the value-creating components it includes (see e.g., Morris et al. 2005), we define business model as *"a concise representation of how an interrelated set of components – the offering, relationships, resources, revenue model and management mind-set – are addressed to create value in defined markets"*. (Multanen 2009) further characterizes these components to represent the most important aspects of the business, and, hence, the business model of a firm. Each of these key components is discussed in more detail in the empirical section of the study, with examples and illustrations from the security service business.

Material and Methods

This paper adopts a qualitative study approach to investigate service orientation in security companies. Our conceptual framework was developed on the basis of a literature review. To illustrate this framework, we conducted interviews with the top managers and line managers in several Finnish security service firms. In addition, we analyzed an extensive set of secondary material on these companies and the industry. All of the interviews support the view, that there is an ongoing shift towards increased service orientation in the security service business, with some companies taking more drastic competitive repo-

sitioning in the market, whilst others developing their offerings to a lesser extent. Through the interviews we can illustrate how changes in the service orientation transcend the boundaries of the security service offerings, covering the key aspects of the business models of the case companies. That is, in addition to analyzing the offerings, the investigation covers the companies' revenue models, resources and relationships as well as the management mindset.

Large data[2] were collected in 2009 from three types of security service firms. For the purpose of this paper, we chose a handful of companies for analysis. Two of the firms are security systems suppliers and one focuses on traditional guarding and other security services. Two firms provide security-related products and support services such as maintenance and training. The turnover of the firms ranged from about 1.5 million to 50 million Euros in 2008.

Yin (1994) emphasizes that a reliable empirical study requires multiple sources of evidence, a sufficiently operational set of measures, and internal and external validity. To this end, Denzin (1978) recommends triangulation as a way of improving the reliability and validity in social research. Data triangulation uses multiple sources and types of data to investigate the research question. In this study, we collected data from several informants in the case companies (semi-structured in-depth interviews) and used secondary data (documents, reports, etc.) from the same companies as support. Some observation data was also collected from a number of meetings and workshops arranged with the participating companies. Investigator triangulation involves multiple researchers in an investigation. In the present study, this was addressed both in the data collection and in the analysis phase when separate researchers in the research team scrutinized the qualitative data to cross-check and verify the findings.

Observations on the security service business models

In this section, we investigate the security service providers' business models through five cases in the private security service business. Due to confidentiality issues the cases are only identified as Cases A to E. As defined earlier, the subjects observed include the offerings, relationships, resources, revenue model and management mindset that are perceived as the elements of the business models of companies providing security services.

Towards new security business models

Business models of industrial firms concurrently undergo a shift towards increased organizational service orientation. In general, Oliva and Kallenberg (2003) suggest that the transition from products to services in firms occurs in stages. That is, the business logic of such firms evolves gradually into a more customer-driven and service-oriented operation. In our data, the security systems suppliers are witnessing a somewhat similar transition, as highlighted with the following excerpt of the interviews:

> *"Our company provides security systems and related services that are valuable to our customers. --- We have a long history as an equipment supplier --- starting from maintenance ser-*

[2] This data collection was a part of a research project ValueSSe (The Value of Corporate Security Services) carried out by Aalto University and VTT (Finnish Technical Research Central)

vices in 1990s --- we have changed gradually towards more service-oriented operations in the 2000s. --- However, we still have a long road ahead." (Case A"

Although the security industry has traditionally focused on guarding services, automation and technology such as video surveillance has over time transformed the industry logic. Our data indicates that the service logic of the security industry is twofold. On one hand, the companies that have a tradition of providing guarding services are searching for new service concepts and offerings, and are chasing more value-adding services. On the other hand, the business logic among the security systems suppliers is also shifting in favour of providing more comprehensive solutions to customers. The view surfaced in our interviews:

"We do not focus on the overhaul of security systems but on 'maintaining' the customer relationship." (Case A)

The service-dominant transition of business models, along with its increasing customer focus, which is ongoing in many industries at the present, seems obvious also in the security service business. However, the change carries many features that have been previously unknown to the industry. Next, we illustrate the various changes in more detail within business models of the firms that have accompanied the shift towards increased service orientation.

Offering

Offering as a business model element refers to products, services and solutions offered to the market to satisfy customers' specific needs and wants (Westerlund et al. 2008). This component, also described as the firm's product/service offering (Rajala and Westerlund 2007; Morris et al. 2005) or value proposition (Chesbrough 2007; Linder and Cantrell 2000), emphasizes the company's decisions on the nature and role of what it offers to the customers, such as the degree of the customization (i.e. standardized or customer-specific) (Westerlund et al. 2008), depth and breadth of the product/service mix (Linder and Cantrell 2000), the role of the firm in service production or service delivery, and how the service is made available to the customers (Morris et al. 2005).

Mathieu (2001) recognizes two distinctive strategies that service providers can utilize: services that support the products (SSP) and services that support the client's actions (SSC). Our data reveals that providers in the contemporary security service business execute both of these strategies. Some security service providers focus more on offering products, and services are additional supporting the implementation and use of those products. In the security service business such services include, e.g., training, maintenance and repair. However, as the following excerpts from our interviews reveal, security businesses are increasingly merging their products and services into more comprehensive total offerings or solutions where services have an integral role:

"Our company offers security service solutions. Our focus is to be even more service oriented in the future." (Case C)

"We aim at providing more comprehensive solutions that increasingly include service components. --- The objective is that the clients need to focus their efforts on security issues." (Case E)

Technology has had a major impact on business and society during the previous century. Our interviews illustrate that companies whose main offerings have consisted of "traditional security services"

such as guarding have started to utilize the latest technology more effectively, resulting in novel service solutions that comprise technology-driven products and services. That is, the increased technology usage may help the service providers to serve their customers more efficiently and to be more flexible with regard to technological uncertainty. Moreover, service coverage can be significantly increased with the help of ICT and other technology, including remote operated camera and 24/7 based surveillance services, as well as wireless emergency alarms and buttons, and even security service related robotics as in the case of Japan. Our interviews clearly show that the role and importance of technology in security business is rising:

> *"Our key business idea is to assist our clients in developing their core businesses. This is pursued through providing security services. A significant part of the security services consists of technology." (Case B)*

Moreover, our data highlight that the investigated security service providers' business models comprise ever more comprehensive and customer-specific offerings and integrated security service solutions.

Resources

Resources constitute a fundamental factor in strategic business decisions (Barney 1991). Betz (2002) investigates resources by differentiating between two forms of resources: tangible and intangible. Firms' resources can be defined as assets and capabilities that are needed to develop and implement a given business model (Rajala and Westerlund 2007). Morris et al. (2005) describe resources in terms of firm's internal source of advantage, 'the core competency', and Linder and Cantrell (2000) as firm's 'distinctive capability'. These concepts can be used to investigate firm's skills or capabilities in developing and delivering specific benefits to customers through service.

> *"All our activities are premised on the basis of trustworthiness. That is, our key qualities and competitive advantages consist in credible processes and we need to be convincing about our resources in providing our customers with security." (Case C)*
>
> *"We aim at providing our customers with comprehensive services based on our internal resources and capabilities." (Case E)*

On the other hand, the service-dominant view emphasizes resource access over resource ownership in the service business. This perspective calls for investigation of resources in relation to other business model elements, such as relationships. Our observations support this view:

> *"We meet the customers' expectations about security through our close collaboration with the clients. --- We will help our customers throughout the lifecycle of the long-term relationship." (Case A)*

The security service industry has been considered as low-level education business environment and significantly the standard of service know-how is somewhat low. Increased service orientation necessitates changes in required skills and expertise. Security service providers are developing/improving their business relationships in order to fulfill and complete their offerings. The use of partners from multiple heterogeneous business fields enables security service providers to offer a more extensive service package. Our interviews indicate that some of the case companies recognize there are important resources and specialization in their partner network consisting of different actors in the security service business.

Another issue that surfaced in the interviews is that almost none of the security service providers use marketing communications to support their sales. For example, security industry magazines and other security-related publications are the main channels used for advertising. Professional direct-mail advertising and specialized market research analysts seem to be an almost untapped resource among the interviewed companies.

Relationships

Relationships in the business model context underscore the value-creation process between the service provider and its clients. More specifically, relationship component attends to the entire network of the firm's social and inter-organizational relationships, including organizational processes and activities (Tikkanen et al. 2005; Betz 2002) as well as the organizational structure (Linder and Cantrell 2000). Relationships in service oriented business models provide an important perspective to understand the roles of different business actors and their contributions to the service provision. The roles include, for example, service component providers, system integrators, end-users' maintenance suppliers, independent service providers and other relevant contributors (Oliva and Kallenberg 2003). Our findings underscore that increased service orientation creates challenges to the whole network of business actors:

> *"We have discussed a lot about daily issues with our customers --- but we need to go further in developing the security solutions together." (Case A)*
>
> *"We had better let our partners focus on their core competencies. We serve them in other important issues. That is, the customers need not to be out there alone." (Case B)*
>
> *"Networking with our partners is the key to growth in this business." (Case D)*

The trend towards tighter customer relationships is shown in the way security service providers describe their value propositions. Our findings highlight that all the essential business operations in the security business are governed by an outcry for trustworthiness. Security service firms provide their customers with the feelings of security, safety, problem-solving, short response times and credible operation and cost efficiency. Our data reveals that the service providers are willing to offer more extensive partnership agreements than what the clients are willing to adopt. Hence, the service providers constantly attempt to train their customers and partners to understand the benefits of accepting more comprehensive services and total solutions, and themselves listen to their customers in pursuing to learn and co-create solutions for emerging customer needs.

Revenue model

Revenue model specifies the ways to appropriate value for the company (Chesbrough and Rosenbloom 2002). Usually this business model component is discussed in terms of revenue sources, pricing policy, cost structure and profit potential (Rajala and Westerlund 2007; Pateli and Giaglis 2003; Chesbrough and Rosenbloom 2002). The first two of these involve determining the different pricing options (e.g., value-based, market-based, or competition-based prices) as well as the modes of transactions (e.g., subscription payments). Moreover, cost structure, which refers to the operating leverage, margins and volumes (Morris et al. 2005) is an important aspect of any service-based business model. Our empirical

findings underscore that the revenue models in the security business are increasingly based on service contracts where the pricing is considered in a case-specific manner:

> *"Security has no price as such. The price is jointly agreed with the customer. We only are taking the first steps to assess the value of security for our customers. --- In my opinion, there are two underlying grounds [for customer and value-specific pricing] --- first, it is uneasy to quantify the value of safety. Second, although some aspects of the value can be measured –such as the costs of damages or mishaps– there are important aspects that are extremely difficult to quantify. These include the state and feeling of safety." (Case C)*

The previous excerpts suggest a significant change in the pricing scheme. According to the data, the common way to price the products in the service business has been the use of fixed product pricing. That is, customers have paid separately for each product they are using. Our interviews provide new evidence that security service firms may probably experience a momentous change in their pricing policy in the near future. This is because companies are taking a more and more value-based pricing approach by introducing, e.g., fixed monthly rates and service contracts that are fundamentally value centered.

> *"We are not aiming at being the cheapest provider of security services in the market, but the most credible partner for our customers." (Case E)*

Value-based pricing appears to be a viable pricing model even in the future. As the previous excerpt from the interviews suggest, its strengths lie in the long-lasting and trustable supplier-customer partnerships. Our data further puts forward that some of the managers of the security firms interviewed would be willing to define the criteria that would serve as the basis for assessing the value of security services and solutions. In addition to this, they are interested in producing specific case examples based on past projects and best practices that could be communicated to prospective customers in order to demonstrate the benefits of purchasing more comprehensive security services and solutions.

Management mindset

Management mindset signifies the business model's existence in the minds of the people pursuing it. In particular, from the perspective of an organization's service orientation, it determines whether the management of a firm specifies the company's business in terms of products, markets or services provided to the clients. Following the idea by Porac et al. (2002), Tikkanen et al. (2005) conceptualize managerial cognition in terms of the industry logic and cognitive representations that link, for instance, product or service attributes, usage conditions and buyer characteristics. Whereas previous literature on service orientation has emphasized the more operational individual employees' service orientation (e.g., Cran 1994), the management mindset focuses on the strategic and organization-level service orientation by considering managers' – those who typically are responsible for strategy-making – perceptions on the relevance and appearance of service business logic in their respective organizations.

> *"We need to shift our mindset towards customer and personnel orientation. --- The personnel is the cornerstone of our service." (Case D)*

Amongst the most important issues that enable or disable a firm to become more service oriented are its managers' perceptions on what the company is doing. Service dominant business logic necessitates a new kind of thinking; one that considers the firm as providing services and not producing products. For this purpose, both unlearning of the old and learning of the new become of essence. If managers main-

tain thinking of the firm primarily as a product company, it is difficult for the staff to communicate the potential value of the amplified service solutions to customers. In fact, the staff and especially the firm's customers may not even learn and understand the difference and potential value of provider's new service oriented logic compared to the old operation logic. In this vein, the firm meets a considerable managerial challenge as it can either succeed or fail in becoming a true service oriented business, as illustrated by the following excerpts from our interviews:

> *"The problem is that our customers still believe they are buying appliances --- and we still think we are producing them." (Case B) --- "We are not just security guards, but a service provider that assists our customers to conduct their business better." (Case A) --- "We need new thinking "when selling security as service"... that is the hardest thing – unlearning. --- And we would be too narrow-minded if we would sell to security managers only." (Case E)*

Discussion and Conclusions

Security industry's business models are facing a shift towards increased service orientation. In general, transition from products to services in many industries manifests the strategic choice of firms to increasingly compete through service. Prior research (e.g., Lusch et al. 2007; Nijssen et al. 2006; Vandermerwe and Rada 1988) shows that several factors drive the increased service orientation in firms' business strategy. These factors include, for example, diminishing product margins and, at the same time, increasing customer expectations (Oliva and Kallenberg 2003; Gebauer 2009). To these points, Mathieu (2001) suggests two distinctive strategies that service providers could employ in their business: services that support the products (SSP) and services that support the client's actions (SSC). It seems fairly obvious that foresight providers in the contemporary security service business execute both of these strategies.

Organizational service orientation has been studied in many fields including manufacturing (Gebauer 2009) and consumer retailing (Homburg et al. 2002). In addition, there are numerous studies on the transition from products to services in business marketing (e.g. Jacob and Ulaga 2008). However, prior research has not paid sufficient attention to describing these transitions in their real-life contexts, especially in the business-to-business firms business. The security industry provides us with novel and interesting examples to analyze the transition from the traditional product/technology-based business towards the more future-oriented service-dominant business logic. Our study draws on a qualitative case study approach to investigate the service orientation of companies providing business-to-business security services in Finland. The data were collected through semi-structured interviews with senior managers in these companies. In addition, we went through observation an extensive set of secondary material on the security service business.

In addition to "servitization", security industry is faced by increasing reliance on technology. There is ongoing debate on whether and how the traditional forms of security service, e.g. guarding, could be replaced by automated security and surveillance systems. In the extreme cases, technology is considered to replace a vast part of the security service, as evidenced by the recent development of robotics in the Japan's security market. However, Vargo and Lusch (2004) and Lusch et al. (2007) underscore that the customer-related exchange processes and business relationships are in the centre of the focus in the ser-

vice-dominant view. This is congruent with our findings, which highlight that service oriented business models can not rely solely on automated service processes.

Figure 1 summarizes the key observations of service orientation in the business models of the security firms studied. Analysis of the organizational service orientation at the level of business model components was found advantageous given the need for analyzing the organizational service orientation in firms' business. This is because business model describes the key components of the business, and, thus, enables us to investigate the appearance of service orientation in specific, easy-to-identify, but utterly crucial aspects of firm's business.

Our findings indicate that security service providers strive to take care of swiftly increasing spectrum of customer needs. There seem to be several ongoing transitions in the security service business, including simultaneous shifts towards more comprehensive, customer-specific and integrated security service solutions. In some cases, these are pursued through more standardized service processes and modularized security service concepts. This is consistent with prior research, which has indicated that many companies struggle to formulate and implement a service orientation in their business (Gebauer 2009).

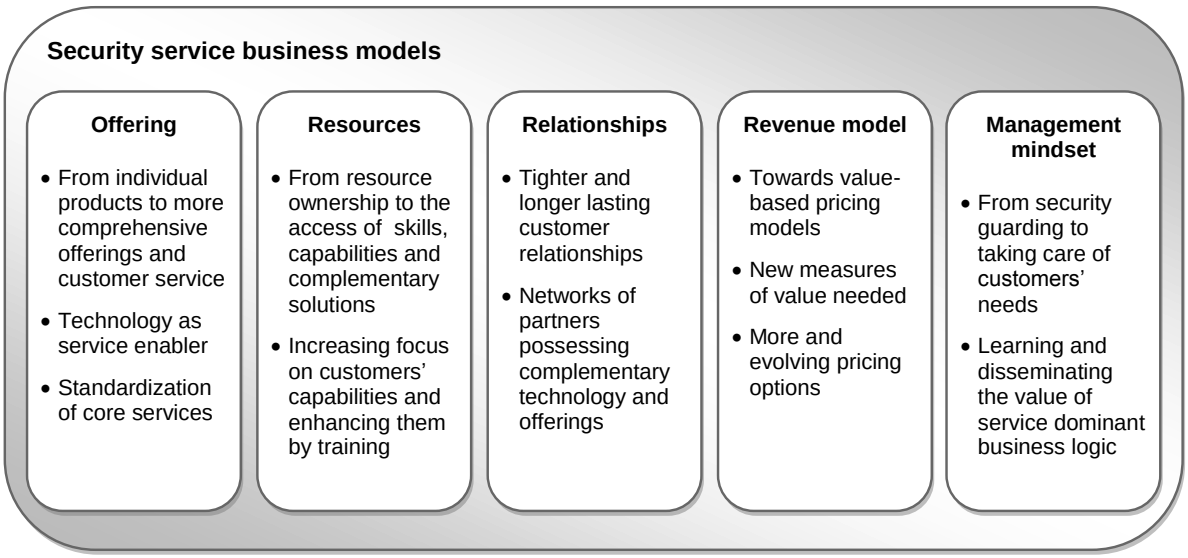


Figure 1. Summary of the findings

According to Oliva and Kallenberg (2003), the number of manufacturing organizations with strong services strategies is short, because 1) firms don't believe in the economic potential of the service component for their product 2) firms think that providing services is beyond their competencies, or 3) firms realize the market potential, decide to enter the market, but fail to deploy a successful strategy. However, we argue that an important reason why many firms struggle and experience confrontations in becoming service-oriented is that they have delimited their development focus on the changes in the company's offerings. That is, many firms emphasize nature of their offerings in the shift from products to services and fail to understand that offerings are a component of the business model of a firm which is firmly connected to other relevant components. Thus, the other elements of firm's business models will not

support their "offering-driven service orientation" very well, but would need similar changes and alignment to support the newly established service dominant operation logic.

In conclusion, our study reveals that although the dominant business logic in the security industry has relied on product-oriented offerings, firms increasingly emphasize service-dominant logic over product-dominant logic in their security solution business. Along with this transition, they have to promote organizational service orientation in their business. Due to its component-like nature, the business model of a firm provides a conceptual tool to investigate and evaluate the appearance and effects of this increased service orientation in security service firms' business. Accordingly, the use of business model approach creates a great potential to enhance a company's foresight capabilities. Our findings provide interesting avenues for further research, such as to what extent do increased service orientation affect on firms' financial performance. Thus, our exploratory study calls for more research on the performance implications of organizational service orientation in the security business.

References

Antioco, M., Moenaert, R.K., Lindgreen, A. and Wetzels, M.G.M. (2008) Organizational antecedents to and consequences of service business orientations in manufacturing companies, *Journal of the Academy of Marketing Science*, Vol. 36, 337–358.

Armitage, R. and Pease, K. (2007) Design and Crime: Proofing electronic products and services against theft. *European Journal on Criminal Policy and Research,* Vol. 14(1). 1-9.

Baldwin, D.A, (1997) The concept of security. *Review of International Studies,* Vol. 23, 5-26.

Barney, J. (1991) Firm resources and sustained competitive advantage. *Journal of Management* (17)1, 99-120

Berthon, P., Hulbert, J.M. and Pitt, L. F. (1999) To serve or create? Strategic orientations toward customers and innovation, *California Management Review*, 42(1), 37-58.

Betz F. (2002) Strategic business models. *Engineering Management Journal*. Vol. 14(1), 21-27.

Brück, T., Karaisl, M. and Schneider, F. (2008) A Survey of the Economics of Security. Economics of Security Working Paper 1. German Institute for Economic Research, Berlin, Germany.

Chesbrough, H. W. (2007) "The market for innovation: implications for corporate strategy." *California Management Review*, Vol. 49(3), 45–66.

Chesbrough, H. and Rosenbloom, R.S. (2002) The role of the business model incapturing value from innovation: Evidence from Xerox Corporation's technology spin-off companies, *Industrial and Corporate Change*, Vol. 11(3), 529-555.

Cran, D. (1994) Towards Validation of the Service Orientation Construct. *The Service Industries Journal*, Vol, 14(1), 34-44.

De Waard, J. (1999) The Private Security Industry in International Perspective. *European Journal on Criminal Policy and Research*, Vol. 7(2), 143-174.

Denzin, N. K. (1978) *The research act: A theoretical introduction to sociological methods*. New York: McGraw-Hill.

Gebauer, H. (2009) An attention-based view on service orientation in the business strategy of manufacturing companies. *Journal of Managerial Psychology,* Vol. 24(1), 79-98.

Homburg, Ch., Fassnacht, M. and Guenther, Ch. (2003) The Role of Soft Factors in Implementing a Service-Oriented Strategy in Industrial Marketing Companies. *Journal of Business-to-Business Marketing,* Vol. 10(2), 23-51.

Homburg, Ch., Hoyer, W.D. and Fassnacht, M. (2002) Service Orientation of a Retailer's Business Strategy: Dimensions, antecedents, and Performance Outcomes. *Journal of Marketing,*Vol. 66, 86-101.

Jacob, F. and Ulaga, W. (2008) The transition from product to service in business markets: An agenda for academic inquiry. *Industrial Marketing Management,* Vol.37, 247-253.

Linder J.C., and Cantrell S. (2000) *Changing business models*. Chicago: Institute for Strategic Change, Accenture.

Loader, I. (1999) Consumer culture and commodification of policing and security. *Sociology*, Vol. 33, 373-392.

Lusch, R.F., Vargo, S.L. and O'Brien, M. (2007) Competing through services: Insights from service-dominant logic. *Journal of Retailing,* Vol. 83(1), 5-18.

Lytle, R.S., Hom, P.W., and Mokwa, M. P. (1998) SERV*OR: A managerial measure of organizational service-orientation. *Journal of Retailing*, (74), 455–489.

Magretta, J. (2002) Why business models matter. *Harvard Business Review*, May 2002.

Mathieu, V. A. (2001) Service strategies within the manufacturing sector: benefits, costs and partnership. *The International Journal of Service Industry Management*, Vol. 12(5), 451-475).

Morris, M., Schindehutte M. and Allen, J. (2005) The entrepreneur's business model: toward a unified perspective, *Journal of Business Research,* Vol. 58, 726-735.

Multanen, A. (2009) *Corporate Social Responsibility in the Retail Business Model: four modes from skeptic penny-pinchers to proficient utilizers*, Helsinki School of Economics, Master's thesis, Department of Marketing and Management, Helsinki.

Möller, K., Rajala, R. and Westerlund, M. (2008) Service innovation myopia? A new recipe for client-provider value creation. *California Management Review*, Vol. 50(3), 31-48.

Naisbitt, J. (2006) *Mind Set: Reset Your Thinking and See the Future*. HarperCollins Publishers, NY, USA.

Nijssen, E.J., Hillebrand, B., Vermeulen, P. and R. Kemp (2006) Exploring Product and Service Innovation Similarities and Differences. *International Journal of Research in Marketing*. Vol. 23(3), 241–251.

Pateli, A.G. and Giaglis, G.M. (2004) A research framework for analysing eBusiness models. *European Journal of Information Systems*, Vol. 13(4), 302.

Porac, J., Ventresca, M. and Mishina, Y. (2002), Interorganizational cognition and interpretation, in Baum, J. (Ed.), *Companion to Organizations*, Blackwell, Oxford, 579-98.

Rajala, R. (2009) *Determinants of Business Model Performance in Software Firms*, Helsinki School of Economics, Doctoral dissertation, A-357. HSE Print 2009, Helsinki.

Rajala, R. and Westerlund, M. (2007) Business models –a new perspective on firm's assets and capabilities: observations from the Finnish software industry. *Entrepreneurship and Innovation,* Vol. 8(2), 115-125.

Rogelio, O. and Kallenberg, R. (2003) Managing the transition from products to services. *Journal of Service Industry Management,* Vol 14(2), 160-172.

Rouhiainen, V. (ed.) (2009) *Scientific activities in Safety & security 2009*. VTT Technical Research Centre of Finland.

Shafer, S.M., Smith, H.J. and Linder, J.C. (2005) The power of business models. *Business Horizons*, Vol.48, 199-207.

Tikkanen, H., Lamberg, J.-A. Parvinen, P. and Kallunki, J.-P. (2005) Managerial cognition, action and business model of the firm, *Management Cognition,* Vol. 43(6), 789-809.

Vandermerwe, S. and Rada, J. (1988) Servitization of business: Adding value by adding services. *European Management Journal*, Vol. 6(4), 314-324.

Vargo, S.L., and Lusch, R.F. (2004) Evolving to a New Dominant Logic for Marketing. *Journal of Marketing*, Vol. 68, 1-17.

Wolfers, A. (1952) "National security" as an ambiguous symbol. *Political Science Quarterly,* Vol. 67(4), 481-502.

Yin, R. K. (2003) *Case Study Research: Design and Methods*. Sage Puclications, London.

Zedner, L. (2003) Too much security? *International Journal of the Sociology of Law,* Vol. 31, 155–184.

NATIONAL SECURITY VERSUS INTERNATIONAL MARKETS: ON FUTURE POSSIBILITIES FOR THE CONTROL OF FOREIGN DIRECT INVESTMENTS IN STRATEGIC INDUSTRIES

Thomas Teichler
The University of Manchester, Manchester Institute of Innovation Research (MIoIR)

ABSTRACT *- The free flow of capital is an inherent characteristic of the world trade order. Yet in recent years it has been increasingly limited, among others by legislation for the control of foreign investments in "strategic industries". Governments have justified such measures by citing security concerns such as the security of supply with arms or the risk of proliferation. The current economic crisis has further raised the spectre of the end of globalisation and the return of economic nationalism.*
The paper examines the possibility for an international mechanism to control FDI in strategic industries in a group of countries, in this case the member states of the European Union (EU). It argues that the need to balance the principle of open capital markets with security concerns related to FDI is particularly significant for the EU due to the fact that it is not merely a robust single market but aspires to become a political actor, albeit with national governments still controlling security policy. Based on regime theory and a comparative analysis of three national FDI control mechanisms, the paper develops a typology of regimes and sketches four relevant types for the control of FDI at EU level.

Introduction and Background[3]

The general background of the problem

The economic crisis that has beset the world economy since 2008 has raised the spectre of the end of globalisation and the return of economic nationalism. "Economic nationalism" means that governments adopt measures to ensure that strategically important assets in one country remain under national control. For this purpose they implement law that allow them to control and constrain the free movement of

[3] This paper represents the state of analysis contained in the mimeo [Strategic controls on foreign acquisitions: National security or economic nationalism? v1.3 10/04/2009, unpublished mimeo, MIoIR, MBS, UK]. MIoIR currently conducts a research project on this topic, which addresses additional aspects not considered here. I would like to thank my colleague Andrew James for his permission to use some of the material from that unpublished mimeo. All errors remain, of course, my own.

capital, which is considered to be the cornerstone of the international trade regime, of globalization and of wealth creation in general. The liberalization of financial markets has allowed for the efficient distribution of financial resources and has enabled corporate actors to access new sources of financing and to hedge against risks, which had been hitherto been closed to them.

The free movement of capital has also been enshrined in various forms in the current economic world order. However, all international agreements of this kind provide the possibility for the signatories to derogate from the agreement for the purpose of their national security (see, for example, (GATT, 1947: Art. XXI). Given that many defence companies[4] do not only supply the armed but also form an important part of a country technological and innovative prowess governments have always been keen to oversee and control the defence industry. In former times direct and majority ownership combined with a dominant position the national government as the main customer and financial supporter of the national defence companies has ensure high levels of control. Privatization and internationalization of the defence industry, however, have led to a situation where the security of supply or the controlled transfer of high technology is increasingly beyond the reach of governments.

Hence, many of them have enacted or tightened laws that allow them to intervene should foreign investors attempt to acquire assets in strategically important sectors such as the defence industry. This has been, for example the case in Poland (2001), the UK (2002), Germany (2004), France (2005), China (2006), or Russia in (2007). In the United States the Exon-Florio Amendment from 1988 allowed the administration to restrict or forbid an investment into an US company for security reasons.

While the adaption of such law is not new, the increase in the number of national governments who have introduced legislation to control foreign acquisition of "strategic" assets is striking, as a recent study by the U.S. Government Accountability Office noted that (GAO, 2008). Moreover, countries with existing legislation have adapted their laws in face of changing circumstances and increased the leverage of governments over the free movement of capital.

There are several reasons for the growing attention paid by governments to this matter.

- First, technological developments, globalization, and the experience of terrorist attacks have shaped a new notion of those sectors deemed to be of strategic importance for the sovereignty of a country. Technology produced for commercial purposes is increasingly used by the armed forces. Hence, some industries that have formerly not been related to the security or foreign policy of a country are now awarded "strategic significance", like parts of the telecommunications industry. The actual and potential scarcity of raw materials has had a similar effect (OECD, 2006). At the same time, the interdependence between countries has increased as transportation, communication, and financial links have intensified. As a result some economic assets usually referred to as infrastructure e.g. gas pipelines or telecom networks are nowadays deemed to be too vulnerable to be simply left to an open investment regime.
- Second, the increased role of non-OECD[5] countries as outward investors seems to have heightened concerns, at least in some countries, that not all actors may necessarily play by common rules or promote high standards of business conduct (OECD, 2006). While traditionally FDI

[4] Although there are other "strategic sectors" that touch upon the "public" or "security" interest of governments, this paper is interested in the defence industry/assets/sector only.
[5] OECD stands for Organization of Economic Cooperation and Development.

have flown to developing countries, the last decade has seen the acquisition of assets in OECD countries by investors from emerging economies, for instance Russia and China. It is not so much the mere arrival of additional actors but rather their business practice and their close political ties that is disquieting governments of Western countries. For example the concern about sovereign wealth funds[6] of some governments stems from the fact that – because they are state owned – they may be guided by political objectives rather than profit maximisation or that they may be motivated to support creation of "national champion" companies.[7]

- Several high profile cases such as the successful takeover of IBM's PC business by the Chinese firm Lenovo in 2004, the attempted acquisition of Unocoal by CNOOC in 2005, or that of P&O by Dubai Ports in 2006 have gained wide public interest. While political aspects were in the foreground of the debates, these cases also revealed public concern over individual acquisitions about the impact on jobs (OECD, 2006).
- The recent financial crisis has added legitimacy to popular demands for to a tighter governmental involvement into business in general and a closer oversight of financial transactions in particular.

While some fear in this context the return of protectionism, speaking of "economic nationalism" these seem to exaggerations. After all, the aforementioned legislation is a milder and more transparent form of state intervention into the defence market than government ownership or special rights such as golden shares. The rise in the number of legal provisions for the control of FDI has also to be seen in the context of the privatizations of many defence companies in Europe after the end of the cold war and of the internationalization strategies that many of these companies have pursued.

Nevertheless, the new legislation has raised concerns in many corners, not least the European Commission and the Organization of Economic Cooperation and Development (European Commission, 2007; OECD, 2007). The latter has set up a special committee to investigate and monitor the development in 2007.[8] With its activities the OECD has mainly sought to increase transparency and build trust through information exchange and conceptualization of concerns.

These are important confidence building measures, contributing to uphold a liberalized international trade order. They do not entail the implementation of commonly agreed rules nor are they in any sense binding but can rather be regarded as a very subtle form of international cooperation. The question arises, whether there would be other possibilities to address the security concerns of countries, on the one hand, and safeguard an open international financial system, on the other. How could a more robust international cooperation on the control of FDI in defence assets could look like? This question seems to be particularly pertinent with regard to the European Union.

---

[6] "Sovereign wealth funds are entities that can manage national savings for the purposes of investment. These funds may be similar in their investment behavior to other forms of investment funds, such as private equity funds. However, they fundamentally differ in that they are not privately owned" (GAO, 2008: 3).
[7] I am grateful to Andrew James for having brought this aspect to my attention.
[8] I am indebted to Andrew James for having drawn my attention to the activities of the OECD.

The particular situation of the European Union

The issue of collaboration on the control of FDI in the defence industry is above all relevant with regard to the European Union because of the double nature of the EU. The EU is not a unitary political actor with a single economic and a single defence policy but it is not simply a part of the liberal world trade order either.

First, the EU is in many respects a single market, which is internally much more open than the remainder of the world trade order.[9] The free movement of capital is one of the fundamental freedoms. Article 63 (1) of the Treaty on the Functioning of the European Union (TFEU) prohibits as a general rule all restrictions on the movement of capital between member states and between member states and third countries (TFEU, 2008). Moreover, the Common Market has with the European Commission a powerful and strong guardian. Finally, the European defence firms are closely linked among each other, through financial participation and by a long history of armaments collaboration (Bitzinger, 1994; 2003; Jones, 2007). Given the particularly high interdependence among EU economies a limitation of the free movement of capital among them would be most disturbing.

While one would expect the defence industry to be part of the Common Market, it is not. Article 346 TFEU enables EU member states to derogate from the Common Market rules if they consider it necessary "for the protection of its essential security interests" (TFEU, 2008: Art. 346). National governments have de facto controlled their defence industries and only recently started to collaborate on industry and market issues within the EU, allowing the Commission a mild say in the matter. For this purpose EU governments have set up an Agency – the European Defence Agency (EDA) – under the EU Council, which is governed by the Defence Ministers of 26 of the 27 EU member states. Defence Ministers have agreed to establish a "truly European Defence Technological and Industrial Base" (EDTIB) and a European Defence Equipment Market (EDEM), which allow for cross-border consolidation and rationalization and the emergence of Centres of Excellence ((EDA, 2004; 2007). While Defence Ministers address several industrial issues through the EDA, FDI control is not among them. The main task of the Agency is rather to support governments in the improvement of military capabilities. A strong and competitive defence industry is to support this purpose, which points to the second specific aspect of the EU.

The EU is second, an evolving political actor in security and defence policy, despite the fact that national governments have the last word on these matters. There is neither a single voice nor a single telephone number that foreign leaders could call in order to listen to "Europe's views". However, EU governments have coordinated their foreign policies, developed instruments, and established coordinating institutions under their Common Foreign and Security Policy (CSFP) and their European Security and Defence Policy (ESDP). Especially the latter, pursued since 1999 offers the possibility to develop a shared understanding about problems and to devise common solutions.

In sum, due to the fact that the EU is a Common Market a common FDI control seems to be more needed than for the cooperation among other countries; and due to the fact that the EU is also an evolving political actor, a common FDI control has more chance to succeed than among other countries. Given that FDI controls in the defence sector touch on the one hand, on common market issues and on the

[9] The recent "Monti-Report" points to considerable shortcomings of the current single market and calls actually for a re-launch of this project. See (Monti, 2010).

other on defence and security policy issues, the question arises of how EU Member States ensure control of investments into their defence assets and what are the effects on the common market. In other words, how can (national) security and economic interests be reconciled?

This paper sets out to examine the current situation and to point the direction for a possible solution to this dilemma. To this end I will briefly discuss the academic literature on the control of FDI in strategic industries; provide a comparative analysis of the control mechanism of individual EU member states, and suggest a framework for the development of a regime for the cooperation of governments on this issue.

The scholarly debate on the control of FDI

The scholarly literature has so not extensively debated this question. Two bodies of work can be distinguished. The first, US oriented texts have addressed the issue of potentially negative effects of FDI on the national security and the adequacy of national control mechanism. While the initial debate focused on the effects of Japanese and Western European investments in the 1980, which saw a stark rise of the number of transnational firms and prompted the adoption of protective legislation in 1988,[10] the recent discussions concentrated on the investment of Chinese firms (Globerman and Shapiro, 2009; Graham and Krugman, 1995; Hemphill, 2007). The question of international cooperation is only raised by Moran when discussing the issue of security of supply of defence materials. Moran suggests the maintenance of an oligopolistic supply at the global level, the interpenetration of defence firms from different countries, since that would reduce the risks of stand-offs between governments; and the creation of an international settlement mechanism, allowing to negotiate and to avoid confrontations (Moran, 1990). It is exactly this latter notion – voiced as early as 1990 with a global perspective – that has been picked up by European researchers in mid-2000s in view of the European Union.

The second body of literature by European scholars has focused on a presentation of several control mechanisms at national level and on the elaboration of a possible European level solution (Nones, 2000; Nones and Darnis, 2005; von Wogau and Rapp-Jung, 2008). Von Wogau and Rapp outline two possibilities for a EU level mechanism for the control of FDI in the defence industry from a legal perspective. While this is entirely legitimate and has the advantage of considering the legal feasibility in light of the complex EU Treaties, the approach limits itself to the institutionally feasible, sidelining the politically possible. While these attempts have made invaluable contributions by providing information about the situation in different EU countries, they have neither compared national legislations nor systematically probed into the full range of options for EU level control.

An in-depth examination and comparison between the different national approaches to the control on FDI in strategic industries in Europe seems therefore to be in order. Regime theory provides us with an analytical starting point for such an examination.

---

[10] The Committee on Foreign Investment in the United States (CIFUS) was established by Gerald Ford's Executive Order 11858 in 1975. It was further strengthened by the delegation of Presidential Oversight by Ronald Reagan's Executive Order 12661 in response to the Exon-Florio Amendment to the Omnibus Trade and Competitiveness Act was adopted in 1988. In 2007 this legislation was strengthened by the Foreign Investment and National Security Act.

In order to compare the different national legislations in view of the topic of this article, several criteria should be used. They should enable an analysis as to the issues and deficiencies of the current situation within the EU, in particular the effects on an envisioned European Defence Technological and Industrial Base and on the efficient allocation of capital i.e. the conditions for investors. With this purpose in mind and based on the aforementioned studies ten criteria will be used for a comparative analysis of the different national investment control mechanisms.

Comparative analysis of control mechanisms of selected EU countries[11]

Generally, investments from outside the EU as well as from other EU countries are not restricted by the governments of EU Member States. However, at least three out of 27 EU countries currently have legislation allowing them to review investments in companies and organizations engaged in defence-related activities: France, Germany and the United Kingdom.[12] The control regimes of these countries differ considerably as to their general approach, as well as with regard to the specific technicalities.

What is the purpose of FDI controls?

The purpose of the FDI legislation control legislation is to safeguard the "public interest", "national security interest" and/or "public order". These terms are all rather vaguely defined and, hence, leave governments considerable room for interpretation.

To what extent does the legislation refer to European security interests?

Does the legislation reflect a concern for the security interest of other EU countries or of the EU as a whole? An analysis of the legislative texts reveals that the notions of „national security interest" and „public order/interests" are understood in national terms without any reference to a European dimension.

Which investors are concerned?

There is a considerable difference as to whose investments can potentially be reviewed. While the control regimes in France and Germany apply only to investors who reside outside the country, the legislation in the UK extends to all investors including domestic residents.[13]

---

[11] The following analysis draws on empirical data presented in (Nones and Gasparini, 2008); (GAO, 2008).
[12] Two caveats are in order: First, the focus of this paper will be put on France, Germany, and the United Kingdom for three reasons. They have been the first EU countries to enact such legislation; they are the top-three EU countries according to the stock of FDI at home (CIA, 2008); and finally, they have the most significant defence industrial and technological base (measured in terms of turnover and employment, largest overall defence, defence procurement and defence R&T budgets of the EU (EDA, 2009). Second, while all countries can shape defence investors' expectations by "indirect means" such as procurement contracts or export licenses, which are not less effective but which are not directly concerned to review and alter investments. This paper is only concerned with legislation directed at FDI control, neither with indirect legislation nor with it application.
[13] The French legislation stipulates slightly different rules for investors from EU and EAA countries respectively 2005).

What types of assets are covered by the legislation?

While all countries consider explicitly (all but UK) or implicitly (UK) the defence industry to be at the core of those assets that need to be potentially shielded from foreign investments, the notions of "defence industry" are by no means comparable France and Germany use lists of products, sectors or activities to specify what they mean with "defence industry", In addition, legislation of these countries extents well beyond defence to cover other types or all economic activity; for example the French list includes dual-use technologies and gambling and the German law refers to satellite equipment. In the UK investments in any company from any sector can come under scrutiny if the authorities deem the "national interest" to be in jeopardy.

What threshold triggers the review?

The minimal size of the investment – measured in terms of shares of the voting rights – that triggers a control differs across the three countries. In Germany a transaction triggers a review if 25% of the voting rights of a defence company are acquired, in France the number is 33% for non-EEA investors or and "a controlling share" for EEA investors. While in the UK such changes don't need to be notified, they can prompt an examination on the initiative of the authorities, if they fall under the merger regulation.

Which body within government is responsible for the review?

The dimension of which department in the government is vested with the authority to oversee the control of FDI shows a high degree of commonality: the Ministry dealing with economic and trade matters is in charge of overseeing the review of foreign investments in the defence industry in Germany and the UK; and the Ministry of Finance in France. While the Minister oversees the process and takes the final decision, a subordinate body such as the Office of Fair Trading (OFT) in the UK is conducting the review. In all countries the authorities in charge consult with the Ministry of Defence on investments in defence-related companies and with other Ministries in case of investments in other sectors deemed of strategic importance.

Is a notification of the intended investment required?

While all countries but the UK require the investor to notify the transaction to the authorities, there are some differences as to the exact obligations of the investor. In France, the investment has to be notified *before* the transaction takes place, as investors have to seek approval or obtain a permit from the authorities for the transaction to go ahead. An omission represents an offense and can be prosecuted. In Germany authorities have to be informed about the investment within one month.

How is the review process structured?

The review process and duration differs from country to country, though the essential steps are similar. Once a review has been announced, the investor is required to submit specific documents to the government. When all documents have been completely submitted to the authorities, the latter have to finalize the review and respond within a period of several months (one month in Germany, two months in France; six months in the UK). In all countries a transaction will be considered automatically as approved if the authorities have not responded within the prescribed period of time.

What are possible outcomes of a review?

In principle there are four possible outcomes of a review procedure – a government can not oppose a transaction, give formal clearance, impose amendments to it and agree on mitigations or ban it. While in France and Germany all four outcomes are possible, banning is not an option the UK. However, the UK authorities can refer a case to the Competition Commission for an assessment of its effects on the conditions of competition, presents a practical equivalent to a ban of the transaction.

Are the decisions made public and can they be appealed?

In none of the countries except the UK do the authorities publish the decisions following a review. It is only made accessible to the investor whose transaction was reviewed. In other words, competitors, other governments or the wider public have no access to this information (or need to rely on leaked information), which has an effect on the transparency of the entire processes. Finally, all countries grant the investor a right to appeal a decision to an administrative court.

Possibilities for cooperation on the control of FDI in defence assets

Possible regimes for the cooperative control of FDI

The comparative analysis has shown that the legislation for the control of FDI in the defence sectors differs considerably across the EU countries with the most significant defence industrial base. In fact there was only one parameter in which they did not vary: in all countries an investor has the right to appeal against the outcome of a review.

Such a situation presents an impediment to the declared political goals to create a European Defence Technological and Industrial Base and a European Defence Equipment Market and to safeguard the free movement of capital. It seems to be worthwhile then to raise the question of how EU governments could cooperate on the control of foreign investment in defence assets. To this end the following section suggests a framework to delineate different types of cooperation drawing on regime theory.[14]

[14] Regime theory provides a formidable starting point for the development of possible solutions for EU cooperation. While being a systematic school of thought it is general enough and at the same time rigorous tool to open up the

According to one often cited definition regimes "are sets of implicit or explicit principles, norms, rules, and decision making procedures around which actors' expectations converge in a given area of international relations" (Krasner, 1983: 2). This definition merits the question, "expectations" about what? As Haas has aptly shown, the size and nature of an issue area are contested, as different governments might have different ideas about which problems to include in the common effort (Haas, 1980). He and others have, therefore, pointed to the importance of the specific activities that actors are interested in, for the set up of a regime (Young, 1980). The activities will in our case be those that are required to ensure control of FDI in defence assets.

Cooperation on FDI control can then be characterized along two dimensions: the degree of integration of national behaviour and the function of cooperation (Ruggie, 1975). Two functions of cooperation can be distinguished for our purposes: the regime can serve governments to *inform* each other – e.g. about the size, structure, and nature of transactions, their review and the outcome of the review or about the understanding of the problem and the application of laws. Alternatively, EU governments could collaborate on *managing* the control activities together.

As for the degree of integration of national behaviour four types can be distinguished here (Haas, 1980; Ruggie, 1975): A *Common Framework* provides for pooling or combining individual behaviour on the basis of sharing information. A *Joint Facility* coordinates national behaviour and tries to make it "commensurable". For example governments will standardize and harmonize some of their information gathering routines, making their behaviour more comparable and compatible. A *Common Policy* regulates the national behaviour according to common rules. While individual national enteritis will continue to exist and to act, they will do so according to a commonly agreed upon set of understanding of the issues involved, rules, norms, and principles that shape the way they manage theses issues. In case of a *Single Policy* states loose their autonomy with regard to a specific issue area. It substitutes common management for independent national behaviour. The Single Policy can be implemented in various ways, either directly by the central organization or indirectly through the national authorities but under common supervision.

The matrix that results from a combination of the two dimensions yields eight *possible* ideal types of EU regimes for the control of FDI in defence assets.

Table 1. Matrix of possible regimes for the EU level control of FDI

Instrumentality Function	Common Framework	Joint Facility	Common Policy	Single Policy
Informing				
Managing				

widest possible space for heuristic investigation into the possibilities of how cooperation could be institutionalized. This aspect is particularly important since cooperation on the control of FDI represents a very sensitive area and a nuanced, step-by-step approach to cooperation seems to be most appropriate to overcome hesitation and mistrust over time.

Out of the eight possible regime types shown in Table 1, not all seem to be sensible, as the two dimensions characterizing a regime type are interconnected. For example, a Common Framework, aiming at the pooling of behaviour will not be sufficient to manage the control of FDI. Equally, a Common Policy managing the control requires a common policy for informing partners about transactions and their treatment. We can, of course imagine a Single Policy for informing each other. However, it would not significantly differ from the behaviour of states cooperating in a Joint Facility.[15] Against the background of these deliberations, it seems that out of the eight possible regime types, four – marked grey in the table above – are particularly relevant, and will therefore be briefly sketched in the following section.

Four relevant regimes for cooperative FDI control

Common Framework for informing about FDI control

The lightest level of integration would be achieved through the establishment of a Common Framework, integrating governments' behaviour with regard to informing partners of FDI activities and (potentially) how they are treated and why. For example, EU member states could agree that they would inform each other if an investor from a non-European country intends to invest in defence assets in one country, given that this might potentially affect the security of supply of defence goods or other aspects of the defence policy of another EU country. The latter would simply be informed without having a right for consultation. The Heads of State and Government of the EU in fact suggested such an information exchange with regard to investments from non-EU countries in December 2008, albeit it seems without any practical implications to this point (Council of the European Union, 2008).[16]

Though a Common Framework to inform partners is only a first step, it is by no means trivial, as the following issues will have to be addressed: which transactions will be scrutinized – only from non-EU countries or also those from other EU countries? Will governments be obliged or can they choose to inform their partners? Will they have to do so retrospectively or in parallel to a transaction or review? What information are they going to share? Which circle of countries should be informed – all EU members or only those with a substantial defence industry? How shall transactions from a EU country in the defence industry of another EU country be dealt with? Which authorities should be informed – the Ministries of Defence or that of the Economy? What would be the role of European institutions?

Joint Facility for informing about FDI control

In a more extensive form of cooperation, a Joint Facility, governments would exchange information about FDI according to commonly agreed norms. A Joint Facility would involve the standardization of procedures and formats of data that is to be collected and transferred on a regular basis. It could then be

[15] The most significant difference would concern the legally binding character of rules and procedures, which is a precondition for cooperation in a Single Policy but not for in a Joint Facility.
[16] I am grateful to Michel Gari for having brought this fact to my attention. The aforementioned roundtables and seminars organized by OECD could equally evolve into such a Common Framework.

compared and consolidated into a common report. This would require, however, joint understanding of key concepts and the change of administrative procedures in each country.

Cooperating in a Joint Facility does not imply any relocation of staff and resources. However, it might require the support through a central organizational structure – for example, the European Defence Agency or the Council of the EU – to compile and consolidate the data. Alternatively, one of the governments could volunteer to provide such a facility. Such an organization would still be light in its character, as national experts would do most work. In addition, a research or advisory staff, for example a board of industry or academic experts, would not need to be institutionalized as a permanent body but could function as a regularly meeting working groups of independent experts.

Common Policy for managing FDI control

In case of a Common Policy national authorities continue to work, albeit according to commonly agreed rules and procedures. While cooperation in the first two regime types does not involve any substantial agreement on the FDI control, a Common Policy requires a shared notion about the general approach and purpose, the scope, the procedures, the assessment criteria and outcomes, and a way to appeal against a decision.

The conceptualization, implementation, and monitoring of such commonly agreed rules would require the support of a central organization, endowed with considerable financial and human resources. As the central organization would merely assist national authorities in carrying out their tasks, the European Defence Agency seems to be well suited for this job, as it plays such a supportive role already today in related matters.

Finally, a Common Policy can but does not need to involve a legally binding agreement on the rules and procedures. It would also not require all EU member states to take part in the management of control according to common rules. Instead governments could sign a voluntary, legally non-binding Code of Conduct. Such a "loose" commitment would not be possible in case of a Single Policy.

Single Policy for managing FDI control

The main difference between a Single and a Common Policy is that a Single Policy requires legally binding agreements on the rules for the management of FDI control and that a central authority substitutes common management for independent national behaviour. The Single Policy can be implemented in various ways, either directly by the central organization or indirectly through the national authorities but under common supervision by an EU body.

While this seems to have been the model that von Wogau and Rapp had in mind in their article (von Wogau and Rapp-Jung, 2008), they did not yet make any suggestions with regard to which institution(s) should be authorized to oversee and conduct the review process. In line with national practice it could be a department of economics e.g. the Directorate General (DG) MARKT or COMPETITION of the European Commission. It is in general responsible for overseeing the common market and has ample experience to assess mergers and acquisitions in other sectors. However, it lacks the security policy expertise, which could be provided by the European Defence Agency. Alternatively, the EDA could oversee the pro-

cess and take the final decision, tasking DG MARKT/COMPETITION with the review of the transactions. The latter option would come close to a solution originally envisioned by Nones and Darnis in their 2005 article (Nones and Darnis, 2005), where they vest the authority of an evaluation and decision with "the Prime Minister's Office" – the EU equivalent of which would be the European Council – with input from various ministries.

A major challenge for a Single Policy is the provision and integration of security policy advice. Who or which institution is going to furnish that advice: the Ministry of Defence of the country in which the target company is situated or a common European Union structure? How can negotiations be handled as to guarantee the informality and subtleties of negotiations that are characteristic for the close ties between national authorities and defence companies? Finally, what if the security assessment of different Ministries of Defence vary on the case, how can conflicts of interest between different EU countries be resolved? While all these are pressing questions, an elaboration of their answers lies beyond the purview of this paper.

Conclusion

This paper has addressed the question of how investments in the defence industry are controlled within the European Union. It started from the observation that the EU faces a dilemma: on the one hand, the single market, of which the defence industry is an organic part, is overseen by the Commission; on the other, control over defence policy and the defence industry has remained with each government. The central question of the paper was how do EU Member States ensure control of investments into their defence assets while at the same time adhering to the rules of the single market? It was shown that three countries representing the bulk of the European defence industry have specific legislation for the control of investment into their defence industry, which differs considerably across countries. Assuming that such a divergence and the fact that only three EU countries have control legislation is not conducive to the political goals of consolidating the EDTIB and the EDEM, as well as ensuring the free movement of capital, the paper suggested a framework for the development of different regimes. It finally sketched four relevant regime types for cooperation on the control of defence-related FDI, which governments might implement in the future.

Bibliography

(2005) 'Code monetaire et financier. Titre V: Les relations financieres avec l'etranger'.

Bitzinger, R.A. (1994) 'The Globalization of Arms Industry: The Next Proliferation Challenge'. *International Security*, Vol. 19, No. 2, pp. 170-98.

Bitzinger, R.A. (2003) 'Towards a brave new arms industry?: The decline of the second-tier arms-production countries and the emerging international division of labour in the defence industry'. *Adelphi Paper*, Vol. 43, No. 356.

CIA (2008) 'The world factbook. Rank Order - Stock of direct foreign investment - at home'. Central Intelligence Agency, available at <http://www.umsl.edu/services/govdocs/wofact2008/rankorder/2198rank.html>.

Council of the European Union (2008) 'Declaration on Strengthening Capabilities, Brussels 11 December'. available at <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/esdp/104676.pdf>.

EDA (2004) 'A strategy forthe European defence technolocal and industrial base, Brussels, 14 May 2007'. Brussels, available at <http://www.eda.europa.eu/genericitem.aspx?area=30&id=211>.

EDA (2007) *A strategy for a European Defence Technological and Industrial Base* (Brussels: European Defence Agency).

EDA (2009) 'Defence Data of EDA participating Member States in 2008'. available at <http://www.eda.europa.eu/defencefacts/>.

European Commission (2007) 'A strategy for a stronger and more competitive european defence industry COM/2007/0764'. available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0764:EN:NOT>.

GAO (2008) *Foreign investment. Laws and Policies Regulating Foreign Investment in 10 Countries. Report to the Honorable Richard Shelby, Ranking Member, Committee on Banking, Housing, and Urban Affairs, U.S. Senate. GAO-08-320* (Washington: United States Government Accountability Office).

GATT (1947) 'General Agreement on Tariffs and Trade - Consolidated text'. available at <http://gatt.stanford.edu/bin/object.pdf?90070088>.

Globerman, S. and Shapiro, D. (2009) 'Economic and strategic considerations surrounding Chinese FDI in the United States'. *Asia Pacific Journal of Management*, Vol. 26, No. 1, pp. 163-83.

Graham, E.M. and Krugman, P.R. (1995) *Foreign Direct Investment in the United States* (Washington D.C.: Institute for International Economics).

Haas, E.B. (1980) 'Why Collaborate?: Issue-Linkage and International Regimes'. *World Politics*, Vol. 32, No. 3, pp. 357-405.

Hemphill, T.A. (2007) 'Balancing international trade policy with national security: The dilemma of China and foreign direct investment in the United States'. *Competition and Change*, Vol. 11, No. 1, March, pp. 59-77.

Jones, S.G. (2007) *The rise of European security cooperation* (Cambridge: Cambridge University Press).

Krasner, S.D. (1983) *International regimes* (Ithaca ; London: Cornell University Press).

Monti, M. (2010) *A new strategy for the Single Market. At the service of Europe's economy and society. Report to the President of the European Commission José Manuel Barroso* (Brussels: European Commission).

Moran, T.H. (1990) 'The Globalisation of America's Defence Industries: Managing the Threat of Foreign Dependence'. *International Security*, Vol. 15, No. 1, pp. 57-99.

Nones, M. (2000) 'A Test Bed for Enhanced Cooperation-Eu defence Industry'. *The International Spectator*, Vol. 35, No. 3, pp. 25-35.

Nones, M. and Darnis, J.-P. (2005) 'Control of foreign investments in aerospace and defence'. *The International Spectator*, Vol. 3, pp. 83-90.

Nones, M. and Gasparini, G. (2008) *Il controllo degli investimenti stranieri nel nascente mercato Europeo della difesa e sicurezza* (Rome: Istituto Affari Internazionali).

OECD (2006) 'Roundtable on freedom of investment, national security and "strategic" industries. Paris, France - 6 December 2006. Summary of discussions'. OECD, Paris, available at <www.oecd.org/investment>.

OECD (2007) 'Freedom of investment, national security and “strategic” industries: An interim report'. In OECD (ed.) *International investment perspectives: Freedom of invesment in a changing world* (Paris.

Ruggie, J.G. (1975) 'International Responses to Technology: Concepts and Trends'. *International Organization*, Vol. 29, No. 3, pp. 557-83.

TFEU (2008) 'Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union'. *Official Journal*, Vol. C 115, No. 09/05/2008, pp. 0001 - 388.

von Wogau, K. and Rapp-Jung, B. (2008) 'The case for a European system monitoring foreign investment in defence and security'. *Common Market Law Review*, Vol. 45, No. 1, pp. 47-68.

Young, O.R. (1980) 'International regimes: problems of concept formation'. *World Politics*, Vol. 32, No. 3, pp. 331-56.

FINANCIAL CRISIS, SECURITY VARIABLES AND ALTERNATIVE ETHICAL FINANCIAL MODEL

Khaldoun Dia-Eddine[17] **& Nader Nada**[18]
Zurich University for Applied Sciences, Winterthur, Switzerland
Arab Academy for Science and Technology, Alexandria, Egypt

ABSTRACT[19] *– The financial crises have large impact on stability and security of persons, corporate and nations. This paper defines a set of security variables to evaluate the impact of the crises on stability and security through the analysis of the needs and expectation of the economical system. The results of the analysis of the causes and reasons of the financial crises are linked to the variables. A proposed ethical financial model is shortly explained and linked to the security variables to balance the impact of the financial crises.*

Key words: Financial crisis, security, stability, security variables, Islamic Ethical Financial Model

Introduction and Background

A financial crisis is a disturbance to financial markets, associated typically with falling asset prices and insolvency among debtors and intermediaries, which spreads through the financial system, disrupting the market's capacity to allocate capital (Eichengreen 1987).

It is possible to differentiate between three different types of financial crises: Banking crisis, Currency crisis and Sovereign debt crisis.

Historically, in total, we count 124 banking crises, 208 currency crises, and 63 sovereign debt crises over the period 1970 to 2007. Several countries experienced multiple crises. Of the mentioned 124 banking crises, 42 are considered twin crises and 10 can be classified as triple crises. (Laeven 2008)

This means that the actual financial crisis is not a unique case, it is one of several. "Yes, we have been through this before, tragically many times" (Gorton, 2010).

At the same time, we do pretend –despite several similarities- that all financial crises tend to be quite diverse. Initial conditions are different; industrial and institutional structures are different; levels of development are different; degrees of openness are different; policy frameworks are different; and external conditions are different (Cecchetti 2009), but as we are going to explain, a lot of common things exist, they are mainly related to the paradigm of the system not to its mechanisms.

---

[17] Dia-Eddine Khaldoun, Head Middle-East, Zurich University for Applied Sciences, School of Management and Law, Center for International Business, Winterthur, Switzerland
[18] Nada Nader, Arab Academy for Science and Technology, College of Computing, Alexandria, Egypt.
[19] The study is a summary of a larger ongoing study.

A recent strand in the literature, suggests that economic conditions are important determinants of the outbreak and recurrence of conflict. Wars often start following growth collapses (Collier, 2009).

In this study, the objective is to establish a model where "security variables" are selected and defined out of the expectations of individuals and groups from the economical and financial sector. The link between these variables and the reasons and impacts of financial crises is established analytically.

An alternative financial model which deals with the different reasons of financial crises is proposed based on Islamic Ethical Financial Model (IEFM). The link between the security variables and this model presents contingencies to the reasons leading to economical crises and their impacts. The ultimate objective is to find a remedy to the recurrence of the financial crises.

The case study (here in the annex), as application of the IEFM on the sub-prime crisis shows the possibilities to reduce -or even to stop- the development of the chain leading to the crisis.

This paper is a part and a summary of some results of an ongoing research project at Zurich University for applied sciences in cooperation with the Arab Academy for Science and Technology. For the purpose of this summary, the number of variables is here reduced to 15 only (in the original study they are 33 variables).

The Human Security Variables

Looking at the history of financiaal crises from 1800 until today, it seems that the more developed the financial sector is, the more likely there will be accidents (Nazari 2009), it is to be asked if Man can learn from his mistakes!.

Human beings are always pretending that they are able to learn from negative experiences and capable to find definitive remedies for these experiences.

To start with let us define a set of security variables. Security variable is a variable related to human needs and expectations and influenced by different factors or elements coming from the economical field. The variable may also be influencing the economical sector and may –under large variation- lead to instability and subsequently to insecurity. Variables could belong to political, social or economical sectors. We will divide these variables into three categories:

First category of variables are related to the materialistic and physiological needs, they are the tangible variables; They are mainly covered by Maslow's first two levels of his model. Second category of variables are related to the non materialistic needs for security, these are the happiness supporting variables. The third category of variables is related to the ethical issues and values as basis for an expanded happiness with sustainable materialistic and non-materialistic security.

"Actually, economics is the study of the factors affecting employment and standard of living" (Jain 2006). This means that the ultimate objective of economics is to achieve higher living standards through higher GDP, per capita income, higher GNP, lesser inflation, higher level of employment, good economic conditions for attracting foreign investors, flourishing of businesses, optimum circulation of money, wise foreign investments , creating favorable environment for businesses etc, making the society and subsequently the individuals in the society the ultimate beneficiaries of this declared objective.

But these elements are not only defining the living standard, they also define the chance of survival and continuity of the corporate and subsequently the individuals and the society in general ensuring certain stability for their development creating through that a sustainable security.

The concept of human security has been slowly developing since it first surfaced in the Maslow pyramid of needs and later in the UNHDP Report in 1994. In box 2.6 of the report, selected indicators of human security risks are listed. These are food insecurity, job and income insecurity, human rights violations, ethnic or religious conflicts, inequity and military spending (Human Development Report, UNDP, 1994).

The International Committee of Red Cross (ICRC) defines economic security as the condition of an individual, household or community that is able to cover its essential needs and unavoidable expenditures in a sustainable manner, according to its cultural standards. Needs include: food, shelter, access to health care, access to education, and fair tax regime among others. Food alone is not sufficient (ICRC, 2008).

The above mentioned definitions were only dealing with the material part of Man's and society's needs and aspirations. This focus on materialistic aspects may be understood in the frame of considering economics as a positive science, but it should also be put in the frame of a capitalist economy. They are more quantifiable than other aspects.

But if we consider the safety and security needs, it will be clear that, both the actual need for physical safety and the need to feel secure from threatening events or surroundings, refer to relieves such as order, stability, routine, familiarity, and control over one's life and environment. This leads us to speak about Happiness, which is a need or requirement ranked higher than the achievement of materialistic income (Ruckriegel, 2007).

This was proven through the Easterlin-Paradox which indicates that happiness is not related to the absolute income but to the relative one (Easterlin, 2005). This didn't inhibit the critics saying that happiness is in any case, not a simple empirical phenomenon but a cultural and historical moving target (Wilkinson, 2007).

We can summarize the retained variables and their categories in the following table:

Table 1. List of security Variables.

#	Category of the variable 1=Material 2=Non- material 3= Values	Security Variable***
1	1	Basic conditions: Food , shelter, work, health care and education
2	1	Guaranteed minimal social security
3	1	Physical integrity (personal security),
4	1	GDP level, per capita income, inflation , National Debts
5	1	Circulation of money, Affordable taxation
6	1	Stable condition for business development, foreign investments
7	1	Sound Financial regulation
8	1	Control of technical development
9	2	Mental integrity
10	3	Freedom of belief, Tolerance
11	2	Providing welfare, solidarity
12	3	Personal belonging, trust and confidence, dignity
13	2	Family relation and broad social cohesion**
14	2	Job satisfaction
15	3	Equity, Equality, Fairness

** With social cohesion we understand the combination of tolerance of differences (race, culture, minorities, social structure and cultural order)

***Originally they were 33 variables, they are grouped here for this paper

Reasons for Financial Crises

International financial crisis can be considered as a nexus of foreign exchange market disturbances, debt defaults (sovereign or private), and banking system failures: a triple crisis, in which the interactions are the key to causality, depth, and persistence (Eichengreen 1987).

Some persons would also add globalization as a factor making a crisis international in today's context leading to problems (Carse, 1999).

In way to understand the impact of financial crisis on security variables and therefore on stability and security, we are going to categorize the reasons behind the financial crises (with focus on the last one) into two set of reasons: Technical set and Ethical set of reasons.

Technical set of reasons

A deeper look to the financial crises –especially the subprime crisis- will give us several technical reasons behind it (not sorted according to the size of their impacts and only shortly explained, the code of each reason is used for reference in the next tables):

1. **Economical cycle (T1)**

   The congruence of the end of a growth period with the blast of a bubble creates a double impact on the economy with deeper impacts.

2. **Distribution of risks through interests based financing (T2)**

   The actual business model is based on charging interests against mortgages and then securitizing the total on the base of -again- charging interests is a manner of transferring the risk from one party to another one, with the creation of unbalanced burdens. In case of crisis, distabilizing one element of the chain may lead to a global destabilization of existing structures.

3. **Dissociation of finance and real economy (T3)**

   It is agreed upon today that through the divorce between finance and the underlying projects there is weak direct participation of finance to the development of the real economy. Institutions providing loans are more concerned with the credit ratings or the financial intermediaries than whith the actual projects being funded (Wilson 1998). Several channels between financial system and real economy do exist (Cecetti 2009) whether they are properly used or not is the issue.

   The "funding costs" channel was actually the start for the actual financial crisis, due to the change of the interest rates. All the other channels reacted as consequence to the first one and to other factors in the set of reasons leading to the crisis.

   The problem is that in case of debt financing, the implication of any crash may not be limited to the persons or institutions involved but spill over to the rest of the system or even goes beyond the region as it is observed nowadays. This spillover may harm all types of deposit institutions once public confidence is shaken, with as result destabilizing the whole economy regardless of the sector or the branch due to the lack of confidence, the lack of liquidity or the lower demand added to the channels mentioned above.

4. **The essence and implementation of the Home Mortgages system (T4)**

   Mortgage is an essential credit form in the capitalist economy. We do here look at the subprime mortgage market and let aside the prime mortgage market. Despite that banks are traditionally conservative in doing business; banks didn't use the same strict conditions to lend the money as the prime market. Mortgages were given with less control; loans were given to clients with poor or no credit histories.

   In US, the reasons behind this development in banks' attitudes were politically, legally, technically and business driven:

   (T4.1) Change in the usage of a law named Community Reinvestment Act (CRA)

   (T4.2) Poor regulation:

   (T4.3) The US financial policy subsidized homeownership in several ways promoting financial fragility in the real estate market.

   Several mainstream scholars, using different methods of scientific inquiry, have concluded that the Fed's accommodative monetary policy and the applied interest rates following the 2001 recession caused the housing boom that followed, Taylor (2007).

   (T4.4) The impact of technological development on mortgage business' landscape.

(T4.5) Networking -through the game of "being-member-of-board"-, created business clans and lobbies. As consequence the distribution of the benefits and privileges happened according to persons' and corporate' interests.

(T.4.6) The operational structure of the system itself. The capitalist system is by nature greedy, steady growth is the key word, the company or the personal or the nation successes are measured by terms of money, expansion, growth, and control.

5. **The lack of risk analysis and the tendency to minimize the impact (T5)**
   Actually, each developed country has a security net in its financial regulation, guaranteeing the safety of deposit and taking care about the failure of banks. The International Monetry Fund (IMF) and the World Bank (WB) as well as some transnational organizations or Development Banks are playing such role for the other countries or on the level of the countries. This gives the impression that failure would never be as dramatic as previous crises. If we add to it the belief that "too big to fail" rule applies, then we see the extended limits of risk acceptance in the business model.

6. **Everything is a commodity for sale as long as partners accept the terms (T6)**
   Within this frame, time is considered a good; money, debts, information, rating of companies, security, personal resources, feelings, values, virtual objects and documents recognizing debts, all are goods. Since they are all goods, this means that they are tradable according to the rules of trading goods; it also means that they are quantifiable and subject to the market laws, to abundance and scarcity as well. This may not be applicable to all "goods" in the same way.

7. **The globalization and belief in a self problem resolving financial system (T7)**
   Shifting the crises from one part of the world to another is one characteristic of the global economy of today. When all players are involved it is easier to continue the game where all are contributing in it. The naïve belief that the market can regulate itself as if the market has a concerted, integrated intelligence and shares the same interests is part of the misleading elements.

Ethical set of reasons

Another set of elements could help to explain the reasons of the financial crisis; they are the "Ethical set of reasons". Here they are presented unsorted:

(E1) "The level of actual ethics embedded in business systems and institutions" (Crane 2010). The capitalist system is based on the theories of Adam Smith; David Ricardo gives a great weight to the individual satisfaction and action, linked in the case of Adam Smith to a certain personal ethic. The definitions of ethic and satisfaction are too open and hard to control in a time where the individual and his search for personal satisfaction became the center of a complete materialized world.

(E2) Actually, Man is developing and applying the ethical rules, this creates de facto a conflict of interest since Man is the legislator, the actor and the judge at the same time.

Additional reasons standing behind the financial crises could be named (Duska 2006):

(E4) Self-interest sometimes morphs into greed and selfishness,

(E5) Some people suffer from stunted moral development

(E6) Some people equate moral behavior with legal behavior, disregarding the fact that even though an action may not be illegal, it still may not be moral.

(E7) Professional duty can conflict with company demands.

(E8) Individual responsibility can wither under unethical demands of the client

(E9) The dissociation between individuals and society in term of interests is also behind the crises: "We lost sight of the structural questions - the systemic questions of how does a certain set of actions in the financial world affect all parts of society rather than that how does this affect those part of society that have most access to the public forum" (Cowley Catherine, 2006)

(E10) The double standards applied in the society regardless whether this is fair, accepted or allowed. The best example –among others- is the myth of "too big to fail" which created differentiated treatment among touched persons or organizations.

The link between the two sets of reasons

The link between the two sets of reasons (technical and ethical) is evident, since the latter influences the personal as well as the collective behavior of decision makers and consumers as well. The dissociation between the two sets of reasons represents some of the roots behind the recurrence of the financial crises.

We do here share the widely spread idea among politicians, economists and financiers that 'Better information', 'early warning' and 'preventive measures' will not remove the need for orderly workouts, whatever the source(s) of the crisis (Richard Portes, 1998); this workout could only be based on a comprehensive ethical measures in addition to the other measures.

The presentation of the financial crisis as just a technical failure is misleading. It is a combination of both technical and ethical.

The Impacts of Financial Crises

The impact of the crisis is the motivation behind an economical instability. The depth of the impact is behind the definitive results of a crisis including instability and security issues on different levels. In fact, in today's world of integrated capital markets, financial crises easily assume international dimensions. This leads us to say, that any of the impacts and the security variables should be taken with consideration to two issues:

1. The culture of the given society, countries or community
2. The actual economical, political and social situations in that given society or country.

Even well managed economies may fall prey to contagion effects, through trade, investment and speculation linkages or changing market sentiment, like what happened lately to Greek financial system and its impact on EU member countries. This transforms financial crises, which may start as national public bads, into regional bads, and eventually global public bads (IMF, 2002).

We are going to focus more specifically on the latest GFC.

Impact of the financial crisis on the economy (C1)

The actual and definitive figures for the actual financial crisis are difficult to know. It may even be difficult to imagine, for instance, an attempt to measure all the costs of a financial-crisis episode (IMF, 2002).

An estimation of IMF made in August 2009 mention the total figure of 11.9 Trillion US$, where 10.2 were for the developed countries while the Emerging states have contributed only with 1.7 trillion (Info Making Money, 2009).

Impact of financial crisis on retirement security (C2)

The impact of the financial crisis on the retirement security is coming from three sides:

1. The return on the amount invested by social security schemes
2. The higher number of unemployed people, leading to less participation and saving in retirement schemes.
3. The exposure to large market swings, as we have experienced twice in the past decade, can send individual investors scrambling for an exit at the most inopportune time. This prevents them from saving enough, and actually increases their exposure to financial market risks and lower retirement saving (Weller 2008 and Munnell 2009).
4. Not only the basic retirement schemes were hit, but also the complementary one like the American 401(k) plans (Munnell 2009).

Impact of financial crisis gender equality (C3)

The threat to gains in promoting gender equality, reducing poverty and hunger, achieving universal education and improving women's health — in fact, to all of the Millennium Development Goals — is serious.

The quality of and access to health care is likely to deteriorate significantly as a result of the crisis, obliging women to take on an increasing burden of unpaid care-giving responsibilities and further restricting their opportunities for paid employment (Alberdi, 2009).

Impact of financial crisis on employment (C4)

During the Asian financial crisis 1998 unemployment rates increased many folds in Asian countries (Fallon 2002).

Regarding the GFC, according to the director general of the ILO (Figure 1) , the global unemployment could affect 231 million people in 2009, an increase of 52 million as compared to 2007(Trendsupdate 2009).

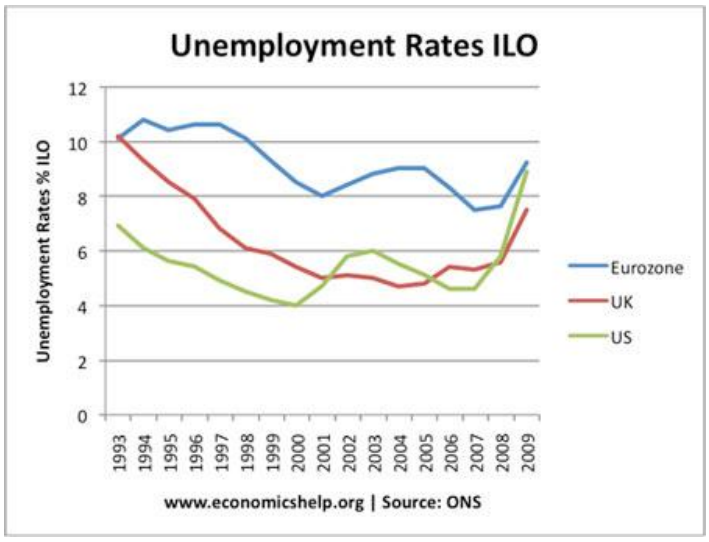


Figure 1. ILO Unemployment rates 1993-2009.

The Bank for International settlements doubts that the current crisis will be typical in its impact on deficits and debt. The reason is that, in many countries, employment and growth are unlikely to return to their pre-crisis levels in the foreseeable future (BIS, 2010):

The employment situation was the worst in the US. The number of net losses during the middle of the crisis was tremendous with 1'763'000 lost jobs for the first 3 quarters of 2000 (Boyer, 2009):

Impact of financial crisis on health and poverty (C5)

According to several studies, sharp economic slowdowns and low levels of income per capita appear to increase the likelihood of conflicts (Kim, 2009).

The crisis comes at a time when the Millennium Development Goals has never been higher. It comes in the midst of the most ambitious drive in history to reduce poverty and distribute the benefits of our modern society, including those related to health, more evenly and fairly in this world (Chan, 2008).

Developing countries expects to have 53 million more people forced to live on less than $2 a day in 2009; this will wipe out much of the progress made through the Millenium Development Goals (NS Network, 2009).

The problem with the health sector is that crises' effects are to be observed on the long term, because budgets were shifted away from investments in the social sectors, most notably health and education and many countries are still suffering the legacy of these errors (Chan, 2008).

Impact of financial crisis on food supply (C6)

According to IFAD, as result of the GFC consumers are responding by eating less and shifting to less nutritious food (The Crawford Fund, 2009).

The financial crisis, along with still high food prices, reduces access to food for many household. In addition to that, the affected government social services, trade, investment, aid, remittances, and exchange rates, will make the food less accessible and imports more expensive. (UN Task Force, 2009).

In addition, speculators looking for assets with rising prices re-oriented their portfolios towards food commodities; this came along with the rising demand on bio-fuel, together with the decline in agricultural production (UNCTAD, 2008).

Speculations skewing agriculture commodity market to such a degree that both farmers and consumers are losing out (IATP, 2008).

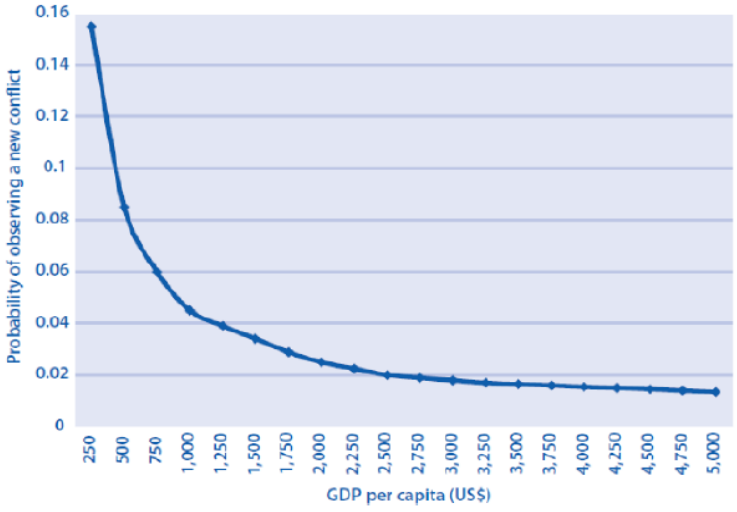
Impact of financial crisis on small crime, identity theft and fraud (C7)

A research report prepared for the congress showed that there was a clear relation between economic factors and crime in the cities of the US. The factors used in the study were unemployment and foreclosure. At the same time, the relation was established between the increase in number of unemployed and number of foreclosures happening during the crisis periods concerning violent crimes and property crime (Finklea, 2009)

But the impact of the financial crisis is not limited to the violent or property crimes. The worldwide financial crisis is also exacerbating Americans' fear of identity theft, according to research conducted by Unisys Corp. In this survey, ninety percent are also at least somewhat concerned about becoming victims of credit or debit-card fraud, compared to slightly more than 85 percent in fall 2008.

Impact of financial crisis on national and regional security (C8)

An extensive and inconclusive literature on relation between economic conditions and security (internal and external) does exist. Ibn Khaldoun, Marx, Tocqueville, Michiavelli, Hoffer, Deng and Huntington, they all mentioned the relation in different forms and visions creating schools of thoughts like the realists and the idealists.



Note: The graph is based on data and a model from Collier and Hoeffler, 2002, pp. 13–28. Humphreys and Varshney, "use[d] the Collier-Hoeffler (2002) model to predict the expected probability of civil war onset conditional upon different income levels ranging from US$250 to US$5,000. To make these predictions [they held] all other variables constant at their means".

Source: Humphreys (2003, p.2), as reported d in UNDP (2008a).

Figure 2. GDP per capita and probability of new conflict.

Recently, Admiral Dennis Blair US intelligence chief warned that the economic crisis may be the source of the primary threat to global security right now. Security experts note that the economic downturn is already creating social unrest and political instability in some strategic hot spots around the world (Trumley 2009). The risk of instability for certain regimes will increase if the crisis persists for a certain time. Economic drivers matter in part because it is economic characteristics that make a rebellion/conflict feasible, it enables fighting parties to buy the weapons, to maintain a private army over long periods, and to perpetrate large scale killing without endangering themselves (Collier, 2006).

Here the issue of proliferation is part of crisis' impacts. The diminishing contribution to the budget of international defense organizations like the NATO may also be an aspect.

Certain researches proved that there is a direct relation between the economic development and conflicts and that the level of GDP is negatively correlated with observing a new conflict (Kim 2009).

After this analysis (summary in table 2), we can say without being far away from the truth that, the actual economical and financial model with all its rules, regulations and organizations couldn't stop the recurrence and repetition of economic and financial crises as well as reducing their impacts on the long term.

It is clear that the level of the impacts is not the same for all security variables. At the same time, the levels of impacts on variables are not everywhere the same, nor are they perceived with the same degree of seriousness.

To have a serious danger on security, a certain degree of pain should be resented by the studied person or group. It is well known that it is important to study pain reactions keeping the socio-cultural factors in mind (Zborowski, 1952), therefore that is very difficult to estimate the total risk on security.

At this stage we get a serious problem since economy instead of being a reason for stability and security –as we defined it at the beginning- is transformed in reason for instability and possible turbulences.

An Ethical Proposed Solution

Our intention is to oppose a global solution to a global crisis dealing with all the above mentioned aspects whether in terms of reasons or in terms of impacts.

A world which is obliged to produce for each event new regulations and forget others, is reflecting its failure. The first handicap is having the Man as player, judge and legislator. Philosophically it doesn't work because of the conflict of interests.

We are going here to present an alternative which is an old one in new shape, adapted to contemporary conditions and contexts.

The alternative is tackling the deep roots of the economical logic, mechanisms and means. This alternative has -in its form and depth- to be comprehensive.

We may name the alternative Islamic Ethical Financial Model (IEFM).

This proposal of having religion in the center of a "materialistic" issue may seems strange for many of us. But to the same results came also different thinkers. In fact, Fukuyama said in 1997: "without the transcendental sanctions posed by religion … modern societies would come apart at the seams". (Fukuyama,1997).

Islam and the economical system:

Actually, Islam arrived with a revolutionary spirit, revolution against: injustice made by strong toward weak, inequity between rich and poor, harm done from men to women, undermining of countrymen by citizens, exploitation of slaves by "freemen", hegemony of society over the individuals, corruption of the society by individuals, etc.

Islam in its vision for a sustainable durable equitable solution integrated all life's aspects whether material, intellectual or spiritual and advanced two very basic dimensions:

First Dimension (Shifting egocentrism) Economical and financial rules (I1):

Islam moved the Man from his absolute egocentric position to a neighboring position where his interests, needs and resources are meeting those of others in a stronger global harmony, relativizing through that the nature of pure materialistic scope and objectives.

The system includes economic and financial rules as well as social directives and injunctions based on principles like:

(I1.1) profit and loss sharing (instead of interest based transactions),
(I1.2) risk sharing (and not risk transfer as prescribed by conventional system),
(I1.3) link between assets, financial transaction and real economies.
(I1.4) Transparent transactions, far from speculation and mainly asset based,
(I1.5) role of the state (guarantor of equitable chances)
(I1.6) role of the work in the economy (as main source of wealth)
(I1.7) wealth and ownership rules
(I1.8) and collaborative insurance system (as the active part of the safety net)
(I1.9) solidarity and institution of charity (as a part of the socio-economic system)
(I1.10) Decision should be taken in accordance to equity and justice as well as following the rule of closing the door of interested motivations
(I1.11) Actions are to follow the rule of no harm (one himself) and no harming (others)

The system is based on the Quran, the Sunnah of the Prophet and the consensus of the Muslim scholars, as well as on the precise methodology developed by scholars during 14 centuries responding to the needs and the aspirations of the people and institutions. The development is continuing nowadays with all possible and imaginable challenges, successes and mistakes.

This IEFM system –as any system- has its products, methodologies, mechanisms, processes and benchmarking which are derived from the above mentioned principles.

Some of the principles, products or issues are:

(I1.12) Prohibition of interest rates and using instead the principle of profit and loss sharing with an equitable distribution of risks. Several financial products were developed for this purpose garanteeing: equity in contribution, mutual counseling, agreed upon contingencies, transparent mechanisms and sharing the outcome of the operation. At the same time every transaction is supposed to be asset backed.

The possibility of securitization is also existing through the different models of Sukuk.

(I1.13) Other instruments with more financial security in term of return were also developed like Ijara (renting) offering fix rate of return. This is also used in a type of Sukuk. On the top insurance products were developed on the base of mutual interest.

Second dimension Ethical and moral values (I2):

In addition to the two dimensions of rights and feelings which are venerated by the Man, a symbiosis between Man, his material and spiritual needs and the cosmos in general should be established. The IEFM gives Man and his transactions a new dimension combining:

- A set of moral and ethical values in business, where the rules and regulations should fit within.
- Response to Man's aspirations for social justice, welfare and spirituality
- Tthus creating -mainly- a "self-control system" (through education and raising awareness).

These points may be an efficient remedy to the possible shortcomings of the first set which remains –by its nature- tightly linked to legal aspects, rules and regulations. The first idea about egocentrism and its set of recommendations and rules is exogenous to the human being and may create some constraints The second set brings the right supporting frame to the first idea leading to self-satisfaction and may offers much bigger chance of success.

Let us take the idea of values: When we mention moral values we mean respect paid to the work, to the workers, to the laws, to the other human beings, to the nature in its multiple dimensions, trust in one's and other's capacity and engagement, perfection and honesty at work, utility of the conducted activity, perseverance, equity, justice, mercy, generosity, love, etc. Interestingly, these values are shared by all "normal" human beings if they were to be asked. When it comes to apply them on own person or interests, then the logic and the measurement change.

These moral values are covering the domain of distribution of production, of consumption, of exchange and of distribution. There shouldn't be superiority for economic logic over the moral values.

Welfare and social justice may be linked to the spiritual aspiration: The idea is that this type of elements is part of the human instinct; it is part of the Happiness search of each person. The fulfillment of Man's aspirations is part of Man's need for global security, where global means: the cosmos wide and beyond the measured time-space dimension of individuals and groups – as example on collective level and beyond the human time span, the transmission of an intact environment to next generations-, hence balancing materialistic needs and non-materialistic ones to reach the global sustainable success and Happiness resulting in stable and balanced behaviors in term of production, consumption, exchange and distribution.

Way and impact of the application of the Islamic principles on security:

The fulfillment of these aspirations needs –for our case- a re-integration of the ethical education in every day life.

The purpose is to have: a better education, sound understanding of one himself in his global dimension, a better exchange of ideas and experiences, a combination of a self-control system and a constructive solidarity to follow the ethical path despite the materialistic temptations.

This integration –in way to be effective- requires not separating personal life from economic life and public life. It doesn't means having a religious economy in the dogmatic form and essence, with a fix set of rules and directives supervised by narrow minded theologists. We think about a moral and ethical economy model.

In our proposal we don't forget that "while a certain degree of regulation is indispensable to ensure competition, maintain order and standards, and safeguard the rights of others, excessive regulation can prove to be a great burden. The absence of moral dimension leads to more and more regulations". (Chapra, 2007)

Having all that in the daily life requires a consequent moral-ethical education imbedded in the whole education process to reach ethical behavior.

The hope for reaching such ambitious objective lays in strengthening the dialogue between the supporters of the ethical values: religious, political, economic, intellectual persons, entities, institutions and organization.

If we take the sum of all the above mentioned elements and transpose them on the macro level in the next table we may have the following links as keys for establishing a certain stability:

Table 2. Security variable and influence of Alternative model.

#	Category of the variable 1=Material 2=Non-material 3= Values	Security Variable****	Influenced by the following results of financial crises	Influenced by the following Causes of financial crisis	Influence of IEFM
1	1	Basic conditions: Food , shelter, work, health care and education	C4, C5, C6	T3, T4.1	I1.1, I1.2, I1.6, I1.7, I1.9
2	1	guaranteed minimal social security	C1, C2, C5		I1.5, I1.8,I1.9,
3	1	Physical integrity (personal security),	C7, C8	T6	I1.5, I1.9, I1.10, I1.11
4	1	GDP level, per capita income, inflation , National Debts	C1, C8, C2, C4; C5	T2, T3; T4,3	I1.4, I1.5, I1.6
5	1	Circulation of money, Affordable taxation	C1, C5	T2, T3	I1.4, I1.5, I1.7, I1.9, I2
6	1	Stable condition for business development, foreign investments	C1, C4; C7, C8	T2, T3; T5	I1.5, I1.6, I1.10, I1.2, I1.4, I2
7	1	Sound Financial regulation		T4.2, E7	I1.5, I2
8	1	Control of technical development		T4.4	I1.5
9	2	Mental integrity	C3, C5, C8		I2
10	3	Freedom of belief, Tolerance	C8		I1.5, I1.10, I2
11	2	Providing welfare, solidarity	C5,C8	E1, E9, T4.6, E4	I1.5, I1.7, I1.9, I2
12	3	Personal belonging, trust and confidence, dignity	C3, C4, C5, C8	T3, T4.5,T7 E8	I1.5, I 1.9, I2
13	2	Family relation and broad social cohesion	C3, C7	E4, E9	I1.5, I1.8, I1.9, I2
14	2	Job satisfaction	C4, C5	E8	I1.5, I2
15	3	Equity, Equality, Fairness	C3, C4, C5	T6, E10	I1.4, I1.5, I1.10, I1.11, I2,

Discussion and Conclusions

Does Islamic Ethical Financial Model prevent from crises?

The proposed system –as any system bringing together a bunch of rules and directives- will lead only to soften the amplitude of the crises and reduce their frequencies but will not deactivate them, for at least one reason: not all crises' elements are controllable. Think about natural disasters, wars, different applied systems in an international environment, etc.

Not to forget that we deal with human beings. Human beings are very different in their behaviors and attitudes and may with the time change too.

Does this system offer a viable solution? Do we have a "proof of concept"?

The system as it is today is not able to really create an comprehensive efficient economical and financial system and hence reduce globally the impacts of crises due to several reasons:

1. The lack of political support.
2. The lack of resources –mainly personal.
3. The lack in creativity and objective orientation in product development due- among others- to lack in human resources.
4. The frozen structures within and above the Islamic financial organizations.
5. The financial inefficiency due to several reasons and the abscense of a needed critical mass.
6. Lack of coordination and collaboration in term of knowledge transfer and exchange of experiences, etc.

As we could establish through this shortened paper, the financial crises are a threat to the stability of individual, corporate, society and countries and as consequence a potential threat to the security if not a source for conflicts.

The situation is worsening in term of the development of the crises' size, number of persons, countries and amounts involved, as well as the frequency of recurrence.

The crises' reasons and their impacts were linked to security variables with the objective to prevent the crises from happening and reduce their impacts.

We proposed as alternative to today's system the IEFM and linked it to the variables. In the annex the model was applied on the sub-prime crisis to show its impact on its elements.

Many questions are to be answered about the inter-relation and cross-influences between the variables and the models. A quantitative and impirical research on the variables over longer period could provide us with additional information about the importance of each security variable. The selection of the variables should be part of a comprehensive security concept or theory on macro as well as micro levels. Defining and prioritizing the security variables would make it possible to see or measure the pre-signs of a crises and allows a better definition of the domains of actions in way to strengthen the stability and security if crises happen.. These points are parts of the further study which we are conducting.

Two other ideas which may be of interest is to analyse the possible development of the selected variables within the frame of future studies to read the possible trends and see if the proposed model will reduce or inhibit the negative developments.

The second point would be to study how to bring the ethical values into application during a transitional period which the education may need to change mentalities and behaviors.

References

Alberdi Inés, (2009) *Executive director, UNIFEM, "The World Economic and Financial Crisis: What Will It Mean for Gender Equality?*" at Fifth Annual Meeting of Women Speakers of Parliament, Vienna, Austria.

Crane Andrew and Dirk Matten (2010), *Schulich School of Business in York University-Toronto*, retrieved from: http://craneandmatten.blogspot.com/, retrieved: 20.03.2010

BIS Working Papers # 300 (2010): The future of public debt: prospects and implications, Bank for International Settlement.

Boyer Marcel, (2009) *"The economic crisis and its impact on employment"*, Montreal Economic Institute Research Paper.

Carse David (1999), Deputy Chief Executive, Hong Kong Monetary Authority, speech at Banking Conference on Banking ethics, *"The Importance of Ethics in Banking"*, Hong Kong.

Cecchetti Stephen, Kohler Marion and Upper Christian (2009); *Financial Crises and Economic Activity, article.*

Chan Margaret (2008), *Dr. WHO Director-General, Impact of the global financial and economic crisis on health*, Statement by, 12 November 2008

Chapra Umer (2007), Dr., *ETHICS AND ECONOMICS IN ISLAM AND THE WEST*, , seminar organized by the Goethe Institute, Munich, Germany, and the Dar al-Fikr, Damascus, Syria, in Damascus on 21 June 2007.

Collier Paul (2009), Anke Höffler and Dominic Rohner; *"Beyond Greed and Grievance: feasibility and civil war"* Oxford economic papers 61(1).

Cowley Catherine (2006), Prof. *"The Value of Money: Ethics and the World of Finance"*, T. & T. Clark Publishers, Ltd.

Crumley Bruce and Karon Tony, Time, 25.02.2009; http://www.time.com/time/world/article/0,8599,1881492,00.html; retrieved 16.04.2010.

Database (2008) , *IMF Working Paper, WP/08/224.*

Duska Ronald F. and Mitchell James A. (2008- adapted from speech) at the meeting of the Business and Organizational Ethics Partnership, Center for Ethical Business Cultures, University of St. Thomas College of Business.

Easterlin, R.A. (2005), *"Building a Better Theory of Well-Being"*, in: Bruni, L., Porta, P.L., "Economics and Happiness – Framing the Analyses", Oxford..

Eichengreen Barry and Portes Richard, 1987, *"The anatomy of financial crises"*, in Richard Portes and Alexandre Swoboda (eds.), Cambridge University Press.

Fallon Peter R. and Lucas Robert E. B.(2002), *The Impact of Financial Crises on Labor Markets, Household Incomes, and Poverty: A Review of the Evidence, 17 The World Bank Observer* (Spring 2002), 24–25.

Finklea Kristin M.(2009); *Economic Downturns and Crime*, CRS Report for Congress, July 28, 2009

Fukuyama, Francis (1997), *The End of Order* (London: The Social Market Foundation), P8.

Gorton Gary (2010), *"Questions and Answers about the Financial Crisis"*, report prepared for the U.S. Financial Crisis Inquiry Commission Yale and NBER, February 20, 2010

IATP (2008); *"Commodities Market Speculation: The Risk to Food Security and Agriculture"*; IATP's Trade and Global Governance program; November 2008

imarketnews; Bernanke: *Economic Costs of Financial Crisis 'Very Severe'*; http://imarketnews.com/?q=node/10561; 20.03.2010, retrieved 16.04.2010.

IMF 2002, *"Profiling the Provision Status of Global Public Goods"*, ODS Staff paper, 2002

Infomaking money; IMF estimated costs of financial crisis at almost 12,000 billion dollars; http://www.infomakingmoney.com/finance/imf-estimated-costs-of-financial-crisis-at-almost-12000-billion-dollars.html, 2009, retrieved 12.03.2010.

International Committee for Red Cross (ICRC) (2008), *"Economic Security"*, 2008

Jain T.R., Grover M.L., Ohri V.K., Khanna O.P. (2006), *Economics for engineers*, V.K. Enterprises, New Delhi, India, 2006.

Kim Namsuk and Conceicao Pedro (2009), *"The economic Crisis, Violent conflict and Human development"*, UNDP/ODs Working paper.

McGee and Firman 2000, in Calum Miller, *The Human Development Impact of Economic Crises*, Human Development Report, Occasion Paper (2005), UNDP, 11.

Munnell Alicia H. (2009), Director, Center for Retirement Research, Boston College Carroll School of Management, *The Financial Crisis and Restoring Retirement Security, Testimony before the Committee on Education and Labor U.S. House of Representatives*, February 24, 2009.

Nazari Ismail Mohammad (2009); *"Financial Crises: Can They Be Prevented?"*, The E-Leader Conference, University of Malaya.

NS Network; *"The National Security Implications of the Global Financial Crisis"*; http://www.nsnetwork.org/node/1326; 29 May 2009, Retrieved 10.04.2010.

Portes Richard (1998), President, Centre for Economic Policy Research , at FRB Chicago / IMF Conference, Chicago, 8-10 October 1998.

Reinhart Carmen M., Rogoff S. Kenneth (2008), *"A panoramic view of eight centuries of financial crises"*, working paper 13882, national bureau of economic research.

Reinhart Carmen M., Rogoff S. Kenneth (2009); *"The Aftermath of Financial Crises"*; American Economic Association meetings in San Francisco.

Rokeach M. (1973), *The Nature of Human Values*, New York, The Free Press.

Ruckriegel Karlheinz Prof. Dr.(2007); *„Happiness Research (Glücksforschung) - eine Abkehr vom Materialismus"*; Georg-Simon-Ohm-Fachhochschule Nürnberg, Fakultät Betriebswirtschaft.

Taylor, John B.(2009); *"Housing and Monetary Policy."* In Housing, Housing Finance, and Monetary Policy. Kansas City: Federal Reserve Bank of Kansas City.

The Crawford Fund (2009), Speech *"The enduring world food crisis"*; Queensland rural press club, Australia, April 2009.

Trendsupdates; http://trendsupdates.com/ilo-financial-crisis-has-become-a-%E2%80%98global-job-crisis%E2%80%99/, 26.03.2010; retrieved: 12.04.2010.

UNECTAD(2008); *"Tackling the global food crisis"*; Policy Briefs, N. 2; June, 2008

UN Task Force on the Global Food Security Crisis (2009), Report: *"Global economic turmoil intensifies the food crisis"*; 2009

Weller Christian E., Ph.D, (2008) Lessons from the Financial Crisis for Retirement Security: Building Better Retirement Plans, Testimony before the U.S. House of Representatives Committee on Education and Labor *"The Impact of the Financial Crisis on Workers' Retirement Security"*, October 7, 2008

Wikinson Will (2007); *" In Pursuit of Happiness Research: Is It Reliable? What Does It Imply for Policy?"*; Cato Institute, Policy Analysis, April 2007.

Wilson R. (1998), *Islamic project finance and private financing scheme, IIUM Journal of economics and management*, No. 2, 1998.

Zborowski, M. (1952); *"Cultural components in response to pain"*, Journal of Social Issues 8 (4)

Annexes

Application of IEFM on the Subprime chain:

As an application we are going to apply the general IEFM rules on the chain of the process which created technically the subprime crisis.

First we may represent the whole process as follows:

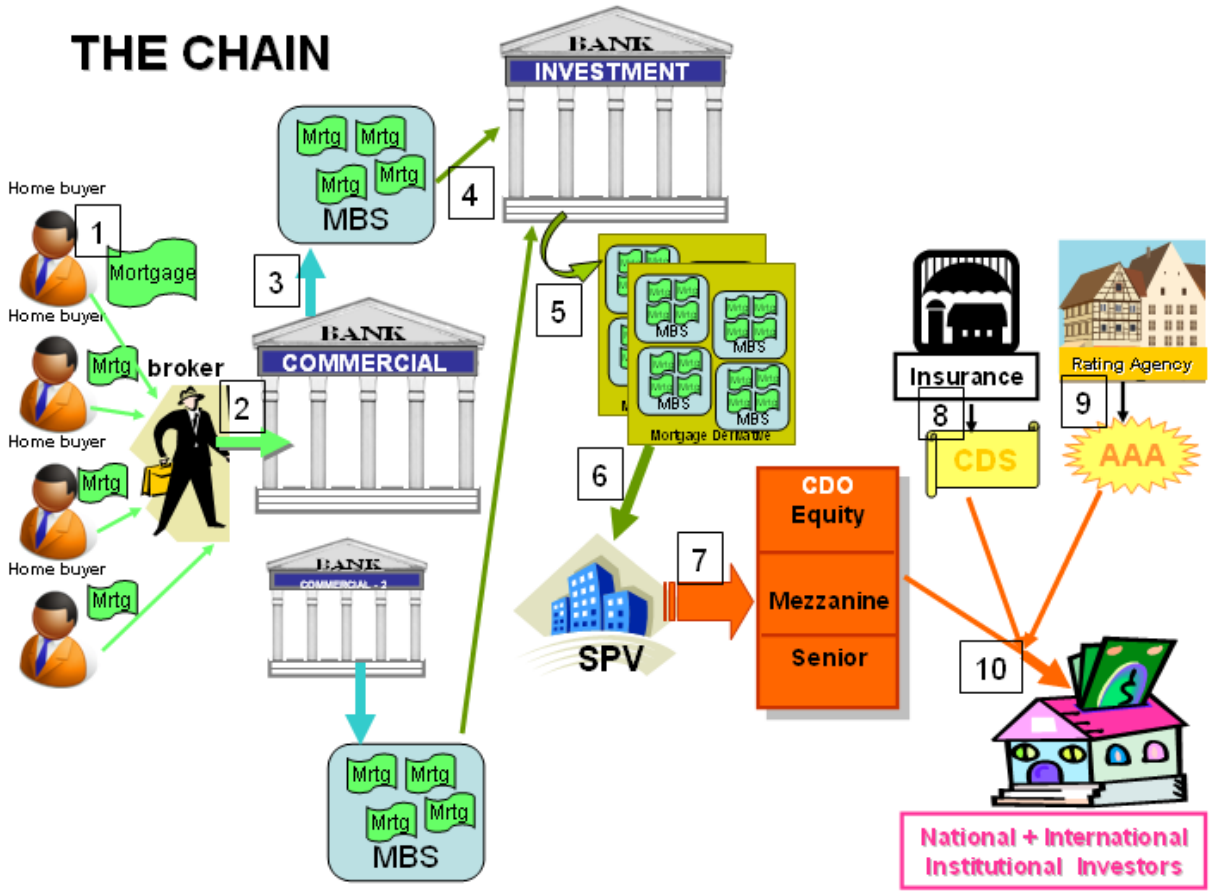


Figure 11. *The subprime chain*

Secondly, we analyze every step of the process and compare it with the IEFM rules:

Step	Process's step	Islamic Opinion	Islam. Model ref.	Islamic Alternative	Impact
1	Contracting a mortgage: money to home buyer, mortgaging home and interests to be paid	The contract between buyer and broker is a loan contract. Contract should not include interests	I1.1, I1.2, I1.3, I1.12,	Murabaha, Leasing, Diminishing Musharaka. Other possibilities do exist for developers through Istisna'.	Transparent transaction until its end, Risk shared, more engagement of the financier, no (or limited) role for brokers→ less fees
2	Selling the contract from broker to commercial bank for a fee or part of the to-be-paid-interest	It is not allowed to sell debts for benefits.	I.1, I.11, I1.1, I1.2, I1.3	Purchase at face value for the debts. Possibility to have broker as agent of the bank paid lump sum or as part of contracted capital.	Such transaction will not work in this form. Knowing that the financier will think twice and evaluate the risks before contracting a mortgage.
3,4,5	Creating securities through MBS in way to make them easier tradable and cross cover the risks	It is not allowed to sell debts for benefits	I1.1, I1.2, I1.3, I1.4, I1.5, I1.10, I1.11, I 1.12, I2	Securitization is allowed but always linked to underlying asset, for example Sukuk al Ijarah.	Guaranteed transparence, sustained link between real and financial economy, larger risks to financier.
6	Creation of SPV and transferring the securities to them, releasing the bank from some legal obligation related to the ration Debt/asset and improving Balance Sheet's outlook	The purpose of such creation is rejected. The transfer of debt is not allowed. The "manipulation" of the BL is not allowed.	I1.1, I1.2, I1.3, I1.4, I1.5, I1.10, I1.11, I 1.12, I2	Creation of special entity dealing with this type of business with the adequate capital and means.	Less intermediary, more transparency, shorter chain between the ultimate financier and home buyers.

7	Slicing and dicing the securities hold by the SPV	This type of distribution of risks is rejected since risks are not dividable and not a good to be sold as such. The different treatment of ultimate holders is also rejected even if accepted by them. This case is considered a gambling	I1.1, I1.2, I1.3, I1.4, I1.5, I1.6, I1.10, I1.11, I 1.12, I2	Differentiated contracts linked to each home buyer's risk assessment could be envisaged (if this is conform to laws or to marketing strategies, is another issue)	Risk evenly distributed, security holders know what they have as assets for what conditions.
8	Insuring the certificates (CDS). The purpose is to get an insured sum if default happens and to improve the rating of the CDOs in way to make them acceptable to institutional investors.	This is insuring what is undefined, since it is not known where the default may happen, neither its size because the risk are distribute unevenly, at the same time, in the case of default the protection buyer delivers the defaulted CDO to the protection seller against the sum insured and not obligatory the face value, which is again a selling debts. The purpose of this insurance is not evident, since it includes the will to improve the rating to attract institutional clients. The other issue is the coverage and reserves put by insurers to cover the certificates. These insurances don't cover all risks since they are mixed. For example what happen if only a certain type of mortgages is defaulting because of changes in regulations concerning these mortgages and not the other?	I1.1, I1.2, I1.3, I1.4, I1.5, I1.8, I1.10, I1.11, I 1.12, I2	Insurance is allowed within the limits of certainty (against ambiguity) , of allowed product (no interest bearing) and not for profit seeking insurance company and certainly not for the purpose of misleading a potential buyer (through rating). The issue of the reserves presents also a point of difference.	Transparent transaction, better relationship between all players, less fees (because less premium due to the transparency and risk sharing instruments), keep closer to the real asset. Insured will think twice before getting in the collective insurance since he is responsible of covering the shortage in coverage.

9	Rating the CDOs through rating agencies in way to get CDOs' market price for potential global investors	Rating for improving the selling chances through institutions paid by issuers represents an unethical step and a conflict of interests. The examples show the misleading information propagated by rating agencies during this crisis as well other crises.	I1.1, I1.2, I1.3, I1.4, I1.5, I1.9, I1.10, I1.11, I 1.12, I2	Rating in term of evaluating the quality of an asset is allowed, but it should be independent. The rating remains linked to the asset and not to documents.	Less fees, clearer picture of the situation, closer to the asset
10	Selling to institutional investors	Investors are cheated due to his conviction that he is doing a good investment based on the information presented by different partners, without having himself any idea about what is behind the CDOs. The greed of the purchasers and the sellers as well as the costs linked to any possible investigation about the assets backing the CDOs will stop any deeper analysis. Uncertainty and deceiving are not allowed.		Through different models of securitization and direct asst backing.	Transparency, reduced fees and complexity in case of default or problems.

This short analysis on micro level (related to one crisis and to a certain product in a definite country) shows us the number of hurdles put by IEFM rules. They are applicable for all the steps and players whether mortgage, securitization or institutionalized investors. These rules enhance the confidence, reduce the parasite internediaries through improving transparency and accessibility to the real players and linking them directly, reuce the fees and costs hence increase the efficiency. This is certainly a contribution to the security.

The model, limits the possibilities of creating artificial financial bubbles not linked to real economy, therefore preserving the investors from surprises. This will stabilize these investors –many of them are social security, retirement and insurance funds-. This is an additional contribution to stability and security.

In addition, the model will discharge the national debts of the countries through higher taxation since no off-shore SPV are systematically needed and less bailout required to save bad players; this liberates means for other development projects and provides a stable business environment as well as enhancing the social cohesion.

All these elements together will create a stronger confidence and trust between the different players, since justice, equity and transparency are guaranteed. This is also an additional element strengthening the security.

4. CULTURE

SECURITY IN FUTURE SHOPPING MALLS

Raija Järvinen[a] & Katri Koistinen[b]
[a]Aalto University School of Economics, Department of Marketing and Management
[b]National Consumer Research Centre

ABSTRACT – *The paper deals with the content and importance of security in future shopping malls. Research data consists of three sub-studies including focus group discussions organised among consumers and semi-structured interviews among sales staff, shop owners and shop managers. The results of the study suggest that the importance of security is increasing and the security element consist of security systems, security guards, product quality and atmosphere. Based on the results three scenarios, human oriented, technology oriented and co-operative scenarios, are introduced.*

Introduction

Security can for good reason be considered one of the success factors in future shopping malls. If customers believe that the mall is not safe, they decide not to shop there (Hayes 2007). The study of Gips (1996) reveals that around ten per cent of customers avoid shopping malls because of feeling unsecured. On the other hand, both disorder and being a target for criminal activity prevent customers shopping habits and result smaller profits for retailers.

According to the study of Juvonen and Järvinen (2010) the store staff forecasts shoplifting, robbery, drug users and problematic patrons the most remarkable threats during the coming years. However, all kinds of smaller and bigger disturbance are being experienced in shopping malls every day, e.g. in Finnish malls alone there has been at least four serious damages during the last year: one smash-and-grab burglary, two plumbing leakages and one shooting. In spite of these and other risks research in the area of security in retailing context is scarce even at the international level

The purpose of the article is to discuss the content and importance of security in the future shopping malls. The empirical part is based on the studies by Koistinen and Peura-Kapanen (2009), Järvinen and Uuspelto (2009), and Juvonen and Järvinen (2010). All these pieces of research belong to the research project titled “Security and competitiveness in shopping centres” that is going on years 2008-2010. The framework of the paper is formed on the basis of the earlier published research. The paper is limited inside the shopping mall and thus outside areas, such as parking facilities, are left outside the scope of the paper.

The article is organized as follows: After introduction the framework of the study is presented, then data and methodology are described and results indicating the scenarios for more secure shopping malls are elaborated. The article ends up conclusions and suggestions how to improve security in future malls.

Framework of the study

The starting point of the article is based on the fact that in order to survive shopping malls are completely dependent on their customers. Successful shopping malls need to be attractive, i.e. preferable or favourable, for their customers on every single stage of the buying process (Teller & Reutterer 2008). Based on extensive literature review, Teller and Reutterer (2008) consider the most important attraction dimensions accessibility, parking, tenant mix, merchandise value, orientation, ambience, atmosphere and distance. Close to attraction are the criteria that customers use when they choose shopping mall. Koistinen and Järvinen (2009) have studied customer choice of retailing outlets and they conclude that price, quality, selection and assortment together with shopping environment are the most important criteria (see also Morschett et al. 2006). Pitkäaho et al. (2005) include also location and ease of patronizing among the choice criteria.

So far, only the study of Takkinen (2009) examines security as one of the key criteria of attraction. In this he refers to Mitchell and Harris (2005) who consider security as a part of general health and well-being including personal and car security, store design, cleanness and quality. However, the results of the study by Takkinen suggest that security in malls consists of pleasant atmosphere, reliability, honesty, high quality products, security guards and technical security systems. All in all, customers aim to optimize their needs in the shopping mall choice, and in this, security has influence at least to some extent (Takkinen 2009).

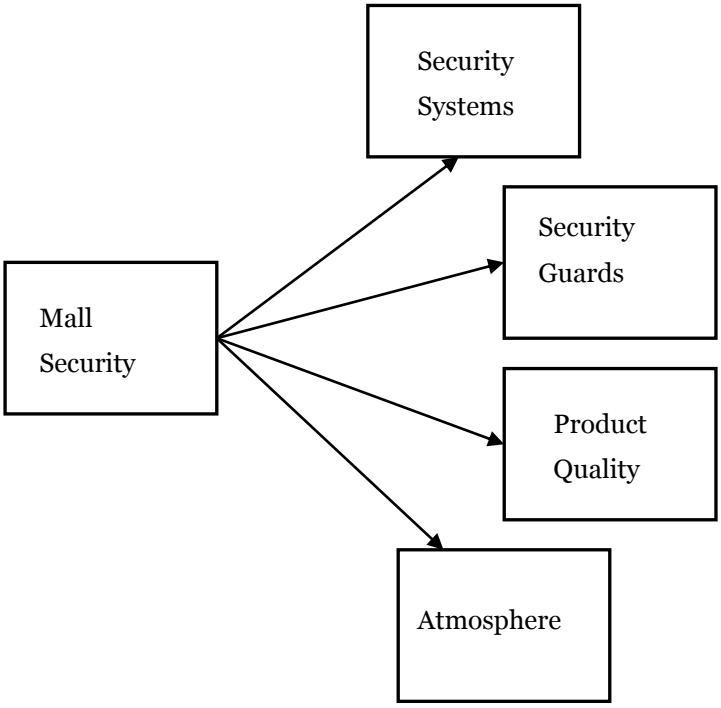


Figure 1. Elements of mall security.

Based on the above discussion the framework of the study is depicted in Figure 1. It is modified on the basis Takkinen's (2009) results, as there is in practice no other published research on the area of security connected to the retail outlet attraction or choice. In Figure 1 mall security from the consumer and personnel point of view consists of technical security systems, security guards, product quality and atmosphere. Security systems as construct covers all the technical devices and equipment required to

maintain security in modern shopping malls. Security guards on their turn are professionals that are employed by the mall to maintain security. Product quality refers to fresh, healthy and tasty food but also other first class products and assortments that please customers. Atmosphere, on the other hand, is a personal and social feeling that is experienced, but on the other hand it contains more concrete issues like store design, lights, music and style. In the framework mall atmosphere includes also reliability and honesty.

Data and Methods

Research data consists of three sub-studies including focus group discussions organised among consumers and semi-structured interviews among sales staff, shop owners and shop managers (called here on 'staff'). The focus groups were formed of consumers living in Helsinki and Turku areas (urban, suburban and rural areas around the two cities) in 2009 and a total of 40 consumers participated in seven discussions. The first semi-structured interviews consists of 16 interviews; two safe guards, three shop owners, five shop managers and six members of sales staff. The interviews were carried out in 2008. The second round of semi-structured interviews were conducted in 2009 consisting of 18 participants of which five shop owners, four shop managers and nine representatives of sales staff.

All three conducted studies are qualitative in their nature. The reason for this choice lies on the limited number of published studies in this research field. In qualitative research to some degree, data collection, analysis and interpretation take place simultaneously (Gummesson 2005). Focus group method is recommended especially in cases when consumer experience, perspective or opinions are studied (Barbour & Kitzinger 1999; Bloor et al. 2001). On the other hand, the major advantage of semi-structured interviews is that data gathered is rather systematic and comprehensive, but interviews are still conversational and informal (Eriksson & Kovalainen 2008). Research data was organised according to the security elements in the framework, and data of each element was analysed by content analysis.

Scenarios have become a paradigm of future studies (Mannermaa 1991). In retailing the future is projected by studying factors that affect long-run performance and then forming contingency plans based on alternative scenarios (Berman & Evans 2004). Consequently, on the basis of the sub-studies we suggest three alternative scenarios.

Häyrynen (2009) calls scenarios as future manuscripts. A scenario is a snapshot of a possible, plausible future outcome. Scenarios are either deterministic or stochastic. An analysis based on deterministic scenarios typically considers just a few scenarios. These scenarios might be historical or hypothetical. A historical scenario reflects a significant event that has occurred in the past, and a hypothetical scenario reflects a significant event that is deemed plausible, but has not yet occurred. (Swiss Re 2009) In this paper the scenarios are deterministic owing elements of both historical and hypothetical perspective. In addition, the method and data of our scenarios are qualitative, although scenarios usually employ quantitative data. Qualitative scenarios can be used to develop alternative views of the future that are meant to stimulate thinking about how to respond to changes, for example, in the business environment. (cf. Swiss Re 2009)

In this paper, the scenarios are mostly formed by the aid of respondents' critical experience and opinions, but also perceptions creating security are taken into account. This means that perceived risks

and threats handled during the focus group discussions and interviews are treated as unsatisfactory states of the malls, which should be eliminated in the future. This follows the guidelines of scenario work suggested by Cornelius et al. (2005), especially when reacting to various changes or events.

Scenario analysis is subject to weaknesses in three major areas: 1) the quality of the model, 2) the quality of the data, and 3) the quality of the scenario team (Swiss Re 2009).

Results

In this section the results of the sub-studies are presented. The results are organized according to the framework presented in Figure 1 and summarized in Table 1.

Consumers connect *security systems* to security in physical surroundings. Especially they pay their attention to the design of the mall interior such as corridors, doors, staircases and lightning. In addition, technical equipment like CCTV, have earned their acceptance. However, staff relies mainly on technology, like CCTVs and various alarm systems, when security systems are discussed. Both consumers and staff see the role of *security guards* important in maintaining security, but consumers would appreciate more service-minded behaviour from their side. Staff, however, rely more on guards and their capability to handle all disturbance. Both consumers and staff emphasise the role of personal service and qualified staff in maintaining security in the malls. In addition, consumers recognise the role of co-customers and their influence on perceived security, whereas staff does not expect customers to play any part in security issues. Instead they believe that security leads for higher customer satisfaction level in general. *High product quality* is important for both groups, but if there happens to be any failure, consumers and staff look at it from the different perspective. Namely, consumers see spoiled products and all other unpleasant 'things', but for staff it materialises in number of product complaints and returns.

Table 1. Elements of security from consumer and staff point of view.

Elements of Security	Consumers	Staff
Security systems	Interior design CCTV Product alarms Check-outs and payments Disorder	IT-assisted information sharing CCTV Product alarms Fire alarms Locked glass displays
Security guards	Amount and quality of guards Staff quality Co-customers	Amount and quality of guards Staff quality Customer satisfaction
Product quality	Spoiled products Dirty shelves, displays and dishes Unclear product specifications Price Assortment	Complaints Product returns
Atmosphere	Staff social competence Loitering gangs Crowded malls	Staff service orientation Disturbance Problematic patrons Shoplifting Vandalism Cheating

The mall *atmosphere* seems to be an issue of delicacy and as a construct it appears to be multidimensional and fragmented. In this paper we included honesty and reliability in the construct of atmosphere (see also Takkinen 2009), but our empirical results give no evidence for this solution. Instead, we find that the atmosphere is formed by both negative and positive issues. Staff has crucial role in maintaining positive atmosphere through social communication and high service orientation towards customers, but if they lack social competence, the atmosphere will suffer without delay. On the other hand, co-customers may cause disorder and disturbance that decrease positive atmosphere and lead some consumers to avoid certain malls totally or at least they select their shopping time outside rush hours.

When consumer and staff opinions of security elements and their contents are compared, it can be concluded that staff is more oriented to technical security systems than consumers, whereas other people and social interaction seem to be more important for consumer security. In addition, consumers emphasize more product quality than staff. Atmosphere is important for both groups but it manifests itself different ways; staff pinpoint the problems caused by customers and consumers connect atmosphere more to phenomena that either cause them stress or pleasant shopping hours. Both groups, however, recognise the importance of staff in creating attractive atmosphere.

Based on the above comparison the future mall security could be built either from the staff or consumer point of view. If consumers' feelings of security are the main focus, the future malls concentrate on security created by people and high quality products. We call this human oriented scenario. If this scenario is chosen, security is provided mainly in co-operation with security guards, staff and customers. The role of customers in security work is completely novel idea, but it seems that they are willing to take this responsibility (see Koistinen & Peura-Kapanen 2009).

If staff will be able to decide the security guidelines for future malls, they would equip malls with technical security systems, and the minor role is given to the security guards. Even more minor role is reserved for staff themselves, and customers carry no responsibility. We call this technology oriented scenario. However, the combination of the interests of both groups provides more holistic scenario which we call co-operative scenario. The co-operative scenario unites superior technology with superior customer service. This scenario has even experienced in UK, where it was used in creating highly controlled and highly successful shopping centre called Highcross in Leicester that opened in September 2008 (see Beck 2010).

The results of the study indicate that the importance of security is increasing in future shopping malls. Like one of the consumers claimed:

> *"... I look to the future and I am scared, extremely scared, how to do my shopping and how to take care of my money..." (man 62 years)*

In fact, we believe that these elements belong more closely to the retail attraction factors in the future. However, this requires more close co-operation between security and retailing researchers and practitioners.

Discussion and Conclusions

The purpose of the article is to discuss the content and importance of security in future shopping malls. The empirical part is based on the studies by Koistinen and Peura-Kapanen (2009), Järvinen and Uuspelto (2008), and Juvonen and Järvinen (2010). The framework of the paper is modified from the study of Takkinen (2009) and accordingly the security in malls consists of following elements: 1) security systems, 2) security guards, 3) product quality and 4) atmosphere.

The study widened the contents of some security elements compared to that of Takkinen (2009). Namely, in this study security systems contain also store interior design like Mitchell & Harris (2005) suggest, whereas Takkinen refers purely to technical devices. Furthermore, this study connects responsibility of human oriented security to the staff and co-customers in addition to security guards. However, consumers connect price and assortment to the product quality (see also Koistinen & Järvinen 2009), especially balanced correlation between price and quality creates trust towards mall, but staff do not pay any attention to price level in this connection. However, staff reports that limited assortment often results negative comments or claims from customers' side.

Our study indicates that consumers still appreciate personal service above all, and at least part of the staff realise its importance, but the problem is the self-service orientation that dominates in retailing in Finland. The trend is likely to continue as self-scanning starts to replace cashiers. In addition, consumers expect service oriented attitude from the security guards (Koistinen & Peura-Kapanen 2009), and as a consequence of this many retailing organizations have now taken steps to train guards accordingly.

When comparing consumer and staff data it become evident that consumers emphasise more human work on maintaining security, whereas staff highlight the importance of technical systems. When combining the two perspectives there will be more options to develop holistic view that is based on co-operation between human beings and technology. As the result three scenarios are suggested: human oriented, technology oriented and co-operative scenarios. However, there is still on alternative scenario to be discussed. It is the scenario, what will happen, if security work is stopped completely in the malls.

The study does not reply to this question, but it is our guess that it will end up in some degree of chaos and corruption.

In this article we did not discuss about the unforeseen threats towards security that are called black swans, because of their ultimate improbability (Taleb 2008). That is simply because theses issues did not earn attention in our empirical data. However, the history of Finnish retailing security tells that even passion murders and bomb men can become reality in shopping malls, which makes it relevant to include black swans in alternative scenarios. Black swans in retailing may materialise in natural and man-made catastrophes, that prevent retailing logistics or in pandemia that put both staff and customers in quarantine.

No doubt the importance of security will increase in shopping malls in the future. Successful mall security is managed in many ways; first, the high technology assists in maintaining and even improving security, while it is more invisible. It also affects staff and consumer perceptions of security and leaves staff more room to concentrate to take care of their customers and serve them the best way they can. Second, for consumers security will be materialised in "soft" ways, such as service oriented and capable staff, friendly and nice looking guards and pleasant atmosphere. All these require more staff and guard training, more interests towards mall architecture and store interior design. After all, the best and most successful results are achieved with superior technology that co-operates with superior staff and security guards. Even co-customers and their behaviour play an important part of the perceived security.

References

Barbour, Rosalie S. – Kitzinger, Jenny (eds.) (1999) *Developing focus group research: politics, theory and practise*. Sage.

Beck, Adrian (2010) *Securing the cathedrals of consumerism*. A UK case study on shopping centre security. University of Leicester. Forthcoming.

Berman, Barry – Evans, Joel R. (2004) *Retail management*. A strategic approach. 9th ed. Pearson.

Bloor, Michael – Frankland, Jane –Thomas, Michelle – Robson, Kate (2001) *Focus group in social research*. Sage.

Cornelius, Peter - Van der Putte, Alexander - Romani, Mattia (2005) Three Decades of Scenario Planning in Shell. *California Management Review*, Vol. 48 (1), 92-109.

Eriksson, Päivi - Kovalainen, Anne (2008) *Qualitative methods in business research*. Sage.

Gips, Michael (1996) Shopping for security. *Security Management*, Vol. 40 (1), 12.

Gummesson, Evert (2005) Qualitative research in marketing: road-map for a wilderness of complexity and unpredictability. *European Journal of Marketing*, Vol. 39 (3-4), 309-327.

Hayes, Read (2007) *Retail security and loss prevention*. 2nd ed. Palgrave Macmillan.

Häyrynen, Simo (2009) Tarinoista todeksi – skenaariot tulevaisuuden tutkimuksessa. *Tieteessä tapahtuu*, 4-5/2009, 26-32.

Juvonen, Marko – Järvinen, Raija (2010) *Turvallisuus kaupan vetovoimatekijäksi? [Security as one of the attraction factors in retailing?]*. Aalto University School of Economics. Forthcoming

Järvinen, Raija – Uuspelto, Juha (2009) *Uhkaavatko asiakkaat? Kaupan henkilökunnan näkemyksiä turvallisuusuhkista*. Helsinki School of Economics, B-111.

Koistinen, Katri - Järvinen, Raija (2009) Consumer observations on channel choices - Competitive strategies in Finnish grocery retailing. *Journal of Retailing and Consumers Services*, (16), 260-270.

Koistinen, Katri – Peura-Kapanen, Liisa (2009) *"Kassajono se on se kaikista turvattomin paikka" Kuluttajien näkemyksiä asioinnin turvallisuudesta päivittäistavarakaupassa ja kauppakeskuksissa*

[Standing in the ceck-out line ranks high on the list of concerns]. Kuluttajatutkimuskeskus, Julkaisuja 5.

Mannermaa, Mika. (1991) In search of an evolutionary paradigm for futures research.

Futures, 23(4), 349-372.

Mitchell, Vincent Wayne – Harris, Greg (2005) The importance of consumers' perceived risk in retail strategy. *European Journal of Marketing*, Vol. 39 (7-8), 821-837.

Morschett, Dirk – Swoboda, Bernhard – Schramm-Klein, Hanna (2006) Competitive strategies in retailing – An investigation of the applicability of Porter's framework for food retailers. *Journal of Retailing and Consumers Services,* (13), 275-287.

Pitkäaho, Mari – Uusitalo, Jemina - Marjanen, Heli (2005) *Ostosmatkojen suuntautuminen ja ostopaikan valintakriteerit Turun seudulla vuosina 2001–2003 – Mylly-projektin toinen vaihe [Shopping trips and store choice criteria in Turku area in 2001 and 2003 – second phase of the Mylly-project].* Turku School of Economics and Business Administration, Series Discussion and Working Papers, 3:2005.

Swiss Re (2009) *Scenario analysis in insurance*. Sigma 1/2009.

Takkinen, Matti (2009) Kuluttajan ostopaikan valintaperusteet: Kyselytutkimus naiskuluttajien valinta-orientaatiosta pääkaupunkiseudulla. In Lindblom, Arto – Olkkonen, Rami – Mäkelä, Vilja (eds.) *Liiketoimintamallit, innovaatiotoiminta ja yrityksen yhteistyön luonne kaupan arvoketjussa*. Helsinki School of Economics, B-106, 219-247.

Taleb, Nassim Nicholas (2008) *Black Swan*. The Random House.

Teller, Cristoph – Reutterer, Thomas (2008) The evolving concept of retail attractiveness: What makes retail agglomerates attractive when customers shop at them. *Journal of Retailing and Consumer Services* (15) 127–143.

5. THEORY AND METHODOLOGY OF FUTURES STUDIES (NOT ONLY SECURITY-RELATED)

ROADMAPPING AS A FUTURES STUDIES METHOD IN THE FIELD OF SECURITY – APPLICATION AND CHALLENGES

Antje Bierwisch, Benjamin Teufel & Kerstin Cuhls
Fraunhofer Institute for Systems and Innovation Research

Contact: Benjamin Teufel, Email: benjamin.teufel@isi.fraunhofer.de

ABSTRACT – *In developing technologies for security applications, awareness is growing that only systemic perspectives can ensure that the various and often diverging needs of citizens, public authorities, operators of critical infrastructures or producers of security technologies are met. Many of the innovations to be developed are systems innovations which are of great concern for the public, integrate many different stakeholders and exhibit a high degree of market regulation. This paper shows how such a perspective can be turned into a participatory technology roadmapping process to arrive at a common understanding of the shaping of future developments and research strategies. This contribution is based on an empirical case where a roadmapping workshop on future sensor technologies in the field of personal security controls and luggage inspection at airports was conducted, for the period from 2009 to 2025. The findings show that within the field observed the roadmapping method is well suited to stimulating the public debate and the participatory formulation of public research strategies.*

Introduction and Background

Introduction

Foresight methods try to cope with problems of incomplete information, complexity and the resulting uncertainty about future developments, as well as adequate political or corporate responses. Among these methods, roadmapping can be seen as a practical method of visualizing future developments, thereby serving different goals, depending on the actors by which they are employed, and the level of observation (Möhrle and Isenmann 2008, 8).

This paper shows how a participatory technology roadmapping workshop can be conducted to arrive at a common understanding of the shaping of future developments and research strategies in the field of sensor technologies for personal security controls and luggage inspection at airports. This contribution is based on the empirical case of a roadmapping workshop on future sensor technologies. By applying an

inductive method, it is shown how the major challenges in this field of strategy formulation can be coped with in a roadmapping process, thereby demonstrating that roadmapping is an appropriate method if applied in this way. The following elements are important: at the end of the roadmapping process, it should be possible to formulate research strategies by integrating the social subsystems that are affected by the technologies, as well as and the perspectives and interests of several stakeholders. Participants in the process should be able to integrate all the non-technical aspects that are relevant for the technological field observed in the roadmapping process, and assumptions about the public interest should be transformed into the formulation of functional requirements on security technologies in the absence of "pure" market mechanisms.

Roadmapping

Technology roadmapping has been a useful method for formulating technology strategies and technology planning for many years (Laube and Phaal 2007). Developed in the 1980s by Motorola Inc, it is recognized as helpful at very different levels by policy-makers, scientists and industry alike as a basis for strategic decisions concerning future technologies. It is a "[…] method which outlines the future of a field of technology, generating a timeline for the development of various interrelated technologies […]" (Popper 2008, 68). In most roadmapping processes, however, technologies are not an isolated object of interest: as future technologies can neither be assessed without the requirements, nor the potentials they contain, roadmapping has to encompass all relevant associated future products, processes, functions, market drivers, competencies or projects (see Möhrle and Isenmann 2008, 5).

A technology roadmap, as the outcome of the process of roadmapping, can be defined as a graphical representation of technologies and their interdependencies (Möhrle and Isenmann 2008, 3), as well as related aspects, over time (Figure 1). There are many different ways to design a roadmap. In the roadmap visualization as a two-dimensional space, the different classes of aspects, like for example market developments, products in this market, product technologies and related R&D projects, can be visualized as levels along the object-axis (ordinate) of the roadmap. The x-coordinate represents the time axis on which future developments are assessed, with the specific time period depending on the thematic focus. Roadmaps explicitly use the metaphor of an itinerary to highlight the importance of a graphical and transparent process of information, in order to enable orientation. During the roadmapping process, new products and markets that are driven by technological developments are recognized (forecasting), and technological developments that are required by future markets and related product needs are identified (backcasting). Figure 1 shows, for example, the interdependencies between new technologies that realize new products, and new products which in turn define new technologies. If one focuses on the technology, it is also important to address the respective know-how in the roadmap, and if one focuses on the products, the applications also need to be considered.

The logic of roadmapping thus integrates the technology push and the market pull perspective. Both perspectives are considered as increasingly important for innovation success if taken into account simultaneously (Moorman and Slotegraf 1999, 248 ff.; Perl 2003, 38 f.). The visualization helps to assess which developments may emerge through new demands and a market-pull effect, and which new developments emerge because of new technological developments, the technology push effect.

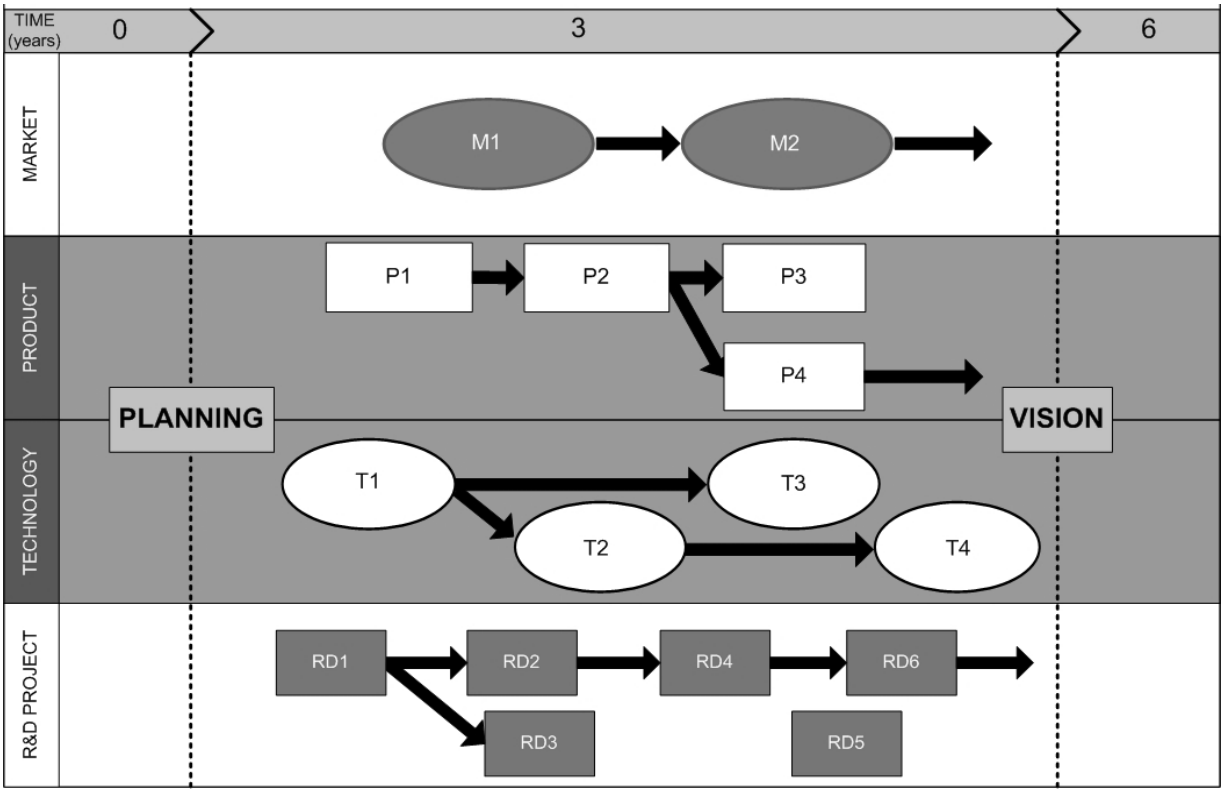


Figure 1. Typical framework of a roadmap design, source: Groeneveld (1997).

Roadmapping can be regarded as the interface between foresight and planning. Moreover, by organizing information on possible futures, it provides a partial solution of the problem that can best be described by quoting Simon (1979, 353): "Given a particular environment of stimuli, and a particular background of previous knowledge, how will a person organize this complex mass of information into a problem formulation that will facilitate his solution efforts?" For Möhrle and Isenmann (2008, 10), roadmapping aims at “thinking out of the box” in combination with a process of communication. A further advantage is its use as an integration instrument that allows structuring of the information gathered from other foresight methods, such as scenario techniques or surveys like Delphi, and thus to arrive at a more coherent, common understanding of the future. Therefore it can be described both as a foresight method and a strategic planning tool (see also Specht and Behrens 2008, 394). Among other foresight methods, roadmapping can further be classified as a short- to medium-term method (Cuhls 2008, 150 ff.). In addition, it can be regarded as a mostly qualitative (Lichtenthaler 2002, 41) and both analytic and normative method (Cuhls 2008, 153) which is applied through the combination of group- and desk-work (Popper 2008, 68). During the roadmapping process, information is gathered exploratively in a communication process that allows for both individual and collective learning (Lichtenthaler 2008, 69). The classification of the method on these aspects is shown in Figure 2.

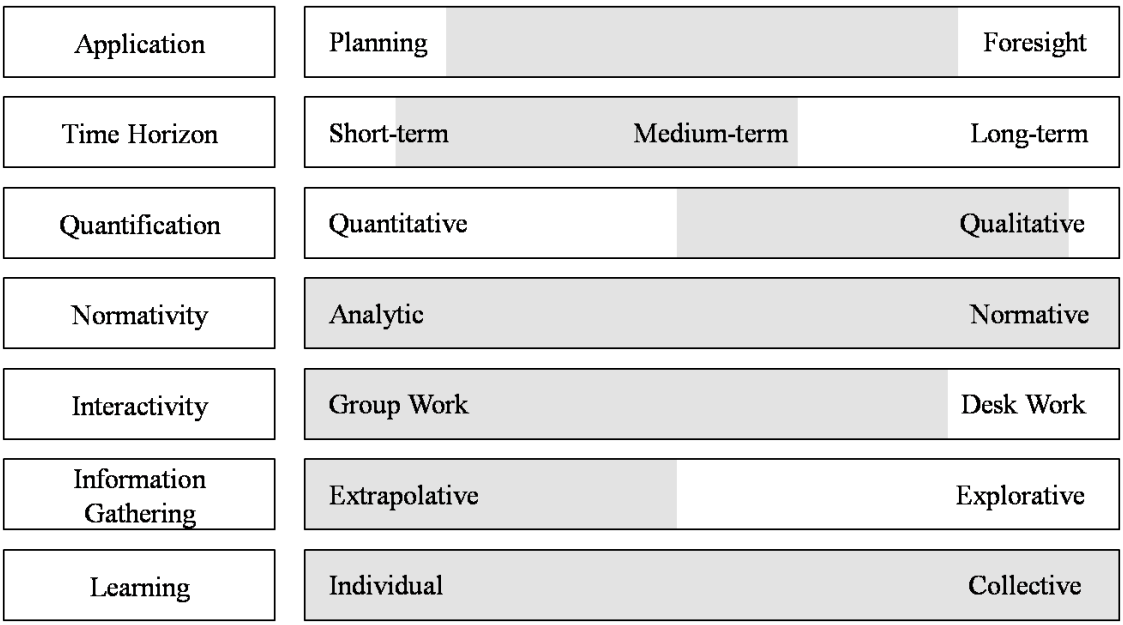


Figure 2. Classification of technology roadmapping.

The objectives of roadmapping also depend on the level to be observed. Roadmaps for R&D units are usually employed for internal steering. Roadmaps at a corporate level ensure the coordination of activities at the company level, and sector-specific roadmaps can focus on the future development of a country's technological or economic sector, and at the level of the National Innovation System (NSI), it serves strategy formulation in science, technology and innovation (STI) policy (see Figure 3), the latter often implying political aspects. To apply roadmapping as a method for inter-personal exchange in a workshop concept (see for example Laube and Phaal 2007), and on a regular basis, roadmapping can be institutionalized in different ways for example as a so-called closed-shop procedure within R&D units as well as "public" participation of suppliers, cooperation partners, key users and other external stakeholders (Möhrle and Isenmann 2008, 8 f.).

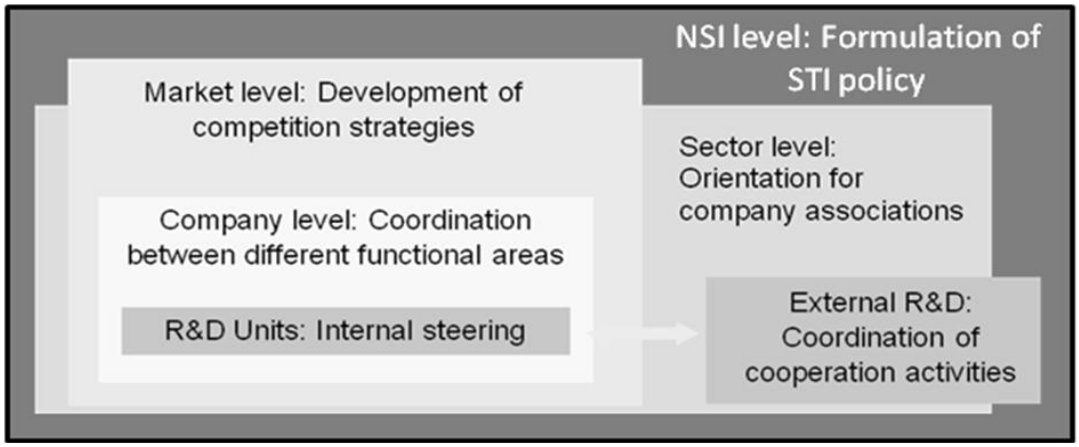


Figure 3. Different goals as a function of different stakeholders, source: Möhrle and Isenmann, 2008.

In order to "fill" the roadmap, a process to work out a vision, or more concretely, a goal is necessary. This is often performed by different foresight approaches, starting from this goal, and in a second step, back- and forecasting are both performed to work out and fill in the "milestones" of the roadmap.

There are different designs for a roadmap, starting from a simple "time arrow" with different layers in a very simple form up to a "radar" or a subway map. The variety of application contexts does not guarantee "one best way" to conduct a roadmapping process. Instead, situation-specific experiences have to be gathered. In the field of technologies for security applications, several specific framework conditions have to be addressed, like the central role of public operators, the relatively high degree of market regulation or the broad range of end users, like for example airline passengers.

Many of the innovations to be developed represent systems innovations which are of (1) great concern for the public, (2) exhibit a high degree of stakeholder integration, (3) have to address many regulatory, ethical and organizational aspects. All these aspects result in a growing awareness that only systemic perspectives can ensure that the various and sometimes diverging needs of citizens, public authorities, operators of critical infrastructures or producers of security technologies are met. In the following sections, it will be shown how such a perspective can be turned into a participatory technology roadmapping process to achieve a common understanding of the shaping of future developments and research strategies. In the empirical case, where a roadmapping workshop on future sensor technologies for personal security controls and luggage inspection at airports was conducted, the following questions are addressed by using an inductive method.

- How can roadmapping be used to formulate research strategies and how can the different social subsystems and the perspectives and interests of several stakeholders be integrated?
- How can the relevant non-technical aspects be identified and integrated in the process of roadmapping?
- In the absence of "pure" market mechanisms, how can assumptions about the public interest be transformed into the formulation of functional requirements on security technologies?

The Case of the SimSecur Roadmapping Process

This section describes the empirical case and its special characteristics compared to other roadmapping processes. Practical implications for similar roadmapping processes in the field of security technologies will be drawn from this case in the next section. The process took place in a one-day roadmapping workshop conducted in the context of the French-German SimSecur project, which was funded by the German Federal Ministry of Education and Research.

The project aimed to develop sensors and sensor systems to detect hazardous materials, hidden weapons and for the biometric control of persons to increase security in critical infrastructures. The contribution of the other Fraunhofer Institutes[1] to the project encompasses the optimization of sensors and

[1] Seven Fraunhofer partners were part of the SimSecur project consortium: the Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut EMI, the Fraunhofer Institute for Chemical Technology ICT, the Fraunhofer Institute for Applied Solid State Physics IAF, the Fraunhofer Institute for Production Systems and Design Technology

their method of measurement, the signal quality, and systemic aspects in the protection against malevolent acts. This optimization was achieved by simulating the performance of sensor functions and systems under various environmental conditions. Because of the significance of passenger streams in aviation security, the technologies are considered to be especially relevant in this field of application. The assessment of the potentials and the performance of sensor technologies for aviation security and the reflection of non-technical aspects of various application contexts becomes increasingly important. This assessment was part of the research conducted by the Fraunhofer Institute for Systems and Innovation Research, an institute working mainly in socio-economic disciplines. Part of these contexts is the discussion of potential security threats caused by malevolent actors, but also the object-specific, ethical, legal and financial framework. This means, for example, asking questions about the choice of attackers' strategies, architectural conditions at airports or about possible invasions of personal privacy.

It was assumed that a systematic integration of these various aspects in a roadmap could offer valuable clues about research needs and potentials with regard to current and future technological developments in this field. Due to the unique combination of experts and contacts in the project network, the goal was to generate and integrate new insights for the formulation of strategies for researchers and policy-makers alike. In the workshop, these research needs and the potentials of sensor technologies for airport security should be discussed in the process of generating a technology roadmap. An interdisciplinary expert group was involved, representing the technically-oriented Fraunhofer project partners, “non-technical” security experts from the field of social psychology, psychology and ethics in sciences and humanities, as well as the airport operators. This was assumed to be a first step towards a common understanding of future developments in the fields of security needs, requirements and framework conditions, sensor systems and the underlying sensor technologies. This common understanding should form a basis for the strategic orientation of future activities in the fields of research and STI policy.

The workshop started with a short introduction about the roadmapping method and its application in the project context. The following three steps for creating the SimSecur Roadmap were introduced in this presentation:

- Step 1: Where are we at the present? (Roadmap level: sensor system)
- Step 2: Where do we want to go? (Roadmap level: security needs and framework conditions)
- Step 3: How can we get there? (Roadmap level: all three)

After that, the technically-oriented experts were asked to position their specific sensor technologies and the connected sensor products at the roadmap level “sensor system” with regard to technical realization possibilities. The non-technical experts were assigned to the roadmap level “framework conditions”. The challenges were to identify ethical, legal, organizational and other framework conditions which play an important role in the present and in the future in the context of sensor technology application in airport security checks. The next step spent time on the security needs. In group work the needs for sensor functions in cooperative and non-cooperative security controls were discussed. The focus was on questions like: Which kind of weapons and hazardous materials should be detected in the future? How can future security checks be designed? How much should passengers know about the control to ensure both

---

IPK, the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB as well as the Fraunhofer Institute for Systems and Innovation Research ISI.

deterrence and customer-friendliness? During the generation of the “framework conditions” and the “security needs” levels, information on non-technical aspects that had been gathered from previous desk research was provided to stimulate the discussion. Subsequently, it was necessary to reflect the interaction between the roadmap levels and to point out which technologies are able to address the needs and the future challenges from technological and non-technological perspectives. These technologies were then assessed according to their market attractiveness and the national competitive advantage. In the following discussion it was possible to jointly analyze the resulting research needs and strategies.

Results

The SimSecur case described how the following major challenges in the field of security can be coped with in a roadmapping process: Firstly, at the end of the roadmapping process, it should be possible to formulate research strategies by integrating the different social subsystems and the perspectives and interests of several stakeholders. Secondly, participants in this process should be able to integrate all the non-technical aspects that are relevant for the technological field observed in the roadmapping process. Thirdly, assumptions about the public interest should be transformed into the formulation of functional requirements of security technologies in the absence of “pure” market mechanisms.

Based on the SimSecur case, it can be assumed that roadmapping is a method that is flexible enough and well suited to an application in the field of security technologies. It could be shown that in particular the combination of foresight and planning logic, the participative application and the possibility to combine previous desk work with group work in a workshop made it possible to arrive at a basis for formulating strategies in the fields of research and STI policy. Moreover, the strategies discussed correspond to many aspects of the "Research for Civil Security Program" of the German Federal Ministry of Education and Research (e.g. the acceptance of technological developments, the sources of threats, data protection and the impact on human rights and civil liberties, as well as the recently published call on “Biometrics”), and of the 3rd Security Call of the European Commission. However, in order to properly and effectively apply the roadmapping method, it became clear that the following aspects, which are summarized in Table 1, have to be taken into account.

Integration of previous desk work: because of the broad range of non-technical aspects that are relevant in conjunction with the sensor products and technologies in the project, these aspects had to be specified in advance of the roadmapping workshop. For this purpose, semi-structured interviews were conducted with the Fraunhofer partners to identify their assumptions about non-technical, contextual factors. These implicit assumptions, which included the types and the relevance of these aspects, were reflected, categorized and complemented by the relevant literature.

Order of the roadmap levels: the project-related focus required a clear definition of the field of observation of all the participants. Therefore, the roadmapping process started by first drawing the product and technology levels of the roadmap (see Figure 4). After drawing the “security needs” and the “framework conditions” levels, assumptions on product and technology developments could be validated against them.

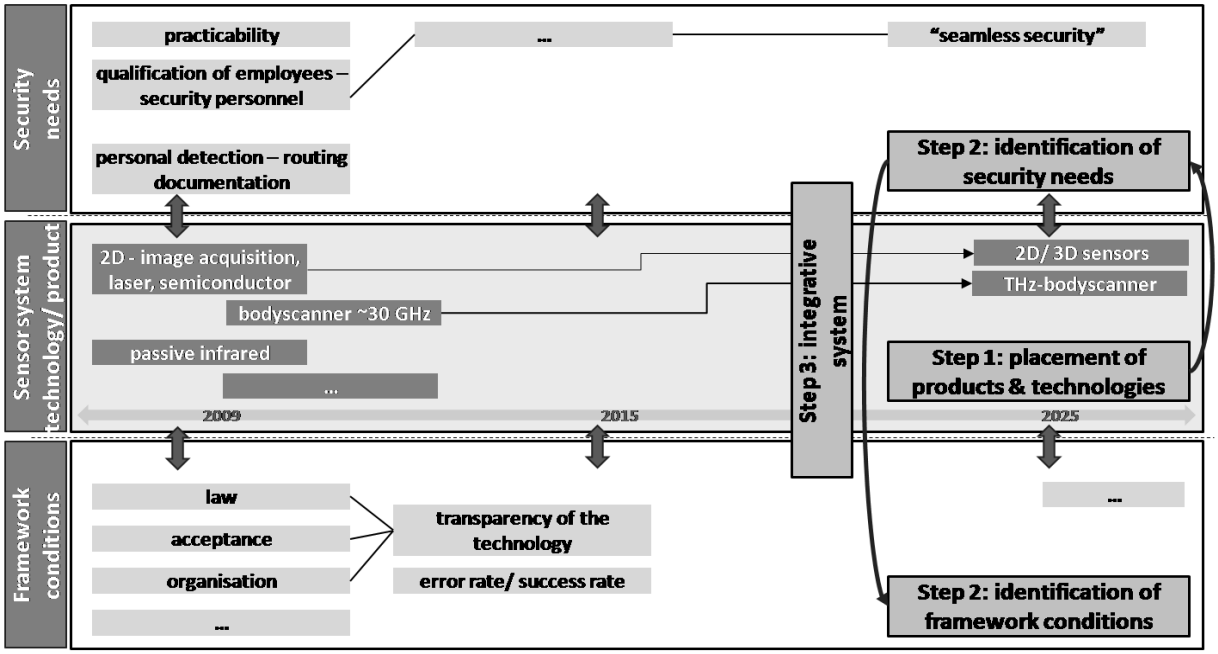


Figure 4. Sketch of the SimSecur Roadmap.

Security needs: as opposed to roadmapping processes for example in some consumer goods industries, backcasting could not be conducted by only focusing on classical market drivers. Especially the fact that every citizen could be potentially affected by the sensor products to be developed required a very broad view of the "customer". Moreover, in place of the classical user-provider relationship, a series of stakeholders from various societal sub-systems, such as citizens, airport operators, representatives of the legal system and research policy had to be addressed in formulating the requirements of sensor products and technologies. Instead of a "market needs" level, a more holistic view was taken by drawing a "security needs" level. The security needs encompassed aspects as different as the similar detection of hazardous substances based on the potential security threats, a good usability of technical devices for the control staff, and customer-friendly controls.

Separate application categories of technology: the security needs and the respective application of the sensor products could be classified into cooperative and non-cooperative person controls. These types allowed for an elaboration of the respective security needs in two groups, and allowed for/ necessitated a general discussion about the desirability of cooperative vs. non-cooperative controls.

Framework conditions: before assessing the human, intellectual and financial resources necessary to pursue the development of the sensor technologies mentioned in the roadmap, the legal, ethical, organizational and acceptance aspects had to be discussed. Thus, instead of a "resource level", which is used in most roadmaps, these framework conditions were worked out at the lower visualization level and discussed as technology enablers or restrictions. In contrast to the resources needed for the development of different sensor technologies, these aspects were considered to be relatively stable over time. Especially the need for an operational stability in airport security led to the assumption that the infrastructure and organization of personal controls and luggage inspection will remain relatively constant until 2025. In a second step, the sensor products and technologies that had been pre-selected according to the broader security needs and framework conditions in a qualitative discussion were assessed in a technology portfolio according to the dimensions of "market attractiveness" and "competitive strength".

"Objective" discussion process: the facts that workshop participants came from different institutions and that the roadmap focus was the macro level of national research strategies had two important implications for the roadmap process: (1) Compared to corporate or other in-house processes of strategy formulation, the "public" nature of this roadmapping process ensured that there was no bias from personal career interests or rivalries in the discussion of future products and technologies, as can be the case in corporate roadmapping processes. (2) At the same time, technologically confidential information could not be exchanged among the participants. However, at this level of detail/ granularity, it became clear that this restriction did not impede or significantly bias the roadmapping process.

Need for the discussion of strategies: since the aim of the workshop was to identify research needs and potentials with regard to current and future technological developments, the roadmapping process was followed by a discussion of research and STI policy strategies. The roadmap visualization contributed not only to providing orientation in the complex thematic field, but also helped to stimulate this debate.

Table 1. Challenges and methodological approaches in the SimSecur Roadmapping Workshop.

Challenge	**Methodological Approach**
Broad range of non-technological aspects	Expert interviews and desk research on relevant aspects as input
Project-related thematic focus	Focus on (1) sensor products and technologies, then (2) framework conditions and security needs
Special characteristics of the security field	Not "market" level, but more general "security needs" level
Different classes of applications	Separate consideration of cooperative and non-cooperative technologies in two groups
Framework conditions instead of a "resource" level: (1) need to be addressed before focusing on resources/ competitive strength (2) relatively high stability of framework conditions compared to resources/ competitive strength	(1) Discussion of legal, ethical, organizational and acceptance aspects as enablers and restrictions for security technologies (2) Generation of technology portfolios with market attractiveness and competitive strength dimensions
Unbiased, "objective" discussion process	No strong social or functional relationships between workshop participants
Strategy formulation as goal	Subsequent discussion of strategies in the plenum with the help of the roadmap as orientation

Conclusion and Outlook

In summary, the findings show that in the field observed, roadmapping is well suited to stimulating the public debate and for the participatory formulation of public research strategies. It could thus serve as an orientation for future roadmapping processes on security technologies that aim to formulate STI strategies.

Although roadmapping has been proven an adequate means for foresight and strategy formulation in the field of security technologies, some extensions are possible. For example, the granularity in the observation of the different roadmap levels was oriented to the still relatively broad focus of the project. Depending on the goal, some roadmapping processes should take a narrower focus to enable discussions in greater detail. Another way of achieving a higher level of detail, would be, if possible, to have a longer workshop duration. The optimal duration of a roadmapping process are several workshop days, each day focusing on a different roadmap level, and the last one on the integration of the levels (Laube and Phaal 2007). Especially in the field of research and STI policy strategies for security technologies, this would allow integration of more and more complex information input to meet the requirements of the systemic view of security innovation. A further extension of the process would be to use the roadmap together with the results of a general strategy formulation, as conducted in the SimSecur case, as an explicit starting point for formulating more specific research questions and STI policy instruments.

References

Cuhls, Kerstin (2008) *Methoden der Technikvorausschau – eine international Übersicht*. Fraunhofer IRB Verlag, Stuttgart.

Groeneveld, Patrick (1997) Roadmapping integrates business and technology. *Research and Technology Management*, Vol. 40 (5), 48-55.

Laube, Thorsten – Phaal, Robert (eds.) (2007) *Praxishandbuch Technologie-Roadmapping. Workshopkonzept für den schnellen Einstieg (T-Plan)*. Fraunhofer IRB Verlag, Stuttgart.

Lichtenthaler, Eckhard (2002) *Organisation der Technology Intelligence. Eine empirische Untersuchung der Technologiefrühaufklärung in technologieintensiven Grossunternehmen*. Verlag Industrielle Organisation, Zürich.

Möhrle, Martin G. – Isenmann, Ralf (eds.) (2008) *Technologie-Roadmapping. Zukunftsstrategien für Technologieunternehmen*. Third Edition. Springer Verlag, Berlin, Heidelberg.

Moorman, Christine – Slotegraaf, Rebecca J. (1999) The contingency value of complementary capabilities in product development. *Journal of Marketing Research*, Vol. 36 (2), 239-257.

Perl, Elke (2003) Kapitel 1: Grundlagen des Innovations- und Technologiemanagements. In: Strebel, Heinz (ed.): *Innovations- und Technologiemanagement*. Utb Verlag, Stuttgart.

Popper, Rafael (2008) 3. *Foresight Methodology*. In: Georghiou, Luke - Cassingena Harper, Jeniffer (eds): *The handbook of technology foresight: concepts and practice*. Edward Elgar Publishing, Cheltenham, 44-88.

Rödel, Jürgen – Weissenberger-Eibl, Marion – Kounga, Alain – Koch, Daniel – Bierwisch, Antje – Rossner, Werner et al. (2008), *Hochleistungskeramik 2025: Strategieinitiative für die Keramikforschung in Deutschland*. Werkstoffinformationsgesellschaft mbH Frankfurt, Frankfurt.

Rödel, Jürgen – Kounga, Alain – Weissenberger-Eibl, Marion – Koch, Daniel – Bierwisch, Antje – Rossner, Wolfgang – Hoffmann, Michael – Danzer, Robert – Schneider, Gerhard (2009), Development of a roadmap for advanced ceramics: 2010-2025. *Journal of the European Ceramic Society*, Vol. 29 (9), 1549-1560.

Simon, Herbert A. (1979) Rational decision-making in business organizations. The American Economic Review, Vol. 69 (4), 493-513.

Specht, Dieter – Behrens, Stefan (2008) Strategische Planung mit Roadmaps – Möglichkeiten für das Innovationsmanagement und die Personalbedarfsplanung. In: Möhrle, Martin G. - Isenmann, Ralf (eds.): Technologie-Roadmapping. Zukunftsstrategien für Technologieunternehmen. Third Edition. Springer Verlag, Berlin, Heidelberg, 145-164.

USING SCENARIOS TO CHARACTERISE COMPLEX POLICY INTERRELATIONSHIPS: THE SANDERA PROJECT

Andrew D James & Professor Ian Miles
Manchester Institute of Innovation Research, Manchester Business School, University of Manchester, UK
E-mail: Andrew.James@mbs.ac.uk

ABSTRACT – *Project SANDERA focuses on the future relationship between three critical European policy domains: namely, the EU science and technology policy strategy to move towards the European Research Area and those EU policies focused on the security of the European citizen in the world both through EU defence policies and EU security policies. This paper addresses the methodological challenges of using scenarios to characterise complex policy interrelationships and reports on some aspects of the methodological approach being adopted.*

Introduction

This paper addresses some of the methodological challenges of using scenarios to characterise complex policy interrelationships and reports on the methodological approach being adopted by Project SANDERA.[2] Project SANDERA focuses on the future relationship between three critical European policy domains: namely, the EU science and technology policy strategy to move towards the European Research Area and those EU policies focused on the security of the European citizen in the world both through EU defence policies and EU security policies. SANDERA is a two-year project funded under the Seventh Framework Programme Socio-Economic Sciences and Humanities theme *Blue Sky Research on Emerging Issues Affecting European S&T*.

This paper is structured as follows: Section 2 provides some background to the SANDERA Project; Section 3 explains our rationale, project aims and methodological approach; Section 4 describes the methodological challenges presented by SANDERA and how we are seeking to conceptualise the complex policy interrelationships between the three policy areas; Section 5 explains how we are seeking to

[2] This paper reports on work that is the product of the joint efforts of a project team led by the Manchester Institute of Innovation Research (UK) and comprises the University of Lund (Sweden); CSIC (Spain); Stiftung Wissenschaft und Politik (SWP); Istituto Affari Internazionali (Italy); ARMINES (France); Copenhagen Business School (Denmark); Institute of Economics of the Hungarian Academy of Sciences (Hungary); and EGMONT Royal Institute of International Affairs (Belgium).

use our conceptual framework to identify drivers of change and build scenarios; and, in Section 6 we provide some conclusions and an indication of the next steps for Project SANDERA.

Background

Over the last decade, the EU has developed a defence and security dimension. In particular, the externally-oriented Common Security and Defence Policy (CSDP), renamed under the Lisbon Treaty and formerly known as the European Security and Defence Policy (ESDP), which is a major element of the Common Foreign and Security Policy of the European Union and is the domain of EU policy covering defence and military aspects. The Member States have also agreed a *European Security Strategy* that guides the EU's international security strategy with the objective of making the European Union "a credible and effective actor" that is "ready to share in the responsibility for global security and in building a better world".[3]

The EU has also developed internally-oriented policies for countering terrorism with the appointment of an EU Counter Terrorism Coordinator and the development of policies designed to prevent, protect, prosecute and respond to terrorism and other security-related risks. These internally-oriented security policies and institutional arrangements comprise a somewhat diverse group of policies that comprise the internal dimension of fighting terrorism; policies for the protection of critical infrastructure; energy security; civil protection; and border security.

These developments have been complemented by a science and technology policy dimension. The Seventh Framework Programme has allocated €1.4 billion for funding security research for civil and non-lethal applications managed by DG Enterprise. The Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks" was established under a Council Decision as part of the General Programme on "Security and Safeguarding Liberties" managed by DG Justice, Freedom and Security. The European Defence Agency has as one of its goals enhancing the effectiveness of European defence research and technology and – as well as acting as a catalyst for more European defence R&T collaboration, it has also acted as a customer for some R&T projects on behalf of a group of Member States or on the EDA's own account (although its budget for this has been modest).

When SANDERA was conceived in 2007 our working hypothesis was that the establishment of security and defence research as an element of the European policy mix was the start rather than the end of policy innovation in this field. This working hypothesis has already proven correct. By 2010, we can observe growing attempts to promote closer linkages between the Framework Programme and the European Defence Agency's defence R&T agenda. This comes against a background of political calls for closer cooperation on defence R&D between the EDA and the Commission from both the European Council and the European Parliament.[4]

Three developments are of particular note:

---

[3] *A Secure Europe in a Better World*. European Security Strategy. Brussels, 12 December 2003.

[4] COUNCIL OF THE EUROPEAN UNION Council Conclusions on the ESDP 2903rd External Relations Council meeting, Brussels, 10 and 11 November 2008: Council of the Europeam Union Brussels, 11 December 2008 Declaration on Strengthening Capabilities; Report on the Implementation of the European Security Strategy - Providing Security in a Changing World, Brussels, 11 December 2008; Motion for a European Parliament Resolution on the European Security Strategy and ESDP (2008/2202(INI)) 28 January 2009.

- The emergence of ad hoc coordination between the civil security research theme within the Seventh Framework Programme and the defence R&D activities of the European Defence Agency in a number of fields;
- Moves by the European Defence Agency and the European Commission (at the request of the Defence Ministers of European Member States) to establish a European Framework Cooperation for Security and Defence together with the European Commission with the aim of "maximising complementarity and synergy between defence and civil security-related research activities".[5]
- Growing discussions in Brussels about the possibility of including defence research in the Eighth Framework Programme (in particular amongst officials from the European Commission and the European Defence Agency).

Attention has focused mainly on the implications of such developments for European security and defence policies, the strengthening of the European Defence Technological and Industrial Base (EDTIB) and the balance between EU activity and Member States. However, Project SANDERA starts from the belief that the emergence of an explicit defence and security dimension to EU science and technology policy also has potentially profound significance for the future character of European science and technology policy, the Framework Programme and the move towards the European Research Area.

The move towards the European Research Area (ERA) has been an important theme in European science and technology policy for the last decade. The term "European Research Area" was coined in a Commission document published in January 2000 ("Towards a European Research Area"). [6] In essence, the ERA approach was a wake up call for a step change in how the research landscape in Europe should be organised and governed, in order to improve its performance. The overall ERA idea was to do away with a traditional multi-layer governance of research in Europe and the scattered and divided landscape of research in Europe. We can identify six main golas of ERA policy as follows: (1) to contribute to a European internal market for research, where researchers, technology and knowledge (fifth freedom) circulate freely, (2) world-class research infrastructures, (3) excellent research institutions, (4) effective knowledge-sharing (5), well-coordinated research programmes and priorities, including a significant volume of jointly-programmed public research investment at European level involving common priorities, coordinated implementation and joint evaluation; (6) a wide opening of the European Research Area.

Accordingly, SANDERA will examine how future developments in European security and defence research and innovation policies combined with technological change and the evolution of European science and technology policies could interact in intended and unintended ways to affect the pace and character of the move towards the ERA as well as priorities for the 8th Framework Programme.

[5] "EDA and Commission to work closely together on research", European Defence Agency Press Release, May 2009.
[6] Commission of the European Communities, 'Towards a European Research Area (Com (2000)6 of 18/01/2000)', http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0006:EN:HTML, accessed 21 March 2007.

Rationale, project aims and methodological approach

Project SANDERA thus focuses on the future relationship between three critical European policy domains: namely, the EU science and technology policy strategy to move towards the European Research Area; EU defence research and innovation policies; and, EU security research and innovation policies. In framing our study in this way we are aware that there is a growing blurring between defence research and security research and this is one of the issues that we will return to later in this paper.

Rationale

The core rationale for SANDERA is not only that these developments may have potentially profound implications for the future character of European science and technology policy but also that this topic has been almost entirely overlooked by both the academic and policy communities.

There are those who see potentially great opportunities arising from future developments in the relationship between European research and innovation policies security and defence and European science and technology policy. From the perspective of security policy, the importance of civilian-origin dual use technologies means that Europe's capability to counter security threats may in the future rely on the innovation capability of the ERA making a strong ERA critical to the security of the EU citizen. From the science and technology policy perspective, interest in demand-side innovation policy has caused some to begin to consider the potential role of security and defence R&D and procurement as a public engine of innovation. At the same time, greater connectivity between defence and civil science and technology may allow Europe to generate some of the competitiveness benefits that appear to have accrued to the US as a result of its spending on defence R&D and procurement in the past.

There are others, however, who worry about what they fear may be the potentially dangerous consequences of the emergence of a security and defence dimension to European science and technology policy. There have long been concerns that defence R&D may distort scientific priorities and the course of scientific development. The Framework Programme has historically been a consciously civilian project albeit one that has funded dual-use technologies. Including defence R&D of any kind in the Eighth Framework programme would raise important questions not least what would it mean for the character and priorities of European science and technology and the ERA? At the same time, the desire of the security community to control the circulation of "dangerous" knowledge and to control the transfer of certain technologies to some third countries appear to be in tension with the ERA vision of free circulation of knowledge within a global scientific community.

Despite the obvious importance of these issues, we observe that policy development for the ERA and policy development for security and defence research and innovation is taking place in separate "silos" with surprisingly little overlap between policy communities. The policy communities are by and large separate. Each has its own discrete set of policy concerns, stakeholders and policy networks despite the fact that developments in one policy field may have direct or indirect implications for the other policy field.

Indeed, we can see that policy making at the European level is effectively taking place in "silos". At the European level, it appears that the two policy communities (security-related community on the one hand and the ERA community on the other) remain more or less isolated from one another: members of

each community are not involved in the activities of the other community. To be sure, there is an intense *inter*-governmental organizational collaboration in security and defence matters in Europe, as described in the Knowledge Dynamics and Security Dynamics Scoping Papers. However, this is very weakly linked to ERA dynamics or instruments as such and the EU as a corporate actor is not involved in many of the inter-governmental activities. On the contrary, for the purpose of defence research and development co-operation governments have over the last two decades developed a dedicated set of forums, rules, and funding mechanisms that are separate from the ERA.

We can go further and argue that they represent different epistemic communities. The policy communities each have their own policy "challenges", their own policy responses and their own organisational and institutional settings. Each policy community has its own set of shared symbols and references, mutual expectations and mutual predictability of intention.[7] This creates "world views" that shape the behaviour of each policy community and delineates a cognitive framework for problem framing and problem solutions.

The extent of boundary crossing between the policy communities remains limited and when the boundaries are crossed the policy communities find it challenging to identify common "world views". Security policy "frames" policy issues as "security" issues and thus "securitises" science and technology, characterising some aspects of knowledge as "dangerous" and seeking to regulate and control its practice and diffusion. The contrast with the world view of the ERA policy community is stark.

At the same time, an important caveat should be added to this discussion namely that the notion of a single ERA "policy community" is problematic. The ERA is different things to different people, it is at the same time a new 'concept' for thinking about European intervention, a new policy and a new set of practices and instruments, and new relations with member states organisations dealing with research and innovation policies and their implementation). Moreover, the definition of ERA and its goals are not widely shared among all stakeholders, in fact even the problem definition underlying ERA is contested.

Similarly, there is not and never has been a single "military-industrial-scientific complex". Instead, there has been a variety of stakeholders with different perspectives and interests. Today, there is no "security and defence" policy community as such. The culture, interests and perspectives of police and fire service first responders is dramatically different from that of the armed forces and within the "military complex" there remain significant differences of interest between the different branches of the armed forces and between the military and the defence industry.

Critics of the security research theme express concerns about the role of policy networks, with one arguing that: "there are real issues about the extent to which hand-picked expert groups are making security policy with little or no democratic oversight and without the inclusion of critical voices".[8] The emergence of the security research theme as evidence of the growing influence of the "military industrial complex" on European policy has also been raised by European non-governmental organisations.[9]

---

[7] John Gerard Ruggie, 'International Responses to Technology: Concepts and Trends', International Organization, 29/3 (1975), 569f.
[8] Jocelyn Mawdsley (2008), "The European Union and Security Research: advocacy, framing and accountability", conference paper presented at UACES 2008 Annual Conference, University of Edinburgh, September 2008.
[9] *NeoConOpticon: The EU Security Industrial Complex*, Transnational Institute and StateWatch, 2009.

Indeed, the FORESEC study and final conference has raised the problem that European security foresight exercises rely almost exclusively on a community of security "experts". By omission or commission, the broader European scientific community and civil society has been effectively excluded from these policy processes.

What are the aims of SANDERA?

Accordingly, the aim of SANDERA is to examine how future developments in European security and defence policies combined with technological change and the evolution of European science and technology policies could interact in intended and unintended ways to affect the pace and character of the move towards the ERA as well as priorities for the 8th Framework Programme. Specifically, SANDERA has four objectives:

- To identify drivers of change in the relationship between European security and defence policies and the ERA
- To develop exploratory scenarios of alternative futures of the relationship between security policy and the ERA
- To analyse the policy implications of the scenarios and develop indicators of change
- To stimulate dialogue and promote stronger networking between the security policy and science and technology policy communities

Methodological challenges and approach

Project SANDERA is a scenario based study. We are using an exploratory foresight approach to develop scenarios of the relationship between policies for the European Research Area and European research and innovation policies defence and security in the year 2030. Our objective is to develop scenarios that will enable policy makers, stakeholders and the scientific community to explore the consequences of future developments at the interface between security policy and science and technology policy. In this way, policy makers will be able to make better informed choices in the present and to be better able to apprehend and comprehend future developments as they unfold.[10]

To address these questions, the SANDERA project team is having to develop a new scenario based approach to characterise the complex policy interrelationships between the three policy domains (ERA; security; and defence). This has presented several challenges, as follows:

- *How to work across epistemic boundaries* – We have noted that at the heart of SANDERA is the view that each policy community has its own "world view" that shapes its behaviour and delineates a cognitive framework for problem framing and problem solutions. Our project team

[10] We assume that *policy makers* may be at the European Union level (either within the Commission, the Council or intergovernmental bodies such as the European Defence Agency) or at Member State level. We also assume that policy makers may be those who are responsible for science and technology policy or may equally be those responsible for the various aspects of defence and security policy. We define *stakeholders* broadly and include (amongst others) research providers (universities or research and technology organisations), the defence, security and related industries including SMEs, representatives of learned scientific societies (such as the Royal Society in the UK) and so forth. We also define *the scientific community* in broad terms to include scientists, engineers and technologists as individuals or as disciplinary groups.

comprises experts on European science and technology policy/the ERA; security and defence policy/international security; innovation dynamics; and foresight methodology. Developing a common and agreed language and understanding of the "problem" has presented a challenge both within the project team and in our engagement with those policy communities. We will not discuss this problem in depth here but simply to say that the challenge has been considerable and has required us to structure our project organization around the creation of multi-disciplinary groups, frequently meetings (physical and virtual) and the conscious use of non-technical language in all our communications.

- *How to conceptualise the interaction between policy areas – SANDERA is concerned with the interaction between three policy areas. However, we have soon come to realize that policy areas do not have "relationships" with one another per se but that the "relationships" are more complex. Thus, we have had to find a means of charaterising the relationship between policy areas in a multi-dimensional framework which we will go on to describe in the next section.*
- *How to characterize drivers of change – we have also had to consider how to characterize drivers of change. Whilst there are some common drivers of change (not least those associated with technological change, economics and the future character of EU integration)), each policy area also has its own specific drivers that are likely to drive change in the particular policy area. Thus, we are having to find a means of charactering both drivers and the interaction of drivers within our multi-dimensional framework.*
- *How to characterize the blurring of the boundary between defence and security - Today and in general terms, "defence" and "security" are separate policy fields with different policy goals, different organisational actors and different policy communities. True, there is growing overlap (or blurring) in some aspects (the "Comprehensive Approach" favoured by the* European Union and many Member States means that military forces may find themselves working alongside civilian police and NGOs such as aid agencies – witness Afghanistan for example). However, this "blurring" is only emerging and may be regarded even as a driver of change in our study.

Characterising the relationships between policy domains

Let us explain how we are seeking to conceptualise the relationship between policy areas. SANDERA is concerned with the relationships between three policy areas. However, as we have come to understand, policy areas do not have "relationships" between one another. The relationship between, for instance, "ERA policy" and "EU security research and innovation policies" is about relationships between:

- Policy goals
- Resource allocations
- Formal and informal regulation
- Organisational actors
- Policy communities

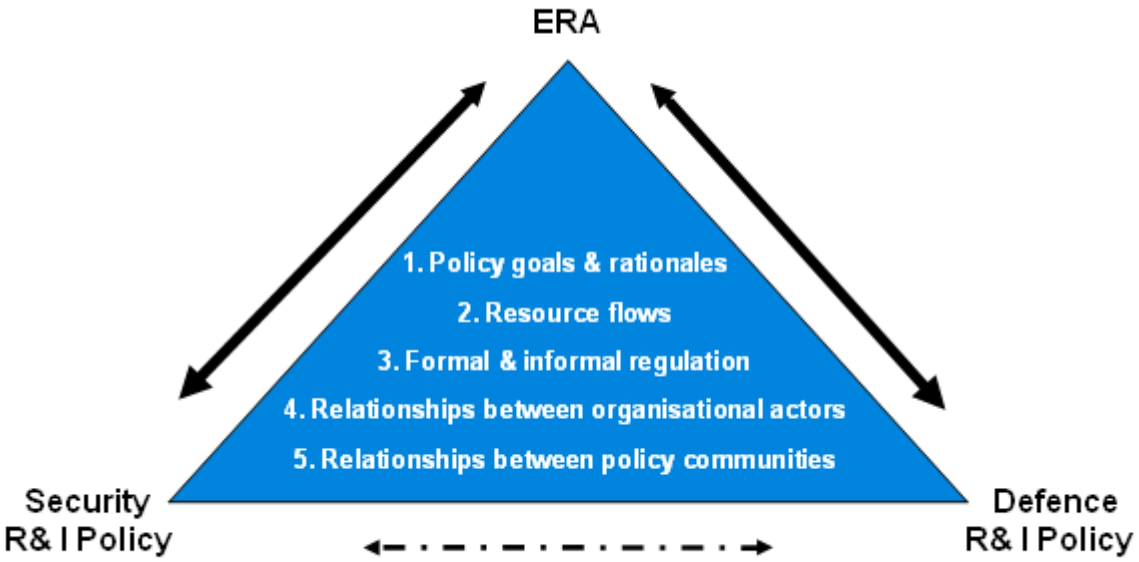


Figure 1. Target variables, to be explained of SANDERA.

Relationships between policy goals

Graphically the focus of SANDERA can be presented as in Figure 1. We begin by arguing that there can be relationships between the policy goals of different policy areas. *We define policy goals as meaning the aims and objectives of a policy area.*

We have already noted the policy goals of three policy areas but for completeness they will be repeated here beginning with the *ERA policy goals* which are as follows:

- Establishing large scale, longer term research projects within the Framework Programme to enable self-governed integrative structures in Europe.
- Supporting the networking of firms and research organisations beyond concrete research projects (technology platforms).
- Tighter co-ordination and cooperation among national research policies and programmes, through the establishment of indicators, benchmarking exercises and mutual learning schemes. 11
- Renewed rationales for research in Europe such as the freedom of mobility of knowledge (the "fifth freedom"), functional integration, and the creation of European added value.
- Grand Challenges

By *European defence research and innovation policy goals* we mean the goals as expressed in the EDA's Framework for a European Defence Research & Technology Strategy, namely:

[11] One key element of coordination was the famous 3% goal, whereby all countries in the EU should aspire to spend 3% of the GDP on research.

"a. ("Investing more…") substantiate the level of spending required to fulfil the needs of pMS, reflected in the targeted EDTIB characteristics which apply to a large extent to the defence technology base, namely: capability driven, competent and competitive;

b. ("Investing better…") help to focus Defence R&T investment at European level on areas not already covered by civil investment, and therefore influence the convergence and alignment of national policies; it should also promote best practice, improving efficiency in collaborative Defence R&T;

c. ("Investing more together…") help to make European R&T activities more transparent, supporting a step change in R&T collaboration, identifying where interdependencies among the pMS would aid the development of the required capabilities and the strengthening of the EDTIB"

By *European security research and innovation policy goals* we mean the goals as expressed in FP7 security research programme, namely:

"To develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism, natural disasters, and crime, while respecting fundamental human rights including privacy; to ensure optimal and concerted use of available technologies to the benefit of civil European security, to stimulate the cooperation of providers and users for civil security solutions, improving the competitiveness of the European security industry and delivering mission-oriented research results to reduce security gaps". [12]

Resource flows

Another important type of relationship between the policy areas that we can observe from the three Scoping Papers is through resource flows between those policy areas. *We define resource flows as movements of financial and human resources between policy areas.*

The main sources of financial resources under the ERA are:

- The Framework Programme
- Joint programming (ERANet and JTI)
- European Space Agency

For EU security, the main sources of funding for research and technology are:

- The Security Research theme of the Framework Programme managed by DG ENTR
- The Specific Programme for Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks managed by DG JLS

For EU defence, the main sources of funding for research and technology are:

- Funds from Member States managed on their behalf by the European Defence Agency

[12] DECISION No 1982/2006/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013)

Relationships between regulatory frameworks

We also propose that there can be relationships between the regulatory frameworks that underpin each policy area. *We define regulatory frameworks as the formal contracts, laws and standards and the informal rules of behaviour such as norms, routines, common habits and established practices that regulate "appropriate" behaviour by actors.*[13]

The regulatory frameworks that are important to the ERA include certain formal contracts, laws and standards such as those that govern intellectual property ownership/patents. The rules that govern the selection of projects under the Framework Programme and the ownership of resulting intellectual property are another example of formal regulatory frameworks. Equally, there are certain *informal* rules of behaviour such as the ERA's emphasis on scientific excellence and openness.

In the case of defence, the Knowledge Dynamics Scoping Paper emphasizes how, during the Cold War, the closed defence innovation system used a culture of secrecy as a means of limiting knowledge diffusion. In turn, this was supported through formal processes including laws governing access to sensitive facilities and the nationality of those who were able to work within the military-industrial-scientific complex. Arms export regulations were put in place by individual governments and international conventions and treaties were agreed to limit the development and production of certain technologies underpinning WMD such as the Nuclear Non-Proliferation Treaty (NPT) and the Biological and Toxin Weapons Convention (BTWC).

In the case of security, one example of the regulatory frameworks that are important is provided in our Background Paper on *Defence and Security R&D in Europe*. This noted how the sensitive nature of some security technologies and the issues surrounding operational security policies and vulnerabilities place an emphasis on secrecy rather than openness. In turn, this means that the Security Research theme of FP7 has some distinctive features that sets its governance apart from other elements of the Seventh Framework Programme.

Relationships between organisational actors

We have also recognized that there can be relationships between organizational actors from different policy areas. *By organizational actors, we mean those organizations who are responsible for a policy area. Organizations can have a facilitative, enabling, or operational role in the relationship between policy areas, depending on how many of the three following tasks are done by the organization: planning; decision-making; and implementation.*

Organisational actors in the ERA include:

- DG RTD
- DG ENTR
- Member States

[13] Krasner, S. D., *International regimes*, Ithaca ; London, Cornell University Press, 1983; North, 1991; Edquist and Johnson, 1997; Nelson, 2008

Organisational actors in EU security policy include:

- DG ENTR
- DG Justice Freedom and Security
- External Action Service
- High Representative/Vice President of the Commission
- FRONTEX
- EUROPOL
- European Maritime Security Agency
- European Space Agency
- Member States

EU defence policy organisations include:

- High Representative/Vice President of the Commission
- European Defence Agency
- European Military Staff
- Member States

Relationships between policy communities

Finally, we might foresee relationships between policy communities. *By policy communities, we have in mind the milieu of elected politicians, government officials, experts and expert bodies, industrial companies and associations and non-governmental organisations (including civil society) that actively influence the policy making process in a particular field.*

The ERA policy community (i.e. those who actively influence the policy making process) includes:

- EU Institutions (for every subject): EU Parliament, EU Committee of the Regions and the EU Economic and Social Committee
- (quasi) institutional groupings linked to EU policies: COST / also EUREKA / ESFRI platform (for infrastructures) / all Technology platforms
- European representations of stakeholders: EUA for universities (but also parallel elitist groupings such as LERU), EUROHORCS for heads of research organisations and research councils (and on a secondary level now ESF), EARTO for research and technology organisations, EARMA for research managers and administrators, EURODOC for PhD students, EASAC for the national academies of science, and the Confederation of European Business (CEB)
- European representations of different industries: maritime, aeronautics, rail, chemistry, iron and steel, digital technologies, software industries
- Non Governmental Organisations representing a diverse body of interests.

The defence policy community includes:

- The European Commission (as policy advocate)
- The European Parliament

- Defence companies and their industrial association (ASD)
- Defence-related research organisations
- Think tanks and the academic community
- Member States

The security policy community includes:

- The European Commission (as policy advocate)
- The European Parliament
- Companies with an interest in the security sector (in some cases there is an overlap with defence companies but there are also security-focused companies)
- Industrial associations for the security sector
- The network of organizations that came together as ESRIF (European Security Research and Innovation Forum) and may soon receive funding as an ERA-Net
- Security-related research organizations (again there are some overlaps with defence)
- Think tanks and the academic community
- Member States

Identifying drivers of change and building scenarios

The core task for SANDERA is to identify drivers of change and develop scenarios as a base for policy analysis and recommendations. We are using a three step process: (1) developing ideal type "tones" for relationships; (2) identifying drivers of change that might influence a move in the direction of one of those "tones"; and, (3) developing scenarios.

Ideal-type "tones" for relationships

Four ideal-type "tones" for relationships have been identified and agreed. The four tones are:

- *Indifference* - The relationship between the different properties of policy areas could be one of "indifference" where the developments of the properties in each policy area are perceived to be independent of one another or are perceived to have little impact upon one another. [14]
- *Competition* - Alternatively, the relationship between the different properties of policy areas could be one of competition where developments in one policy area are perceived to be in competition or actively antagonistic to one another. The relationship between the policy areas may be one of "competition" where the majority of properties of the policy areas are competing (or in conflict with one another).[15]
- *Cooperation* - Under a situation of cooperation, there is a recognition by policy actors that working together may generate mutual benefits, identifying many common interests while re-

[14] Note there are possible scenarios where one of the subsystems is very interested in the work, resources, etc. of the other, but the latter is fairly indifferent to the former and seeks to continue with its existing goals and activities.
[15] For the time being we agreed to stick to the slightly less confrontational term competition rather than conflict.

taining their distinctive goals, regulations and rules, and largely working with separate funding mechanisms.

- *Integration* - Finally, the relationship between the different properties of policy areas could be characterised as one of "integration". The major properties of formerly distinct policy areas would grow together at European level. Under a situation of integration, the policy areas give up some aspects of their separate identities and processes in favour of shared goals and processes in some discrete and well defined aspects of policy.

Drivers of change

Our next step is to consider the drivers of change that might influence a move in the direction of one of those "tones".

This task has presented some challenges. Whilst there are some common drivers of change (not least those associated with technological change, economics and the future character of EU integration), each policy area also has its own specific drivers that are likely to drive change in the particular policy area. We are charactering those drivers as follows:

- *Contextual drivers* - common drivers of change that act on all policy areas (although they may act to different degrees and in different ways). For example, these contextual drivers might include those associated with technological change, economics and the future character of EU integration.
- *Drivers specific to a policy area* – there are likely to be drivers that are specific to a policy area. These drivers promote changes in the policy area that in turn may have an impact on the tone of the relationship between that policy area and other policy areas. For example, new tasks for the military such as peace keeping are requiring a new understanding of the causes of conflict and means of conflict resolution short of armed conflict. This is causing the military to pay more attention to the social and behavioural sciences and in turn is a driver from the defence side for closer linkages to non-defence sources of expertise residing in the ERA.
- *Drivers that act directly on the relationship between two policy areas* – there are likely to be drivers that act directly on the relationship between two policy areas. For example, political pressures for closer linkages between defence and security research and innovation policy.

We are in the process of identifying drivers of change based on a combination of desk based research and face-to-face interviews. Our desk based research has been undertaken by three multi-disciplinary groups comprising members of the SANDERA consortium only that have looked at: security dynamics; ERA dynamics; and technology dynamics. Each analytical Task Group has collated and analyzed public domain material drawn from secondary sources including government reports, academic studies and reports produced by think tanks and expert bodies. They have also identifed and reviewed the results of foresight exercises that are relevant to SANDERA. There is a growing body of reports from foresight ex-

ercises that focus in whole or in part on security-related issues.[16] Equally, there are a number of European Commission-sponsored foresight studies on the future of the ERA.[17]

We are (as of May 2010) just beginning our face-to-face interviews. These interviews will be conducted with a variety of experts across the European Union including policy makers, stakeholders, scientists in key disciplines and experts located in universities and think tanks. We are conducting interviews across four groups: ERA policy; security research and innovation policy; defence research and innovation policy; and a fourth group comprising independent analysts, civil society and those we have characterized as "dissenting voices" (i.e. who have expressed critical perspectives on current developments).

We are also seeking to draw on other Commission funded studies as a source of drivers. In particular, "wild cards" derived from the iKNOW project and on evolving security threats from the FESTOS project.

Scenario building

Drawing on the drivers, the next stage of our methodology will be a driver-based scenario building exercise leading to scenarios on the future role of defence and security policies in the ERA. The core of the scenario building exercise will involve a workshop involving approximately 20 experts drawn from policy makers, stakeholders and the scientific community. The scenarios will focus on how each relationship "tone" could emerge by 2030.

Conclusion

In this paper we have introduced Project SANDERA which focuses on the future relationship between three critical European policy domains: namely, the EU science and technology policy strategy to move towards the European Research Area and those EU policies focused on the security of the European citizen in the world both through EU defence policies and EU security policies. We have considered some of the methodological challenges of using scenarios to characterise complex policy interrelationships and we have reported on some aspects of the methodological approach being adopted. The project remains a work-in-progress and we would welcome comments and suggestions which we ask you to send to Andrew.James@mbs.ac.uk

[16] We have already noted the foresight studies undertaken by the United Nations, European Defence Agency and NATO amongst others.
[17] See for instance, The Future of Key Research Actors in Europe. DG Research, 2007. This and other studies are available at http://cordis.europa.eu/foresight/

USING FAR AND DELPHI TECHNIQUES FOR ANALYSING FUTURE SPACE SCENARIOS: LESSONS LEARNED

Vivian Nguyen, Andrew Cruickshank, Len Halprin & Simon Ng
Defence Science and Technology Organisation, Department of Defence, Australia

ABSTRACT – *Scenarios are an important tool for strategic planning, policy and capability development, and, ultimately, investment decision-making. They play a major role in providing the context against which future planning decisions are made. Equally important is an understanding of the implications of the potential changes depicted in the future scenarios. Rigorous methods are required for developing scenarios and analysing the implications. Field Anomaly Relaxation (FAR) provides a way of developing plausible future scenarios and has been widely used to support strategic analysis and planning. The Delphi technique is used to gain consensus from Subject Matter Experts (SMEs) through a series of rounds of questionnaires, where results from the previous rounds are fed back to the panel of SMEs through the subsequent rounds. This paper describes how these two methods were employed within the Space 2030 Study conducted by the Australian Defence Science and Technology Organisation. The paper discusses the different stages of the study, how a set of alternative future scenarios were derived and how the Delphi technique was adapted and used to obtain expert opinion on how military operations and national security might be affected by space-related future technological, political and economic trends. The strengths and weaknesses of the tools are examined with the intention of communicating important lessons and key insights to other researchers doing a similar type of work.*

Introduction

Scenarios are an important tool for strategic planning, policy and capability development, and, ultimately, investment decision-making. Scenarios are used to identify and represent a range of new threats and opportunities that arise across a set of plausible alternative futures, uncovering early warning signals and refining perceptions of emerging problems to inform capability development and strategic planning.

Scenario planning methods have been employed by various organisations, ranging from academia and research institutions to law enforcement agencies and the military. They have been used to address issues ranging from global environment and climate change[1, 2] and future energy planning[3] to future military planning[4-6]. Field Anomaly Relaxation (FAR)[7] provides a way of developing plausible future scenarios and understanding how they may evolve, and has been widely used to support strategic analysis and planning. FAR does not, however, provide a rigorous approach for assessing the implications of scenarios. Other methods, such as the Delphi technique[8] (used to gain consensus from Subject Matter Experts (SMEs) through a series of rounds of questionnaires) can provide such an approach.

This paper describes how these two methods were combined within the Space 2030 Study conducted by the Australian Defence Science and Technology Organisation (DSTO) in order to investigate the implications of space-related future technological, political and economic trends on how military operations may be conducted in 2030.

Space 2030 drew on existing bodies of work conducted by DSTO and the Organisation for Economic Co-operation and Development (OECD). DSTO and the Future Land Warfare Branch of the Australian Army Headquarters used the FAR technique to develop the OPTEC[4] model as part of Defence's analysis of requirements for future warfighting capabilities. The model identifies five key drivers that will shape the future - political, physical, technological, economical and cultural. In 2004, the OECD developed a set of space scenarios to describe the future space environment in 2030[9]. These scenarios were constructed using influential factors, similar to those in the OPTEC model, but focussed largely on commercial and civil futures.

The paper discusses the different stages of the study, how a set of alternative future scenarios were derived and how the Delphi technique was adopted and used to obtain expert opinion on the implications of potential futures for space-related military operations. The paper discusses the strengths and weaknesses of the tools and techniques used in developing the scenarios, and establishes lessons that will be of value for other researchers in the field of futures analysis.

Space 2030 Study

The Space 2030 study was commissioned by the Defence Space Coordinating Office within the Australian Department of Defence and is being conducted by the Joint Operations Division of the Australian Defence Science and Technology Organisation (DSTO). The aims of the study are to:

- develop view of potential future trends in the drivers and enablers of space-related activities;
- develop a reusable set of future scenarios to support analysis of space operations;
- establish the impacts of future trends on space operations; and
- raise awareness of implications of trends for developing space capability and space policy.

Its scope includes a consideration of anticipated political, military, economic and technical trends and drivers that will define the future operating environment out to 2030 and how these trends and drivers will impact on future space operations. The study's initial focus has been on the Space Situational Awareness (SSA)[10] mission.

Overview of the FAR Process and Delphi Technique

Future Strategic Planning and the FAR Process

A variety of methods, have been developed for supporting future strategic planning. Some of these methods, such as forecasting and backcasting, are better suited to short- or medium-term planning because they cannot anticipate rare (but plausible) events[11-14]. Various interactive, workshop-style techniques have been used for constructing alternative future scenarios for long term planning[7, 15]. One such

method, Field Anomaly Relaxation (FAR)[7, 16] allows researchers to systematically identify, describe and link potential plausible futures through a four-stage workshop style process:

1. *Identify influential drivers*. For example, the OPTEC model was built on pOlitical, Physical, Technological, Economical and Cultural drivers.
2. *Develop a matrix of these drivers and their range of possibilities*. The OPTEC matrix was populated with the five identified drivers and their associated factors. For instance, OPTEC's Technological driver can be in 'revolution', 'evolution', or 'stagnation' state.
3. *Eliminate anomalies (implausible configurations of futures)*. The developed matrix allows construction of an enormous amount of futures, many of which are implausible. Such anomalies are removed which significantly reduces the number configurations, which are, in turn, clustered into distinct environments.
4. *Form a Faustian tree from remaining clusters and create narratives for scenarios.* A Faustian Tree is a visual representation of how the future might evolve depending on the type of change that can occur. The paths within the tree represent these changes. Short narratives are created to provide a broad description of each scenario, represented by a node in the tree.

Gathering Expert Opinion and the Delphi Technique

Various processes have been developed to help gather expert opinion[17-19]. The Delphi technique has been widely used as a way of seeking consensus amongst experts[8]. It originated in a series of technology forecasting studies conducted by the RAND Corporation in the 1950s[20] and has proven to be popular amongst researchers due to its flexibility in allowing positive attributes of interactive groups while avoiding negative dynamics of such interaction (for example, a dominant member influencing the group opinion). It is an iterative process, where the collected results or opinions from the previous rounds are summarised and fed back into the subsequent rounds and respondents are asked to revise their responses. This is conducted through a series of questionnaires. The technique's key features are anonymity and iterations of questionnaires with the purpose of refining opinion through controlled group feedback[21].

Space 2030 Study Process

This study has followed a four-stage process. This section describes these stages in detail.

Stage One – Exploratory Phase

In this exploratory stage, a comprehensive (but by no means exhaustive) literature review established a broad-brush overview of the current state of the space domain and its future trends. This process produced a qualitative picture of future space trends, classified into the categories of Drivers – Enablers – Constraints. Drivers strategically shape efforts and priorities in the space domain, and include the geopolitical environment and operational requirements. Enablers are the various technologies (satellite platforms, sensors, etc) and research and development activities that underpin new space-related sys-

tems and capabilities. Constraints, such as cost, space law or space weather, inhibit what can plausibly be achieved. These trends were inputs into the development of a set of future space scenarios.

Stage Two – Scenario Construction Phase

This stage produced a set of "Future Space Worlds": plausible alternative scenarios intended to support future analysis of space operations.

Rather than implement the FAR technique in full in order to produce a set of space futures, this study drew on an existing body of futures analysis (DSTO's OPTEC model[4], which was created using the FAR process, and OECD space scenarios[9]) and the trends identified in the previous stage in order to develop the study's space futures.

Comparison of OPTEC and the three OECD scenarios revealed that the OECD scenarios mapped well onto the major clusters of the OPTEC Faustian tree (Figure 1). The paths leading to these clusters within the OPTEC tree were judged to be plausible within the next two decades given the results of the initial literature review.

The OECD scenarios were further extended. The trends established in Stage one were used to inform the development of finer levels of detail in a set of space-focussed, militarily-relevant future scenarios. The resulting three scenarios can be described from the geopolitical and technology development aspects as "Continuity", which depicts the natural evolution of today's world out to 2030, the "Dystopian world", which represents the high tension – low tech future, and the "Utopian world" for the low tension – high tech future. For completeness, two more scenarios were created to encapsulate the high tension – high tech and low tension – low tech worlds.

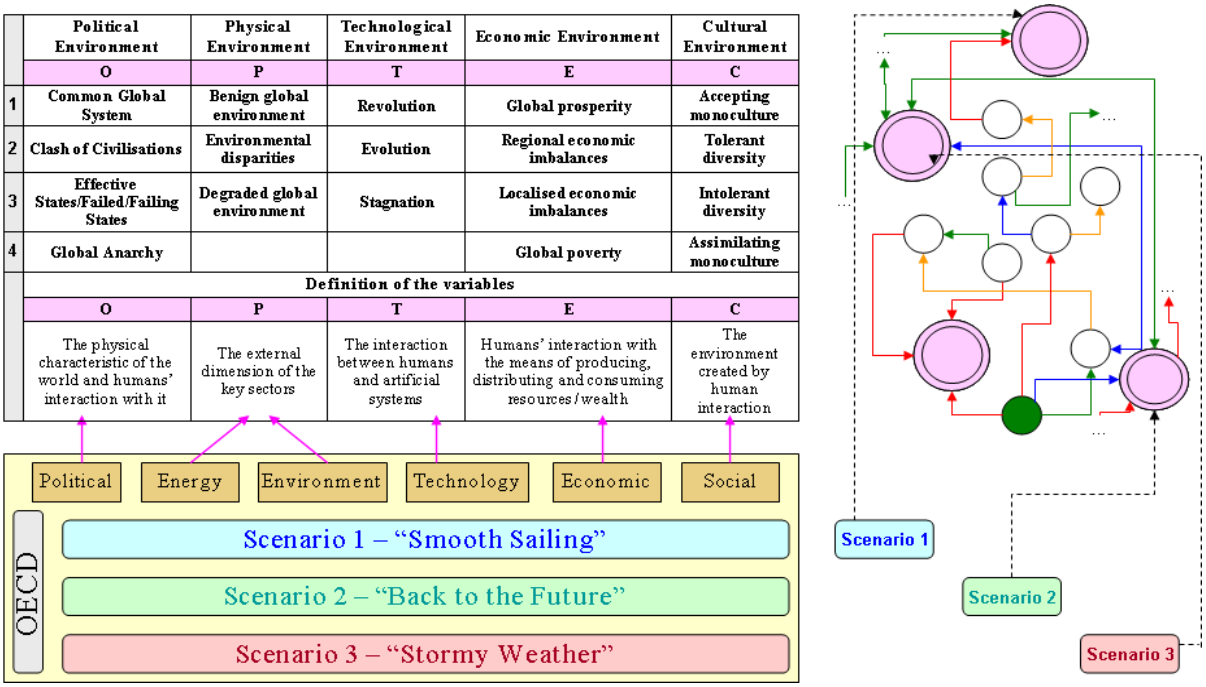


Figure 1. Mapping of OECD scenarios to OPTEC matrix and Faustian tree.

Stage 3 – Scenario Refinement Stage

A two round Delphi study was used to refine the "Continuity" scenario by gathering best estimates from experts in the space-technology field about the likelihood of progression for each of the trends identified in the initial literature review.

Subject Matter Experts (SMEs) were chosen for their experience and expertise in the area of space technology research and development. A total of 20 SMEs completed the Delphi questionnaires. Of the 20 participants, there were four academics working in the field of space systems and space technology (20%), four experts from space industry (20%), six military space operators (30%) and six defence scientists (30%). Representatives from US and European Space Agency were included.

Questionnaires were developed with the aim of identifying the importance of established trends to military space operations. The questionnaires were constructed so as to capture the following four types of information:

- Probability of a specified trend,
- Military importance of a specified trend,
- An estimate for a numeric value, and
- Open-ended discussion of a specified topic.

The questions were grouped based on the identified trend areas (including but not limited to satellite size, debris, sensors, communications), with each trend examined using questions of all four types. The questionnaire were designed to allow the SMEs to self rate their degree of confidence in each answer along a clearly defined scale of 0 to 1, providing a means for the study to incorporate degree of expertise or confidence in subsequent analysis. SMEs were able to make comments against any question as they saw fit. The developed questionnaires were tested on a group of four scientists (who are not in the original list of SMEs) with the purpose of removing ambiguities and identifying complex questions. The questionnaires were emailed to the SMEs specifying a two-week response time.

A snapshot of the questionnaire is shown in Table 1

Table 1. A snapshot of round 1 Delphi questionnaire.

Trend	#	Question	Answer	Explanation/Comment	Confidence
Size	1	What is the probability that the average size of a satellite launched in 2030 will be less than 10kg?	<0 - 1>	<Please enter your comment here>	<0 - 1>
	2	What is the probability that in 2030 satellite systems will mainly come in the form of satellite constellations or swarms?	<0- 1>	<Please enter your comment here>	<0 - 1>
	3	What is the probability that satellites in 2030 will be smaller than satellites with equivalent capabilities today?	<0- 1>	<Please enter your comment here>	<0 - 1>
	4 ...	In 2030, do you think size of the median satellite in the population of all PNT satellites, in any orbit, will be: *<highlight one option>*	1. Small picosatellite 0. 1-0. 3kg 2. Large picosatellite 0. 3-1kg 3. Small nanosatellite 1-3kg ...	<Please enter your comment here>	<0 - 1>
	10	What will be the military importance of small satellite size?	<0 - 1>	<Please enter your comment here>	<0 - 1>

Quantitative and qualitative analysis of the collected data was undertaken. Scatter plots were produced to visualise SME viewpoints on probability and importance questions showing their self-assessed

level of confidence. The resultant set of plots consisted of one plot for each probability and importance question. Based on the graphs, SME responses were then clustered into four categories – strong agreement, strong disagreement, mixed responses with mixed confidence disagreement, and interesting patterns (e.g. probability/importance grows as confidence grows).

SME comments were analysed together with the scatter-plots to identify associations between SME comments and the numerical responses. This uncovered ambiguities in the first round questions that may have contributed to the apparent lack of consensus identified during analysis. The second round questionnaire was designed to eliminate these ambiguities. Contentious views were also fed back into the second round.

Answers to open-ended questions and SME comments were analysed using a 'theming' technique. This was done by going through the SME's answers and counting the number of times a certain theme was mentioned. This indicated the bias or preferences the SMEs might have established in their minds.

This two-round Delphi process allowed the production of a refined set of space scenarios. The SME estimates were projected in the "Continuity" world. The four other scenarios were modified to take into account the SME estimates of technological rate of development.

Stage Four – Analysis of Implications on SSA operations

A two-round Delphi process was designed for this impact analysis stage. Two to four scenarios are considered sufficient to allow futures to be explored[22], and the "Continuity" and the "Star Wars" (*high tension – high tech*) worlds were chosen for this stage. The list of SMEs was modified to focus on experts with space operations (and especially SSA) background and experience. SMEs were informed about the purpose of this part of the study, the methodology and the expected outcome. The purpose of the scenarios was clearly explained, emphasising the fact that scenarios intended to provide an illustrative context for an analysis of implications but not to be predictive.

The questionnaire for this stage was used to elucidate the implications that the trends presented in the two scenarios would have on SSA operations in 2030 timeframe. The questionnaire sought expert opinion on how SSA operations might be performed in each of the presented worlds and how differently these operations might be carried out if there were any "game changing" technological events.

To design the questions for this round, it was critically important to understand the 'how' of modern SSA operations from a functional point of view. Current doctrine and contemporary research on space operations formed the basis of this understanding[10, 23, 24]. From this, two identical questionnaires, one for each scenario, were structured as follows:

- For every hypothetical event x in the set of SSA vignettes24:
- For every SSA function y necessary to be performed in the event x:
- How would SSA function y be carried out?
- How well (based on that function's specified measure of performance) will it perform?
- What are the consequences if it cannot perform or perform well enough?
- What are the alternative ways of performing this function?

The analysed data collected from these two rounds formed the basis of recommendations given to the stakeholders of this study.

Discussion and Lessons Learned

Synergy between FAR and Delphi

FAR is suitable for exploring wide-ranging dimensions of future worlds, and, thus, for providing means to deal with problems wide in scope. Delphi allows for delving into the depth of a problem by asking questions that requires specificity or low level detail.

In the Space 2030 study, FAR was used to construct a set of scenarios (incorporating several influential drivers) across a *wide* range of technological trends and then the Delphi questionnaires were used to gain a deeper understanding of *specific* trends. For example, the satellite size trend area was explored to a certain extend in the scenario construction phase (Stage 2), but Delphi was used to estimate the distribution of satellite size and configurations.

Potential exists to make better use of this synergy. The Delphi questionnaires were very long because we attempted to examine the specificity of the trends while still covering all ten trend areas. Variability in some trend areas can be reflected in careful construction of FAR scenarios, with those aspects that need more detailed examination tackled using Delphi. For example, the 'access to space' trend area could have been removed from the Delphi stage: initial findings in Stage one showed no major breakthrough in this field for the next few decades, and the Delphi questions on this trend was not to discover any major advances over the next two decades but only to confirm the initial findings; any possibility of a significant advance could have been represented in a FAR variation rather than requiring a set of Delphi questions.

Reuse of FAR Model

It is not always feasible to conduct a FAR process in its entirety due to the challenge of bringing experts together to conduct a face-to-face workshop over several days. Instead, this study demonstrates that existing work can be leveraged to good effect if such work satisfies the requirements of the study.

Stage 2 and 3 demonstrated that a considerable amount of effort was required in creating the set of space scenarios while building on an existing body of work. When considering which FAR model to use, it is important to take into account the drivers the model was built on, because these drivers are the ones that determined the paths to the alternative futures described by the model's Faustian tree. It is also vital to check whether the model remained valid and the Faustian tree is still relevant by examining the "presence" (present scenario) described by the tree's root node. Moreover, the validity and feasibility of the paths within the tree must be evaluated. Mapping of the OECD scenarios with the OPTEC Faustian tree confirmed the suitability of these artefacts to the study. The process also revealed that the paths to the scenario clusters were not too far fetched and were plausible for the next two decades.

The Delphi Experience

The Delphi technique proved to be a useful tool for gaining consensus amongst experts. However, the credibility of the technique is easily compromised with poor implementation. Gupta and Clarke[20] summarise criticism of the Delphi technique:

> *conceptual and methodological inadequacies, potential for sloppy execution, crudely designed questionnaires, poor choice of experts, unreliable result analysis, limited value of feedback and consensus, and instability of responses among consecutive Delphi rounds. (p.187)*

Reflecting on the methodology undertaken in this study, the experience gained and the lessons learned can be grouped based on these categories.

Choice of Experts

There is no precise mechanism for identifying an optimal number of participants to obtain valid results from a Delphi survey. Some authors[25] suggest ten to fifty participants as a good range. Miller[26] argues that feedback beyond the first thirty responses would generate repetitive information. Van Zolingen and Klassen[27] suggest that an acceptable number of respondents may vary according to the nature of the research being conducted.

In the context of this study, it was not simple to gather a large number of experts as space operations is a relatively new area in Australia. The final number of 20 participants (out of 38 invited and 26 accepted), covering experts from academia, military, industry and research organisations was deemed adequate for the study, with an analysis of the confidence measures obtained from SMEs indicating a reasonable amount of expertise within each trend area. However, it would be more efficient to ask the SMEs to self rate their expertise with regards to each trend area during the selection process to ensure adequate coverage of the topics of the study, and future work will adopt this approach.

Questionnaire Design

As previously discussed, the questionnaires were extensive. In the invitation letter and information sheet, we specified that two to three hours would be required to complete the questionnaires, but the time required for the SMEs to complete the questionnaires was considerably greater. This had an impact on the timeliness of questionnaire completion and the degree and completeness of commentary provided by the SMEs. Reducing the number of questions from round one to round two (82 questions in round one to 37 in round two) significantly improved the timing as well as the quality of commentary responses. More thorough testing of this variable prior to circulation of the questionnaires would also have been beneficial.

Given the multi-dimensional nature of the study (ten trend areas), it was difficult to reduce the number of questions in round one without compromising the data to be gathered. An alternative approach might be to split the SMEs into panels based on their expertise and provide separate questionnaires covering different trend areas to each panel.

The comments box proved to be a useful tool for gathering interesting insights when participants provided justifications for the answers in a form of comments. These comments provided further quali-

tative understanding of the SME judgements and helped uncover the ambiguities in round one that led to the disagreements identified during analysis.

Feedback

Nelms and Porter18 provide a useful scheme for classifying expert opinion gathering techniques. The techniques are differentiated based on whether they possess certain attributes: Talk (whether there is interaction between experts), Feedback (whether there is any feedback provided to help with the subsequent stages of the gathering process) and Estimate (whether the expert opinion gathering aims at arriving at a final decision).

The Space 2030 study was undertaken in an environment where collocation was not feasible. However, it required that experts engage with one another in discussion and feedback. Given these requirements, the Delphi technique was chosen as the means for gathering expert opinion. The technique worked well in Stage 3. However, due to the exploratory nature of the questions in Stage 4, the study required more elements of Talk and Feedback amongst the participants. If geography and logistics permit, it would be more productive to bring the SMEs together in a more interactive Delphi-style workshop to increase the level of idea exchange between the experts.

Having international representatives was useful in gaining an international perspective. However, given the security and the sensitivity of some topics, it was not possible to obtain information beyond unclassified levels from the international participants. In one instance, a SME returned an incomplete response because they had to remove some potentially confidential information. One SME from a particular organisation withdrew from the study in order to not compromise the integrity of their response. One other SME response contained classified information, which required extra effort during analysis and feedback. While gaining more insightful information is helpful to any study, it is important during the design stage to consider the effort to be invested in handling unclassified and classified responses, especially during feedback stage. Declassifying classified responses for feedback can result in distorted information.

Data analysis

Numerical responses invite numerical analysis, but for the most part the SME commentary provided the more significant information. The goal of data analysis was primarily graphical representation of data to allow the development of intuition about the participant responses. Several standard formats were used (Figure 2), including

- Scatter-plotting SME responses (of probability or importance) against confidence;
- Taking histograms of SME responses; and
- Taking histograms of SME responses weighted by confidence.

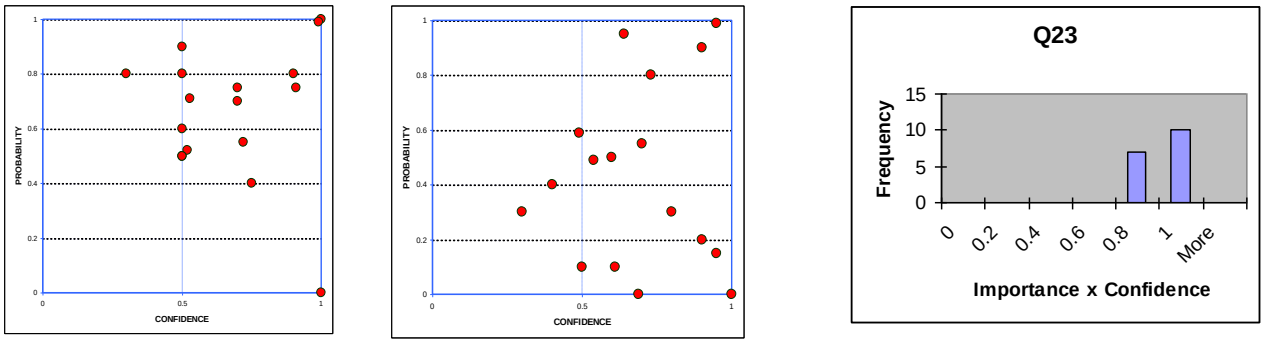


Figure 2. Example graphical representation of collected data.

The design of the questionnaires for Stage 3 investigated trends independently from one another. To test this non-dependency, *all trends vs. all trends* probability plots were generated. These plots were intended to show any correlation in the ideas of participants – did those who thought 'near-space developments' likely also believe that 'in-orbit' manoeuvring would be necessary. Results show that correlations are generally rare and usually weak. We might conclude from the relative rarity of correlations that:

- the trends selected are in fact orthogonal, with little real overlap in either their more primordial (science) or their higher (more applied) levels.
- most SME's thinking is not organised with the intimate detail that would allow relating the trends to one another.

Finally, one disappointment was that the logical combination of probability and importance (i.e. Risk) was not a direct subject of inquiry, since these parameters were estimated for different circumstances in different questions. Consequently such analyses had to be made inductively.

Conclusion

This paper has presented how the FAR process and the Delphi technique were employed within the Space 2030 Study and discusses the valuable lessons that were gained.

FAR has proven to be a useful method for constructing future scenarios and providing a traceable path from one scenario to another. This study has shown that, within limits, a well constructed FAR model and Faustian tree can be reused and the scenarios can be adapted for the requirements specific to this study, and that the Delphi technique could then be used to fine-tune scenarios to reflect the best estimated futures and to gather expert opinion on the implications of the scenarios on the space operations.

Implementing the Delphi technique requires considerable understanding of the analytical purpose, the required expertise and the domain of enquiry: sufficient expertise is required to cover the important areas of the study; a deep and broad understanding of the domain of interest is needed to formulate meaningful questions that will net useful data, and this process might require iterations of questionnaire design and testing; gathering data on expertise during Delphi provides a powerful tool for supporting future Delphi iterations and for interperating the results

Each technique has strengths and weaknesses. However, when combined the two are complimentary, providing a means for exploring the scope of a given problem and for undertaking more narrow development of aspects of that problem through structured and rigorous use of expert opinion. These insights will prove valuable as others seek to exploit these two techniques within analysis of futures.

References

1 O'Neill, B. C. & Nakicenovic, N. (2008) Learning from global emissions scenarios. *Environmental Research Letters* Vol. 3(045014).

2 Parson, E. A., Burkett, V., Fisher-Vanden, K., Keith, D., Mearns, L., Pitcher, H., Rosenzweig, C. & Webster, M. (2007) Global-Change Scenarios: Their Development and Use. *Washington, DC: US Climate Change Science Program.*

3 Silberglitt, R., Hove, A. & Shulman, P. (2003) Analysis of US energy scenarios: meta-scenarios, pathways, and policy implications. *Technological Forecasting and Social Change*, Vol. 70(4), 297-315.

4 Tri, N., Boswell, S. & Dortmans, P. J. (2004) Developing Possible Future Contexts Using the Field Anomaly Relaxation process. *DSTO Technical Reports*, DSTO-TN-0604.

5 Nicholson, J., Duczynski, G. A. & Knight, C. (1999) Defining Future Scenarios for the Special Forces After Next. in *Defence Operations Research Conference*, DSTO Salisbury.

6 Stephens, A. K. (2006) Future Urban States: a Field Anomaly Relaxation Study. *DSTO Technical Reports,* DSTO-TR-1910.

7 Rhyne, R. (1981) Whole-pattern futures projection, using field anomaly relaxation. *Technological Forecasting and Social Change*, Vol. 19(4), 331-360.

8 Dalkey, N. & Helmer, O. (1963) An experimental application of the Delphi method to the use of experts. *Management Science*, Vol. 9(3), 458-467.

9 OECD (2004) Space 2030: *Exploring the Future of Space Applications* Organisation for Economic Co-operation and Development (OECD). 239 p.

10 Space Operations - Joint Publication 3-14. (2009), United States Government.

11 Dortmans, P. J. (2005) Forecasting, backcasting, migration landscapes and strategic planning maps. *Futures,* Vol. 37(4), 273-285.

12 Coates, V., Fahrooque, M., Klavans, R., Lapid, K., Linstone, H., Pistorius, C. & Porter, A. (2001) On the future of technological forecasting. *Technological Forecasting and Social Change*, Vol. 67(1-17).

13 Robinson, J. B. (1990) Futures under glass: A recipe for people who hate to predict. *Futures*, Vol. 22(8), 820-842.

14 Goodwin, P. & Wright, G. (2009) The limits of forecasting methods in anticipating rare events. *Technological Forecasting and Social Change,* Vol. 77(3), 355-368.

15 Loveridge, D. (2002) The STEEPVacronym and process - a clarification. Paper No. 29 *Ideas in Progress*.

16 Rhyne, R. (1995) Field anomaly relaxation: The arts of usage. *Futures*, Vol. 27(6), 657-674.

17 Porter, A. L., Roper, A. T., Mason, T. W. & Rossini, F. A. (1991) *Forecasting and management of technology*. 1st ed, Wiley, John & Sons, Incorporated. 448 p.

18 Nelms, K. R. & Porter, A. L. (1985) EFTE: An interactive Delphi method. *Technological Forecasting and Social Change*, Vol. 28(1), 43-61.

19 Ford, D. A. (1975) Shang inquiry as an alternative to Delphi: Some experimental findings. *Technological Forecasting and Social Change*, Vol. 7(2), 139-164.

20 Gupta, U. G. & Clarke, R. E. (1996) Theory and applications of the Delphi technique: A bibliography (1975-1994). *Technological Forecasting and Social Change*, Vol. 53(2), 185-211.

21 Baskarada, S. (2010*) Information Quality Management Capability Maturity Model*. 1st ed, Vieweg and Teubner. 329 p.

22 Ratcliffe, J. (2000) Scenario Building: A Suitable Method for Strategic Construction Industry Planning? in *Construction Industry Development in the New Millennium*, Singapore.

23 Graham, D. & Gani, R. (2010) Space Situational Awareness Requirements Analysis. DSTO *Technical Reports*, Draft in preparation.

24 Australian Space Situational Awareness (SSA) Capability - Provisional Operational Concept Document. (2010), Defence Space Coordinating Office, Department of Defence, Australia. Draft in preparation.

25 De Loe, R. C. (1995) Exploring complex policy questions using the policy Delphi: A multi-round, interactive survey method. *Applied Geography*, Vol. 15(1), 53-68.

26 Miller, M. M. (1993) Enhancing regional analysis with the Delphi method. *Review of Regional Studies*, Vol. 23(2), 191-212.

27 van Zolingen, S. J. & Klaassen, C. A. (2003) Selection processes in a Delphi study about key qualifications in Senior Secondary Vocational Education. *Technological Forecasting and Social Change,* Vol. 70(4), 317-340.

ANTICIPATION AND INTERPRETATION OF BLACK SWANS AS A LEARNING PROCESS – LESSONS OF A VOLCANIC ASH CLOUD

Sirkka Heinonen & Juho Ruotsalainen
University of Turku, Finland Futures Research Centre (FFRC)

ABSTRACT - *One of the aims of futures studies is to highlight the possibility of sudden, rare, unlikely and unexpected events with widespread impacts, as well as to teach the capacity to anticipate them. In our turbulent world, such competence is critical not only in order to diminish the vulnerability of society and of its actors facing such events, but also to adapt our activities proactively to sustain the consequences of these occurrences. Such events have traditionally been called as Wild Cards in futures studies. The concept of Black Swans emerged as a synonym for wild cards, introduced by Nassim Taleb a few years ago. The list of modern Black Swans is getting longer all the time, while the concept itself is highly debatable. The Icelandic volcanic ash cloud in April 201 is being discussed in this paper as a case in point for collective learning from a black swan. The effort to anticipate and analyse Black Swans is related to several crucial issues in futures studies. First, it is an epistemological and semiotic question. Second, Black Swans are closely related to the notion of risks and uncertainties (Future as Risks). Third, Black Swans can be used to trigger a learning process towards higher futures awareness, futures consciousness, systematic proactiveness, sustainability and impact analysis (Future as Learning).*

Introduction and Background

One of the aims of futures studies is to highlight the possibility of sudden, rare, unlikely and unexpected events with widespread impacts, as well as to teach the capacity to anticipate them. In our turbulent world, such competence is critical not only in order to diminish the vulnerability of society and of its actors facing such events, but also to adapt our activities proactively to sustain the consequences of these occurrences. Such events have traditionally been called as Wild Cards in futures studies. The concept of Black Swans emerged as a synonym for wild cards, introduced by Nassim Taleb a few years ago (2007). The list of modern Black Swans is getting longer all the time, while the concept itself is highly debatable. Often presented, well known examples include such events as 9/11 terrorist attack in 2001, tsunami in SouthEast Asia in 2004, global financial crisis 2008, Haiti earthquake in 2010, as well as the Icelandic volcanic ash cloud in April 2010 which is being discussed in this paper as a case. The most recent event as a candidate for a manifestation of a Black Swan is the earthquake in Japan in March 2011, followed by a devastating tsunami and consequent impacts for a potential nuclear disaster.

The effort to anticipate and analyse Black Swans is related to several crucial issues in futures studies. First, it is an epistemological and semiotic question. Can futures be anticipated through various signs and signals at the present - can futures be foreseen through signs? Can futures be perceived as consisting of signs? Black swans can be preceded by weak signals or signs of possibly emerging trends pointing to them. However, black swans should not be confused with weak signals even though some of them may be interconnected. Second, Black Swans are closely related to the notion of risks and uncertainties – can futures be perceived as consisting of risks? Third, Black Swans can be used to trigger a learning process towards higher futures awareness, futures consciousness, systematic proactiveness, sustainability and impact analysis - can futures be approached as a learning process?

The Icelandic volcanic ash cloud provides a case in point for collective learning from a black swan. This case covers several issues ranging from the future of transport, ICT, health, food and agriculture, to the relationship and interaction between humans, nature and technology interaction.

Material and Methods

At the moment, there is no existing commonly acknowledged methodology for anticipating and identifying Black Swans. This is because black swans are by definition almost impossible to identify prior to their happening. However, there is a body of theoretical futures research around the topic of Black Swans and Wild Cards. A literature survey was made as a web search covering the journals of Futures, and Technological Forecasting and Social Change. The time horizon was chosen as that of a 12 years' period, starting from January 1995 up to January 2011. The results are presented in the following chapter of results.

All this discussion in futures literature about Wild Cards and Black swans has not, however, been so far developed into a coherent framework for identifying and anticipating sudden, rare, unlikely and unexpected events. Futures research is a proactive discipline that seeks for sense-making by developing understanding of the future world and helping decision-makers and citizens to prepare themselves for the future. There is growing interest shown towards the concept of black swans. They are a challenging and debatable but central topic for the advancement of futures research.

Although no stable models able to predict the future of the earth or of global economy exist, and even their theoretical possibility is an open question, it can be argued that the models and toolboxes used in futures studies can be significantly improved by a more sophisticated understanding of unexpected, Black Swan -like events. There are a few efforts worldwide to provide a methodological framework for monitoring forthcoming black swans[18].

[18] For example, Singapore has established a comprehensive system for Risk Assessment and Horizon Scanning (RAHSS). Since its inception there is an international conference programme to provide input to the system. The University of Manchester has developed another system for gathering and assessing weak signals and wild cards in its iKnow project http://wiwe.iknowfutures.eu/scan/easy/. In Finland, a few organisations such as Tekes (The Finnish Funding Agency for Technology and Innovation) and Finpro scan regularly futures signals. At Finland Futures Research Centre we have developed a concept "Creative Foresight Space" for creatively imagining possible futures and corroborating futures thinking and consciousness. The focus of action within this hybrid space (physical, virtual, digital, social) is on using imagination, intuition, improvisation, and exploratory experimentation as co-creative futures design. (Heinonen & Kurki 2011).

Consequently, this paper aims at presenting an evolutive approach to black swans, consisting of a three-fold analysis of the Future (futures) as signs, as risks, and as learning. A futures wheel was applied in conference session for analysing the case of the volcanic ash cloud from the eruption in Iceland in spring 2010.

Results

Future as Signs

The effort to anticipate and analyse black swans is related to several crucial issues in futures studies. First, it is an epistemological and semiotic question: can futures be foreseen through various signs and signals at the present or be perceived as consisting of signs as proposed by e.g. Kuusi & Hiltunen (2007)? Is it possible to acquire foresight knowledge of forthcoming sudden events? Can such foreknowledge be sought through identifying futures signs and signals?

Futures signals can be strong as presented by megatrends. They can be medium as shown through trends. They can be weak as presented by weak signals which are signs of emerging issues, possibly strengthening. [19] It is advisable to monitor the emerging world by identifying, analysing and interpreting futures signals at all these levels (megatrends, trends, weak signals and black swans/wild cards). Black swans can be preceded by weak signals or signs of possibly emerging trends pointing to these low probability but high impact events (see e.g. Petersen 2000; Hiltunen 2010, 74; Kaivo-oja; Kuosa 2007; 2009; 2010; Schoemaker 2002; Day & Schoemaker 2006). However, Black Swans should not be confused with weak signals even though some of them may be interconnected.

So, what then is a Black Swan? It is by definition a rare, sudden, unlikely, subjectively unexpected event that has wide impacts, either unfortunate or fortunate. Its characteristics are rarity, extremity, and post-event efforts to explain it. The concept of Black Swans emerged as a synonym for wild cards, introduced by Nassim Taleb in 2007. In the 17th century people in Europe were convinced via empiric observation that all swans are white. Later on they discovered that black swans exist too. This proves that mere observations are not reliable in forming theories about reality. Taleb, while describing Black Swans, says:"the world is most changed by extremely unlikely and unexpected events." The list of modern Black Swans is getting longer by the day. Recent events befitting the description range from the man-made 9/11 terrorist attack in 2001 and the ongoing financial crisis of 2008 to the natural ones such as the South-East Asian tsunami in 2004, the Haiti earthquake in 2010 and the volcanic ash cloud of Iceland in 2010. The most recent black swan was seen in Japan in March 2011, followed by a devastating tsunami and consequent impacts for a potential nuclear disaster.

[19] The concept of weak signals dates back to the 1970s (see I.H. Ansoff, Managing strategic surprise by response to weak signals. California Management Review Vol. XVIII (2) (1975) 21-33).

Wild cards have been discussed in futures studies since the 1970s and black swans since 2007 [20]. We conducted an article search using search words “black swan” and “wild card”. The Journals Futures, and Technological Forecasting & Social Change were included in the search. Among the search results we selected the following articles due to their relevance: Devezas 2010, Elahi 2011, Goodwin & Wright 2010, Kuosa 2010, Mendonça et al. 2004, van Notten et al 2005, Saritas & Smith 2011, Smith & Dubois 2010 and Walker et al. 2010. In the following we summarise and synthesise the discussion on the topic in these texts.

The black swans are about discontinuities and unexpected, they are manifestations of unlinearity. The concept of black swan can be seen as a complement to the standard, linear way of anticipating the futures by trend analysis (Dubois & Smith 2010). Scientific methods focus on issues that can be empirically studied and that can be assigned a probability of some degree. An obvious weakness of this approach is that it neglects discontinuities and the unexpected. Still, the unexpected happens and its wide-range impacts result partly from the very fact that we are not prepared to their occurrence. Our understanding of discontinuities is rudimentary. According to van Notten et al. 2005 the scientific function of black swans is the very exploration of potential discontinuity. Discontinuities and unexpected events are of crucial importance especially in social sciences where they are ubiquitious and where mathematical and strictly scientific methods are largely quite ineffective (Devezas 2010).

By definition black swans cannot be predicted by looking at the past and present trends. This does not mean they are unimaginable, though. Uncertainties are always plausible and surprises conceivable (Saritas & Smith 2011). The notion of surprise is strongly related to perception and expectation. Events are never surprising in itself, but only in relation to certain views about the environment. A proper scenario development should explore discontinuities to avoid future shocks catching us off guard (van Notten et al. 2005). Thus, black swans can be seen as a *practical tool* in adapting to turbulent environments. They help to switch our thinking mode into a more non-linear and imaginative direction and prepare us to confront the environment of constant flux. Though, it is not a sole question of preparedness and adaptation. Black swan consequences can open up new space and unforeseeable directions. Black swans tend to alter the fundamentals and have radical impacts so that new, possibly beneficial trajectories are created. (Saritas & Smith 2011.) In order to escape from the restricted approach of linear trend extrapolation Kuosa (2010) proposes an environmental scanning and pattern management framework to provide sense-making tools for futures signals.

Imaginative and open thinking mode is one way of approaching black swans. Goodwin and Wright (2010) stress that because anticipating rare and non-linear events is problematic there are only two remedies to them: firstly a) to provide protection for the organisation against the unexpected and also allow it to benefit from them if possible and secondly b) to provide conditions to challenge conventional ways of thinking. Altough black swans are hard to anticipate, expecting the unexpectable can also be empirism-based. Mendonça et al. (2004) suggest a tool that combines imaginative and empiristic approaches to identifying black swans and preparing to them: the wild card management system. It is based upon two components: weak signals and organisational improvisation.

[20] Another concept, synonymous of wild cards and black swans is "xevent" or extreme event as proposed by John L. Casti at IIASA to illustrate shocks that change our environment. ks. Casti, John, Ilmola, Leena, Rouvinen, Petri & Wilenius, Markku (2011) Extreme events. Helsinki.

The component of weak signals takes into account those black swans and wild cards that can be anticipated by observating, analysing and interpreting the environment. Weak signals are usually seen as information on potential change toward an unknown direction and thus as indicators of black swans. (Ibid.) An efficient way to operationalise this kind of research is to mine out-of-the-ordinary sources of information (Mendonça et al. 2009). The blindness for black swans and wild cards is often due to lack of awareness and a disregard for weak signals and not so much a total surprise (Dubois & Smith 2010).

The second component of organisational improvisation shows how improvisation can be used to deal with the events that cannot be predicted and are unexpected. It encourages non-linear thinking and not remaining loyal to planned actions. When needed general plans should be complemented with locally sensitive plans. Organisational improvisation highlights emergence: contrary to traditional planning practices which ignore emergence issues, organisational improvisation views them as inevitable part of complex systems. It calls for experiment with new and untested ways of thinking and problem solving. (Mendonça et al. 2004.) Consciousness of black swans tests and enhances the ability of a system to prepare and react to unforeseen but high-impact events (Dubois & Smith 2010).

Future as Risks

Black Swans are closely related to the notion of risks and uncertainties.

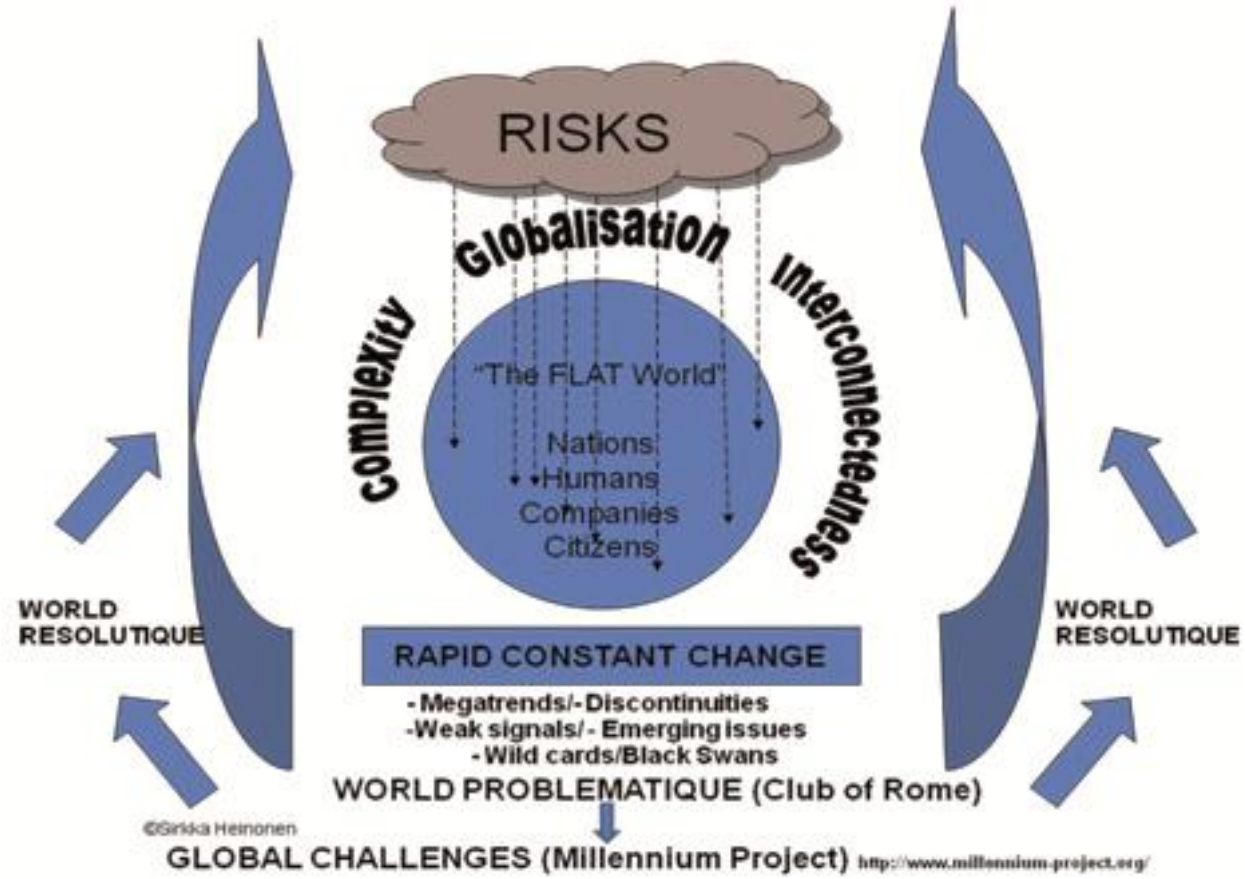


Figure 1. *Futures studies aim at highlighting and alleviating the risks looming above the globe (Heinonen 2008).*

Risks are about survival. Humans, companies, nations, wish to have continuity as individuals and within communities. This is the basis for both security thinking and futures thinking. (Heinonen 2008). New, uncertain, or unexpected things often threaten the feeling of security and survival. Risks have to be identified, faced, interpreted and managed. Risk is like the future, they both share the same qualities. The future holds a spectre of promises, a huge menu of possibilities. Only a fraction will be realised. Similarly of all the risks looming in the future above the globe and humankind – near or far – only a fraction will be realised. The concept of risks merits re-thinking within the futures thinking paradigm – new interest has been shown towards risks. The current foreseeable major risks emerge from social, environmental and energy-related issues. These risks have to be anticipated alongside with economic and technological risks that are often more conspicuous – new angle must be given. Some social phenomena put pressure on social cohesion, emerging rapidly and unpredictably in virtual communities – new risks are emerging. It is important to note that there are risks looming in real life, but also in virtual life. Not just computer crime, but pathological thinking of some minority groups (which can attract masses rapidly in virtual communities).

Risks are associated with uncertainties, and become visible in the flat world due to rapid change, interconnectedness and complexity (Friedman 2006). The future may look as a risky business due to such uncertainties. Competitive edge and even survival may result if one is strategically prepared for anything. Schoemaker (2002) even claims that one can profit from uncertainty and succeed in any circumstances because of the very capacity to expect the unexpected. Flexibility and robustness are essential characteristics of a strategic vision. (Ibid, 220). Aaltonen (2010, 28-29) draws attention to a multi-ontological futures landscape where different kinds of systems exist in which different causal assumptions apply. Therefore, robustness is needed to distinguish between linear, visionary, and disruptive systems. Uncertainties and risks are especially related to disruptive systematic change. Petersen (2008, 6) emphasises the necessity of not only understanding what is coming, but also adapting and adjusting to the new reality of coming large-scale disruptions. This is all the more challenging a task, since there are no direction-pointing precedents for what is coming. However, he points out that preparation is only useful before the fact.

People tend to think in probabilities and getting the odds right is treated as a critical skill in decision making. Black Swan phenomena pose a challenge, because their probability cannot be estimated. (Posner 2010.) Uncertainty can be simply defined as missing knowledge. Policy failures often follow from a failure to take uncertainties into account. Thus considering uncertainties is often crucial for long-term policymaking. (Walker et al. 2010). In a world of deep uncertainties illusion of knowledge is the greatest danger of all. Despite this ignorance is not associated with wisdom; Socrates said he knew nothing except the fact of his ignorance. (Elahi 2011.) One of the aims of futures studies is to highlight the possibility of sudden, rare and unexpected events with widespread impacts. Another aim is to teach the capacity to anticipate them – learning from futures.

Future as Learning

Black Swans can be used to trigger a learning process towards

- higher futures awareness,
- deeper futures consciousness
- systematic proactiveness,
- agile adaptation strategies
- alternative thinking
- sustainability and
- impact analysis.

The Icelandic volcanic ash cloud provides a case in point for collective learning from a Black Swan through interpretations. The volcanic ash cloud case covers several issues: the future of transport, the business of air transport, utilisation of ICT and social media, health issues, food and agriculture, the humans' nature–technology relationship. Black Swans can be used as a starting point for new development (patterns of behaviour). Their identification and interpretation is one sub-field within foresight competence, foresight intelligence and futures consciousness. In analogy to mathematics where arithmetic and geometry provide important fields within the discipline, in futures studies and futures consciousness anticipation of black swans is a useful, although controversial skill that can be learned and practiced. Learning to expect the unexpected, to imagine the unimaginable, and to know the unknown is a mental aptitude and process. It can be learned by doing, by using the existing few systems and frameworks for identifying and analysing weak signals and black swans/wild cards as mentioned above. It is also a part of the peripheral vision that Day & Schoemaker (2006) propose for companies to develop, in order to look beyond the field of core businesses or known developments. Peripheral vision aims at detecting weak signals that are considered as critical to company strategies and futures. Such peripheral vision could also be sharpened to detect black swans as well. [21] Futures consciousness could then cover not only horizontal scanning including megatrends, weak signals, and black swans or wild cards, but also multisensory and multidimensional grasping of futures as a learning process both in organisations, government, and educational institutes.

Description of the chain of events of the Icelandic volcanic ash cloud

The 2010 eruptions of Eyjafjallajökull in Iceland, although relatively small for volcanic eruptions, caused enormous disruption to air travel across western and northern Europe over an initial period of six days in April 2010. Additional localised disruption continued into May 2010, as the dry volcanic ash that lay on the ground was intermittently swept up by surface winds. The seismic activity started at the end of 2009 and gradually became more intensive until on 20 March 2010, a small eruption started. The ash

[21] Day & Schoemaker (2006, 5) use the metaphor of peripheral vision (human eye cf. organization eye) to highlight the complex mechanisms underlying an organization's capability to see what lies around the corner. They propose seven steps to bridging the vigilance gap: scoping, scanning, interpreting, probing, acting, organizing, and leading.

plume rose to a height of approximately 9 kilometres (30,000 ft).[22]. A few weeks after that, a larger eruption created an ash cloud that interrupted all air traffic to, from and within Europe for almost an entire week. The volcanic activity of Eyjafjallajökull has of recent returned to normal levels but the scientists at the Icelandic Meteorological Office (IMO) and the Institute of Earth Sciences, University of Iceland (IES) continue to monitor the volcano. [23]

This paper also presents the results from a workshop session in the conference on Security in Futures - Security in Change organised by Finland Futures Research Centre (FFRC) in June 2010 in Turku. Participants in the methodological session were invited to analyse the case of the above mentioned volcanic ash cloud, by applying the futures wheel method (Glenn 2009). On the wall of the conference room, there was a futures wheel. The participants then wrote their comments and ideas on the impacts of this black swan and attached them directly on the futures wheel. Immediate impacts from the event of the volcanic ash cloud were generated on the first circle of the futures wheel. Then indirect or secondary impacts were envisioned on the second circle.

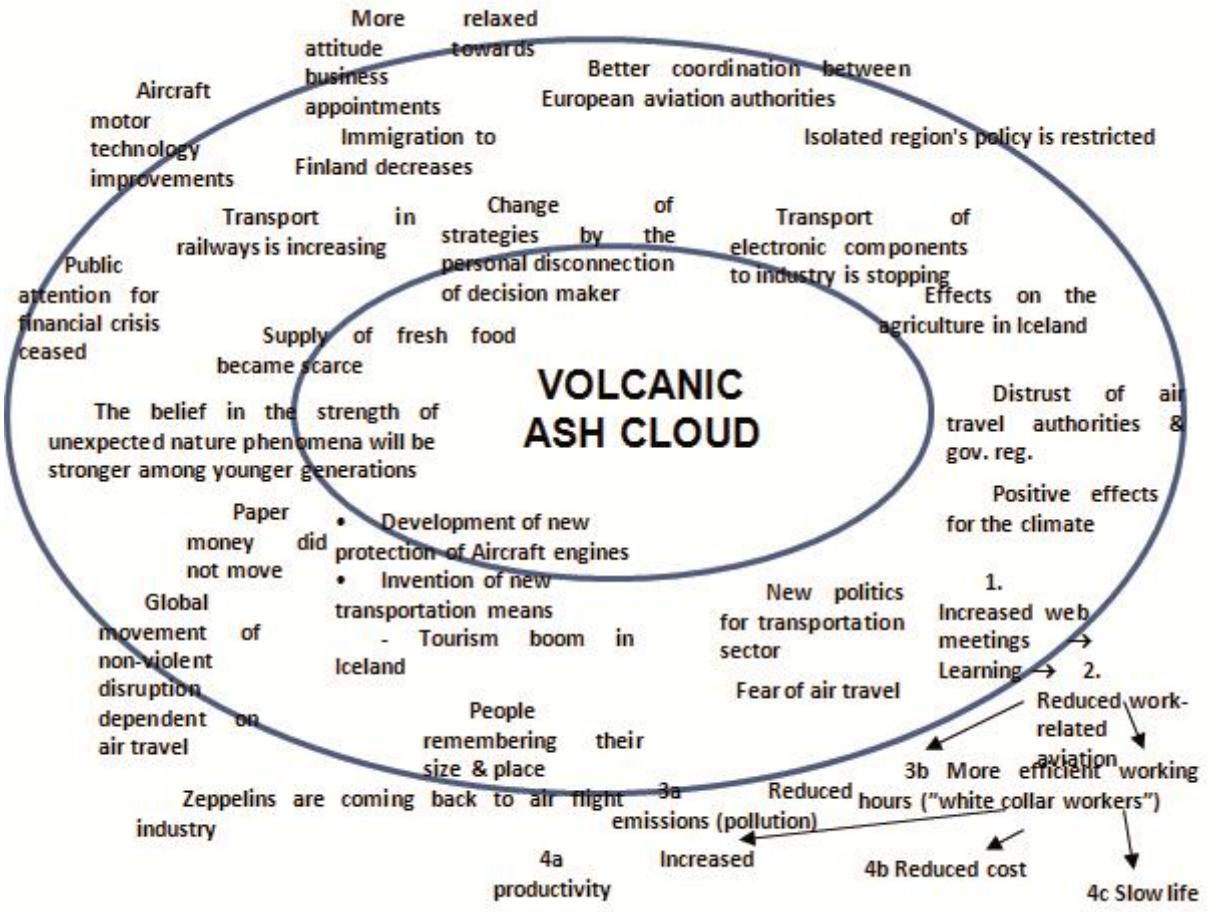


Figure 2. Futures wheel of the impacts of the Icelandic volcanic ash cloud.

[22] By 21 May 2010, the second eruption phase had subsided to the point that no further lava or ash was being produced. However, due to the large quantities of dry volcanic ash lying on the ground, surface winds frequently lifted up an "ash mist" that significantly reduced visibility and made web camera observation of the volcano impossible
[23] Igrún Karlsdóttir, Guðrún Nína Petersen, Halldór Björnsson, Halldór Pétursson, Hróbjartur Þorsteinsson, Þórður Arason: Eyjafjallajökull eruption 2010 - the role of IMO. http://en.vedur.is/earthquakes-and-volcanism/articles/nr/2072. Retrieved 27.3.2011 at 17:54.

As the Futures wheel indicates, although black swans are often natural disasters, their consequences are socio-cultural, political, economic, technological and also ecological. Black swans have deep and far-reaching impacts on the whole human world. Most consequences of catastrophes are naturally negative (e.g. economic losses, negative impacts on the agriculture, and decreasing supply of fresh food), but a few positive results can also be found (positive effects for climate, more relaxed attitude towards business appointments and slow life, technological improvements). All in all, the consequences are in multitude, so not only a thorough contemplation of possible black swans is essential but analysis and interpretation of their effects also. Thus, we can learn besides anticipation mindset, to rethink the existing paradigms and patterns of behaviour. This black swan was another reminder of the vulnerability of sophisticated technological systems (here air traffic). The lack of an alternative functioning transport system by rail in eastern Europe was accentuated. High speed train network throughout the whole continent could outbalance negative impacts from air traffic coming to a halt. One of the participants pointed out that the belief in the strength of unexpected nature phenomena will be stronger among younger generations. Perhaps the most critical lesson learned was that people remember their size and place on the globe and in their respective environments. Human interaction with nature should not take place through technological domination or dependent on vulnerable constructions, but through human/nature companionship with ambient technology as enhancing the quality of life.

Discussion and Conclusions

What you do not know, may become more relevant than what you do know. Anticipation of black swans builds up our preparedness for extreme futures. The identification and interpretation of weak signals (especially as clustered) may also help in anticipating black swans. The interpretation of black swans that have occurred may become a game changer – understanding how the current structures, thinking and behaviour should be changed to survive in our turbulent world. Black swans may on one hand lead towards discontinuities and tipping points, on the other hand they may be a result of such turns. Anticipation of possible (not yet occurred) black swans also means methodological evolution where various tools and systems have and will be developed specifically for this purpose. Since the black swans swim where the dragons are hidden (Elahi 2011), such techniques, approaches and frameworks are most welcome as focus on using imagination, intuition even, and exploratory experimentation as co-creative futures design.

We found no major differences or controversies in the definitions of the concept black swan. Instead we could formulate a clear synthesis. Above all black swans have a practical function: recognising them makes it easier to live and navigate an a world of deep uncertainties. Black swans were seen as vital complement or even replacement of the linear, predictable, scientific world view we are so used to. A world view that includes black swans brings a lot of added value into human systems: black swans are radical by nature, so their impacts are also profound. There are no definite methods to foresee black swans, but they can be imagined by thinking out of the box and prepared to by changing the ways we organise our actions and systems into a more improvisational direction. Acknowledging the importance of weak signals and synthesising individual ones can lead to possible black swans. Re-appreciation of

ignorance and the importance of unexpected events is needed: it sets our cognitive framework to suit the reality it really is.

References

Aaltonen, Mika (ed.) (2010) *Robustness. Anticipatory and Adaptive Human Systems.* Emergent Publications. Arizona.

van Asselt, M.B.A – van Notten, W.F. & Sleegers, A.M. (2005) The future shocks: On discontinuity and scenario development. *Technological Forecasting & Social Change,* Vol. 72, 175-194.

Cunha, M.P. – Kaivo-Oja, J. – Mendonca, S. – Ruff, F. (2009) Venturing into the Wilderness. Preparing for Wild Cards in the Civil Aircraft and Asset-Management Industries. *Long Range Planning,* Vol. 42, 23-41.

Cunha, M.P. – Kaivo-Oja, J. – Mendonça, S. – Ruff, F. (2004) Wild cards, weak signals and organisational improvisation. *Futures,* Vol. 36, 201-208.

Day, George S. – Schoemaker, Paul J.H. (2006) *Peripheral Vision. Detecting the Weak Signals That Will Make or Break Your Company.* Harvard Business School Press. Boston.

Devezas, Tessaleno C. (2010) On phase transitions, catasthropes and sudden changes. *Technological Forecasting & Social Change,* Vol. 77, 1412-1422.

Dubois, A. – Smith, C.J. (2010) The ´Wild Cards´ of European futures: Planning for discontinuities? *Futures,* Vol. 42, 846-855.

Elahi, Shirin (2011) Here be dragons... exploring the ´unknown unknowns´. *Futures,* Vol. 43, 196-201

Friedman, Thomas L. (2006) *The World Is Flat. A Brief History of the Twenty-First Century.* First updated and expanded edition. Farrar, Straus and Giroux, New York.

Glenn, Jerome (2009) *Futures Wheel.* Futures Research Methodology V. 3.0. Millennium Project. Washington.

Goodwin, P. – Wright, G. (2010) The limits of forecasting methods in anticipating rare events. *Tehcnological Forecasting & Social Change,* Vol. 77, 355-368.

Heinonen, Sirkka (2008) Multidimensional Concept of Risks in Horizon Scanning and Futures thinking. *Thinking About the Future. Strategic Anticipation and RAHS.* Volume published in conjunction with the second International Risk Assessment and Horizon Scanning Symposium. Ed. by Tan Hon Ngoh, Edna & Hoo Tiang Boon. National Security Coordination Centre & Centre for Excellence for National Security, S. Rajaratnam School of International Studies. Singapore, 53-68.

Heinonen, Sirkka & Kurki, Sofi (2011) Transmedial Futuring in Creative Foresight Space. Forthcoming article in: World Future Society Conference proceedings.

Hiltunen, Elina (2010) *Weak Signals in Organizational Futures Learning*. Helsinki School of Economics. Acta Universitatis Oeconomicae Helsingiensis A-365. Helsinki.

Hiltunen, Elina (2008) The Future Sign and Its Three Dimensions. *Futures,* Vol. 40(3), 247-260.

Hiltunen, Elina (2006) Was It a Wild Card or Just Blindness to Gradual Change? *Journal of Futures studies,* Vol. 11(2), 61-74.

Kuosa, Tuomo (2010) Futures signals sense-making framework (FFSF): A start-up tool to analyse and categorise weak signals, wild cards, drivers, trends and other types of information. *Futures* 42 (2010, 42-48

Kuosa, Tuomo (2009) Towards the dynamic paradigm of futures research – How to grasp a complex futures problem with multiple phases and multiple methods. Turku School of Economics. Series A-8. Turku.

Kuusi, Osmo – Hiltunen, Elina (2007) The Signification Process of the Future Sign. *FFRC eBooks.* Finland Futures Research Centre, Turku School of Economics. Turku.

Marchau, V. – Swanson D. – Walker E.W. (2010) Addressing deep uncertainty using adaptive policie: Introduction to section 2. *Technological Forecasting & Social Change,* Vol. 77, 917-923.

Petersen, John L. (2008) A Vision for 2010. Planning for Extraordinary Change. Fulcrum Publishing, Colorado.

Petersen, John (2000) *Out of The Blue - How to Anticipate Big Future Surprises*. Madison Books.

Posner, Kennet A. (2010) Stalking the Black Swan. Research and Decision Making in a World of Extreme Volatility. Columbia Business School, New York.

Saritas, O. – Smith, J.E. (2011) The Big Picture – trends, drivers, wild cards, discontinuities and weak signals. *Futures,* Vol. 43, 292-312

Schoemaker, Paul J.H (2002) Profiting from Uncertainty. *Strategies for Succeeding No Matter What the Future Brings*. The Free Press. New York.

Taleb, Nassim (2007) The Black Swan. The Impact of the Highly Improbable. Random House, New York.

6. MILITARY AND DEFENCE (INCL. TERRORISM AND CRIME)

ORGANISED CRIME AND ENERGY SUPPLY: SCENARIOS TO 2020

Victoria Baines
The European Police Office (EUROPOL)

ABSTRACT - *This paper presents the results of a joint scenario exercise which considered the impact of different energy futures on state, society and security, with particular emphasis on lifestyle and behavioural change – of the public, the authorities, and organised crime groups.* [1] *The scenarios presented highlight a number of different dynamics with the potential to affect interaction between organised crime and energy supply at all levels, and the responses of EU law enforcement.*

Introduction and Background

Around the world and more specifically in the EU, concerns have been raised regarding future energy availability, particularly levels of dependence on hydrocarbon imports (oil and gas). At the same time, law enforcement and open source information has indicated that organised crime groups are involved in energy supply to the EU and within EU Member States (MS). In the Strategy for Europol 2010–2014, the organisation has committed itself to scan the environment for new developments in internal security threats. With this in mind, Europol has carried out a scenario management exercise to examine the possible future involvement of organised crime in energy supply.

Material and Methods

A timeframe of ten years was set for the exercise, with the focus on interaction between Organised Crime and the energy sector in 2020. Narratives were drafted on the basis of plausible features within this timeframe.

Experts from MS law enforcement, the EU Commission, academia and the private sector were consulted on both the current situation and future developments. Analysis of these responses enabled the identification of current signals and helped to structure a subsequent workshop, in which the same group of experts identified critical uncertainties based on common themes and key factors in the participants' contributions. The following uncertainties were identified as the most critical: geopolitics and security of supply, price volatility, "respectabilisation" of crime, and lifestyle change.

[1] This paper is a condensed version of the full report, which can be viewed at www.europol.europa.eu

Security of supply and price volatility were considered to be the two uncertainties with the largest impact on the energy future and the greatest levels of uncertainty, and as such formed the axes on which the scenarios were plotted. A high level of price volatility correlates with a world of unplanned responses and inconsistent regulation, while a low level of price volatility correlates with planned responses and more consistent regulation. Organised Crime's drive for respectability and lifestyle change were nevertheless considered to be cross-cutting issues and key factors in the possible futures described, which therefore served to flesh out the narratives.

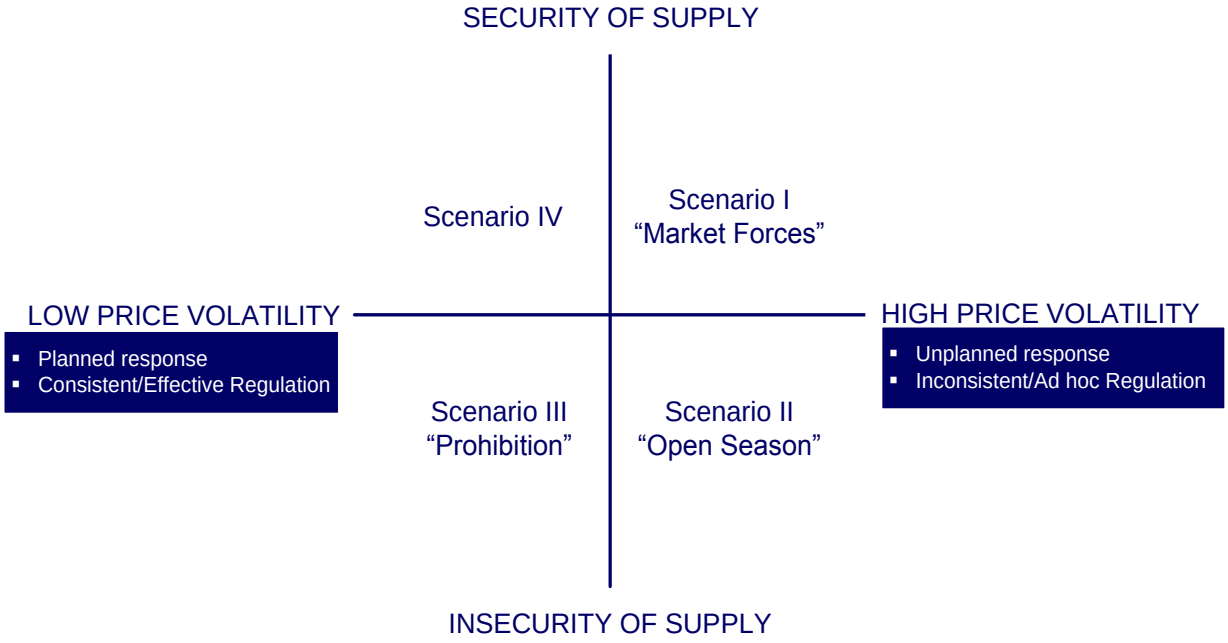


Figure 1. Plotting the Scenarios.

This paper presents the first three of these on the basis of consideration of their plausibility, impact and opportunities for Organised Crime. Scenario IV remains possible: where energy supply is secure and highly regulated, Organised Crime finds opportunities in, for example, illicit fuel supply which undercuts legitimate pricing by means of regulatory non-compliance, and the exertion of corruptive influence in order to subvert existing restrictions or press for regulation which is more suited to its interests.

The worlds which result from the dynamics between the two critical uncertainties have been elaborated using the PESTELO approach to environmental scanning[2], not only responding to signals presented by current and developing interactions between Organised Crime and the energy sector, but also drawing on an extensive literature review.

[2] The PESTELO approach considers in turn the political, economic, social, technological, environmental, legislative and organisational factors.

Results

Scenario I - "Market Forces"

This is a world in which energy supply is secured by various means, and an absence of more stringent regulation of the energy and financial sectors affords a continued role for the major commercial suppliers. In the sense that the energy supply arrangement is not sustainable, this world represents an intermediate stage on the road to "Open Season" (Scenario II).

MS engage in a certain amount of cooperation in order to achieve comfortable levels of energy security on the basis of national priorities. The EU loses its vision in as much as it comes to serve national, and even personal, interests: EU policies are somewhat changeable as a result. MS come together to secure energy supply from the most important sources. In cases where supply companies experience high levels of OC infiltration, governments and the EU increasingly rely on "deals with the devil" – e.g. bilateral agreements with partners infiltrated by OC, further legitimising OC interests.

The agreement reached at the 2009 Copenhagen summit on climate change (COP15) is viewed as a bargain based on shifting national priorities. As a result, there is little will at central government level to exceed the minimum expectations set. Measures to reduce emissions are driven by the prospect of profit rather than by climate change concerns: "cap and trade" gains strength because of an already established trade in carbon credits and a market for Carbon Capture and Storage (CCS); in the absence of requisite regulation, this is accompanied by an increase in Emissions Trade Fraud (ETF). Moreover, in light of limited will to drive forward anything but the minimum requirements to tackle climate change, populations outside the EU experiencing the first effects of global warming are on the move. Within the EU, national borders remain open, facilitating migration for employment purposes. Such freedom of movement not only acts as a pull factor for both licit and illegal migration to the EU but, especially in areas of energy development, also begins to create temporary migrant communities which are vulnerable to the influence of OC because of their isolation from mainstream society.

Free market principles preserve a role for international energy companies, and both globalisation and the import/export trade are largely unhindered. The liberalisation of the EU energy market continues apace, and competition results in price reductions for some consumers. Since the EU market remains open both to foreign direct investment and to acquisitions by foreign energy supply companies, OC groups based within and outside the EU have the opportunity to act as shareholders and suppliers respectively. Both eventualities afford OC greater control and influence over the legitimate economy, and opportunities to exercise power in commercial decision making.

Outside of the EU, private companies compete with local governments to exploit remaining fossil fuel reserves, including those – such as unconventional gas or shale oil – made profitable or accessible through technological developments. In cases where supply companies experience OC infiltration, this leads to increased OC influence over fossil fuel production. Ultimately, competition for resources leads in some source areas to tension between governments and international energy supply companies, and the re-nationalisation of dwindling fossil fuel reserves. In this event, such actions push the future towards the "Open Season" scenario.

Fuel prices, meanwhile, are still subject to volatility: speculation on energy markets initially goes unchecked, and recession prompted by spikes in liquid fuel prices remains a real possibility. Further OC infiltration of the EU energy sector and the continued practice of speculation conspire to create a situation in which OC has the ability to affect energy prices for its own profit, whilst each economic setback renders legitimate business more vulnerable to compromise. In a similar vein, OC engages in corruption of the private sector to gain privileged information on energy futures and to capitalise on short-term investment opportunities by anticipating price changes. By playing the energy markets, OC groups are also able to engage in potentially profitable money laundering.

Because on the whole EU energy supply is not yet self-sufficient, it remains vulnerable to disruption by non-state actors, with a potential impact on price levels. Whilst disruption can be achieved by means of terrorist activity (e.g. damage to oil pipelines), equally this vulnerability presents OC groups with opportunities to disrupt supply in order to affect price levels, thereby deriving increased profit on investments.

In many ways lessons have not been learnt from the global financial crisis of 2007–9. Amongst private citizens, meanwhile, the fear of recession and financial hardship remains. This manifests in behaviour such as stockpiling and voluntary, consumer driven transition to energy efficient technologies in the belief that these will reduce individual expenditure. A cycle of "boom and bust" – be this actual or merely perceived – encourages OC groups to hoard liquid fuels and other consumer items for resale in the event that prices rise. At the same time, lack of tax harmonisation results in differences in price for end consumers in MS. OC profits from these discrepancies, smuggling liquid fuel within the EU, from low duty/price to high duty/price areas.

Although renewable energy technology remains expensive, some individuals and local communities choose to meet the initial outlay of small-scale independent generation, on the understanding that it will be more cost effective in the longer term. Likewise, energy efficient technology is embraced because it is money-saving technology. Lithium batteries, for example, are popular because they require less charging, and there is increased uptake of hybrid vehicles in response to rising or unpredictable fuel prices. As energy efficient products become more sought after by consumers, so too is there an upsurge in their illicit and counterfeit supply.

In the absence of enforced limitation on energy consumption and globalisation, however, MS populations remain active consumers of electrical appliances and electronic gadgets. There is a persistent trend for incorporating several different functions and applications in a single appliance, and increasingly efficient infrastructure – e.g. ever faster broadband Internet connections – puts less of a strain on electricity consumption: at a global level, this is counterbalanced by the first-time introduction of such products to the developing world. By the same token, portable electronic items continue to be highly sought after, and illicit supply of these – be they stolen or counterfeit – proves attractive to OC.

In terms of the energy sector's attractions to OC relative to other criminal activities, continued globalisation and free market principles combine to make this world one of persistent expansion of telecommunications and Internet-mediated functions such as online retail and banking. In this environment, Internet-facilitated frauds by means of identity theft and hacking allow OC to derive higher profit and quick gains by less visible – and therefore lower risk – methods than direct involvement in energy-related sectors. Equally, when loss of revenue prompts the adoption of more stringent data security measures by banks, retailers and individual consumers, and more concerted legislative and law en-

forcement responses, the focus of OC reverts to the assured demand and essential supply of the energy sector.

In a profit- as opposed to policy-driven energy landscape, legitimate investment in large-scale renewable technologies runs into difficulty. The larger energy companies are unable to justify the comparative lack of quick return to their shareholders, leaving those willing to make longer term investments and those with lower capital costs – such as OC – to step in. Beyond 2020, the implications of this are that by default OC will be a leading player in renewable energy supply, on which the EU will become increasingly dependent as remaining fossil fuel reserves dwindle.

The dominant legislative feature of this world is an absence of effective regulation of the energy and financial sectors, or more specifically, prevailing self-regulation, a situation reinforced by a comparative lack of law enforcement knowledge of these sectors. Since the geopolitical and economic factors provide fertile ground for OC infiltration of the energy sector, self-regulation serves to facilitate concealment of OC activity.

Eventually, however, a more consistent focus on asset recovery by governments, and the desire of energy companies to know and manage the expectations of their shareholders, lead to the introduction of tighter controls on investments, e.g. to determine the origin of investments in the energy sector, and legislation throughout the EU against money laundering. As prices continue to fluctuate, speculation on energy futures comes under particular scrutiny in an attempt to encourage stability. Additionally, there develops a greater focus on corporate criminal liability, in response to the effects of OC infiltration of energy supply companies. Legislation to protect the environment from damage related to energy production and supply is an afterthought.

Due to a lack of knowledge and experience in the field, law enforcement initially fails to provide effective responses to OC involvement in the energy sector and energy finance, preferring that these industries police themselves. As the amount of lost revenue and the level of OC influence on private companies become apparent, the tendency for transnational OC investigations to follow money trails leads to prioritisation at both national and international levels of financial investigation and money laundering cases, incentivised in some countries by the prospect of additional funding for law enforcement, as provided for in Proceeds of Crime legislation.

Scenario II - “Open Season”

In a world of low energy security and high price volatility, governments and non-state actors alike compete to secure access to remaining fossil fuel reserves. Absence of a binding agreement on climate change results in poorly coordinated and ad hoc responses to the problem. Outside the EU, populations experiencing the first effects of global warming are on the move, putting added strain on the energy resources of EU MS against a backdrop of increasing scarcity.

In some parts of the developing world, this competitive atmosphere manifests as neo-colonialism: interested parties seek to carve up territory in energy hotspots, which in turn engenders geopolitical instability. Recognising that fuel ownership is power, the best resourced OC groups move to infiltrate and influence both government machinery and large energy companies in source countries, perpetuating the

culture of "rent-seeking"[3] already observed in some areas. OC groups from overseas, including those from the EU, profit from opportunities for unregulated investment in these areas.

At the same time, rising prices prompt an increase in oil bunkering, and other fuel thefts in consumer nations such as the laundering of "marked" oil[4]. Meanwhile, suppressed economic growth associated with the "resource curse"[5] acts as a push factor amongst source country populations towards both involvement in criminal activity and migration (both licit and illegal) to countries with better living standards. Prioritisation of energy security in source areas prevents the authorities from responding effectively to other types of criminal activity, abstracting law enforcement resources from policing the trafficking of other illicit commodities, such as drugs, counterfeits and human beings.

Within the EU, increasing energy scarcity, unpredictable price levels and changes of government in some MS weaken the implementation of the Lisbon Treaty and prompt a movement away from planned cooperative responses to ad hoc bilateral agreements. Whilst designed to secure energy supply for individual countries, unless complemented by supply diversification these in fact result in new interdependencies, and a shift in the balance of power towards those countries within and outside the EU on which the MS depend, and those MS who are self-sufficient, e.g. those with unconventional gas deposits. Moreover, in cases where there is direct OC involvement in the energy sector, this entails MS dependence on OC for essential services. Cracks start to show in the EU itself, as new political alliances are formed and old alliances regain their strength on the basis of energy requirements. In such a competitive environment reduced communication between MS and less effective regulation at EU level foster political corruption, thereby providing opportunities for fraud, and the undue influence of OC on decision-making.

Accordingly, and in line with an increasing politicisation of energy, MS turn inwards and work to expand their own energy supply capacities by developing alternative energy sources at a national level and improving energy efficiency in response to uncertainty over its availability – also expanding or renewing development of local fossil fuel reserves which have previously been inaccessible or unprofitable. In some MS this heralds a reversion to nuclear power, in others to solar, wind and hydroelectric generation. Whilst nuclear power generation itself remains under state control, nuclear fuel and components become sought after commodities, and impaired cooperation amongst MS means that those nations embracing nuclear power have to make difficult choices concerning the disposal of nuclear waste. In light of sensitivities over the risks attached to local storage, there are increased opportunities for OC groups experienced in waste disposal: given OC's propensity for non-compliance, this presents obvious risks to public health and safety in both MS and countries outside the EU, especially the developing world. The drive for local energy supply also prompts increased development of waste-to-energy (WTE) technology, doubly attractive in so far as it combines energy production with recycling. Whilst this technology is still in its infancy, OC's historical involvement in waste management means that they are in the vanguard of its introduction.

---

[3] "Rent-seeking" denotes behaviour whereby individuals or companies use their resources to effect changes in public policy from which they themselves will derive benefit.
[4] E.g. cheaper diesel dyed red and intended for use only by off-road agricultural vehicles.
[5] "Resource curse thesis" denotes the phenomenon whereby countries with abundant natural resources experience lower economic growth than those with fewer natural resources.

Renewable technologies remain expensive to develop in the short term, so public subsidies continue to be offered in order to attract investment. These in turn are liable to exploitation by OC, to the detriment of local and national budgets and ultimately, in the event of a failure of these projects to be realised, the end user. Whilst greater focus on renewables and energy efficiency has self-sufficiency as its aim, some dependence on countries with reserves of components and expertise essential to current renewable technology is inevitable: for example, the importance of rare metals to wind power generation and energy efficient battery development, and advances in green energy research and development (R&D) not only find world leaders in East and South East Asia, but also open up these markets to the possibility of illicit trafficking of components and intellectual property (IP) theft.

High price volatility results in part from a lack of effective regulation. Energy prices – particularly those of liquid fuels – impact on transport costs and, by extension, on the price paid by consumers for basic supplies such as food. Because MS enjoy different levels of economic growth, some are more equipped than others to weather the storm. Higher operating costs mean fewer opportunities for "new" MS growth, which renders legitimate business structures (LBS) vulnerable to investment from OC. At the same time, OC profits from differences in terms of taxation and prices by means of illicit trafficking/smuggling of fuel, food and other essential commodities. Black markets thrive, OC profiting from price volatility by buying low and selling high. Since these markets are entirely unregulated, customers come into contact with dangerous, poor quality and waste-grade commodities.

The inward focus of MS and constraints on long-distance commercial transport encourage local industry and agriculture, including biomass crop cultivation. In so far as this improves energy efficiency and helps to secure the availability of essential items for local populations this is a positive move. However, it also presents new opportunities to legitimate and criminal investors alike. Equally, it acts as a pull factor to migrants from countries outside the EU and, indeed, MS with lower economic growth and living standards. Gangmasters have sizeable irregular workforces at their disposal, and MS become increasingly dependent on OC and irregular labour for the production of both essential and luxury consumer items.

In the absence of EU-wide financial regulation, investment in MS energy sectors by non-EU actors continues apace, with legitimate and criminal investors alike exploiting opportunities presented by regulatory diversity in the EU, facilitating the further infiltration by OC of essential legitimate services. Moreover, a world in which energy is increasingly sought after and subject to fluctuations in price is one in which OC is able – with the requisite knowledge and expertise – to launder money at a profit, thereby generating further funding for criminal activity. Additional opportunities emerge in the form of privatisation of state-controlled services in response to recessions triggered by oil spikes: with comparatively high levels of ready funds, commercial concerns with links to OC are well placed to step into this gap in the market.

Private citizens subject to higher prices, a lower quality of life and perhaps unemployment come into increasing proximity with OC, through direct involvement in criminal activity, purchasing fuel and other goods from the black market, or indeed looking to OC groups for security. In this society, outages and brown-outs are a reality, and low-level criminals take advantage of the cover of darkness to engage in looting and robbery. Fear of crime increases, fuelled by feelings of insecurity and isolation, and tensions between resident and migrant communities: national and local law enforcement, meanwhile, are subject

to the same cuts in expenditure as other government services and are less able to respond effectively. Street policing is increasingly conducted by private security firms, and OC groups are instrumental in keeping the peace and communities safe. At its worst, this manifests as racketeering, with OC profiting from threats of violence.

Reduced availability of liquid fuel at a stable price combined with technological advances encourages more people to work from home. This has a positive impact on both family life and community spirit, marking a reversal of the trend for commuter towns which are deserted in the day. Overseas tourism is adversely affected by fuel prices. In some MS a surge in local tourism driven by family budgets compensates for this, and opportunities for investment present themselves accordingly: in those MS and non-EU nations with high levels of economic dependency on overseas tourism, numbers of unemployed and deprived citizens swell.

Driven by uncertainty and financial constraints, there is increased interest in small-scale power generation by individuals and local communities. Since in the short-term this technology remains expensive there is a corresponding increase in the theft and resale of generators and components: at the same time, OC steps in to provide power facilities where local funds are lacking. As individuals seek to become more self-sufficient, MS also begin to see an increase in organised wood theft and resale, with a corresponding impact on local environments as a result of both deforestation and higher levels of emissions from wood burning.

In an effort to save money the public also embraces energy efficiency. There is a captive market not only for stolen, but also counterfeit or "duty free" versions of, goods such as lithium batteries, energy efficient light bulbs, and electrical appliances with low energy ratings. This buoyant illicit trade has a negative impact on the legitimate trade in such products, further restricting economic growth in MS.

Legislative measures are largely reactive, driven by perceived energy insecurity and introduced only in response to observable activities. In an effort to preserve dwindling resources, MS legislate against immigration, effectively shutting their doors to migrants: accordingly, the largest migrant communities are found in the MS which are last to legislate. Higher penalties are introduced for crimes such as theft of fuel and energy components, and electricity diversion, as are administrative penalties for energy wastage and inefficiency. Legislation against counterfeit products becomes more stringent as the negative effects of counterfeit medicines, etc. on public health and safety are observed, as does legislation against the underground economy in an attempt to protect legitimate commerce.

By the same token, new investigative priorities (e.g. fuel and IP theft) and reduced law enforcement capacity conspire to take their toll on the concept of Intelligence Led Policing. A shift of focus to national and local policing priorities makes transnational OC less visible, enabling it to flourish comparatively undetected. Environmental crime becomes a priority only when the effects of unregulated waste disposal become visible. Whilst there exists the will to regulate the energy and financial sectors with a view to determining the origin of investments and stabilising energy prices by limiting speculation, in practical terms the need for capital injection in an uncertain financial climate overrides this.

Scenario III - "Prohibition"

A world of low energy price volatility is one in which effective regulation – be this by means of fuel price banding or taxation – is key. EU MS therefore cooperate to achieve fuel price stabilisation. A stable price

is not necessarily a low price, however, and the elimination of differences in taxation puts some of the newer MS at an economic disadvantage.

Subsidies on fuel are afforded to MS with lower levels of economic development. Indeed, this is an EU which relies on subsidies not only for price relief, but also for the implementation of planned energy transition. These subsidies enable, for example, MS with land to spare to become powerhouses for the production of biofuels, thereby boosting growth. From a social perspective, subsidies create new energy production and transition "hotspots" within the EU, which experience the social problems and volume crime associated with rapid urbanisation, and which act as a pull factor to migration – both licit and illegal – from outside. This inevitably puts added strain on law enforcement in these areas.

Subsidies incentivise energy efficiency, and demand and emissions reductions in MS, encouraging active participation in the EU. But where there are subsidies, there is subsidy fraud, and the potential for political corruption with the aim of rent-seeking. And since subsidies are necessary to the successful introduction of a range of green energy initiatives including renewable energy production, research and development (R&D), public transport and industrial Green Growth (e.g. LED production) there are a plethora of opportunities for OC in this arena.

A united EU negotiates with major oil and gas companies to ensure supply of hydrocarbons, impacting on bilateral agreements between MS and energy companies, companies' revenue from these and, ultimately, relations between the EU and major suppliers. Whilst the energy market within the EU continues to be liberalised, regulation is such as to discourage non-EU involvement.

Producing nations excluded from major deals with the EU start to engage with criminals in MS with a view to feeding illicit markets in the EU. By this token, state and non-state actors deemed unsuitable for partnership in licit energy supply have the opportunity to forge powerful networks of illicit suppliers. Some producing nations outside the EU are consequently in the process of transforming into rogue or pariah states, ultimately risking military intervention from consuming nations.

Standard fuel prices and tax levels across the EU shift OC focus from smuggling within the EU to smuggling to or from the EU. Policing the borders of the EU is therefore a high priority, with low levels of energy security making "leakage" particularly undesirable. By the same token, standardisation prompts the involvement of EU OC groups in illicit energy supply outside the EU, exploiting those areas where price and taxation differences persist. EU policing agencies therefore find themselves increasingly responsible for preventing and investigating energy-related crimes committed by their nationals overseas.

In line with a more planned response to the issue of energy security, there is some political will to drive forward climate change targets. Accordingly, there is greater regulation of carbon emissions, and more severe penalties are introduced for environmental crime – both of which have positive effects on the environment in the longer term. Policy rather than market forces stimulates expansion in the EU Emissions Trading System (ETS), providing further opportunities for Emissions Trading Fraud, whilst the burgeoning industry of Carbon Capture and Storage (CCS) attracts the attention not only of public subsidy fraudsters but also of those wishing to place criminal investments. Beyond 2020, advances in carbon transport enable those MS wishing to store large amounts of CO_2 to benefit from subsidies and growth opportunities, but also engender a situation in which a small number of states become "carbon

dumps" for the rest of the EU. Where OC is directly involved in CCS provision, its tendency to non-compliance raises legitimate concerns about public safety.

Measures taken to minimise price volatility also contribute to improving energy security, in time bringing the situation closer to the "ideal" scenario of low price volatility + high levels of energy security. In fulfilment of commitments to reduce emissions, renewable and nuclear energy solutions are developed at both MS and EU level. These require considerable amounts of investment over and above subsidisation which, along with investment in price-stabilised hydrocarbons and electricity, offer the prospect of sound returns in the longer term: with regard particularly to renewable technologies, as in "Market Forces" (Scenario I) OC's lower capital costs mean that it can step in to meet the shortfall in legitimate investment.

The overwhelming need for substantial investment in the energy sector to fund transition therefore supersedes the requirement for comprehensive legislation against money laundering and regulation of the origins of investments. Energy speculation, on the other hand, is increasingly the object of regulatory scrutiny, as MS and the EU seek to eliminate sources of price volatility: accordingly, energy investment is not so attractive to OC groups looking for quick returns, but rather benefits those who are willing to play the long game, or who are content merely to have successfully placed the proceeds of crime. As in "Open Season" (Scenario II), transition to renewables entails – at least in the short term – a level of EU dependence on countries with reserves of essential components such as rare metals, or those with more developed expertise in green technologies. As a result, the EU is a choice destination for the illicit trafficking of renewable components.

Price stabilisation contributes to the prevention of economic volatility in general, which helps to make life more predictable for end consumers. At the same time, energy consumption is subject to a number of controls, and measures are introduced which are designed to effect profound lifestyle change. Energy efficiency measures are welcome where they have the added benefit of reducing costs for consumers, e.g. in the use of energy efficient light bulbs, white goods and buildings insulation. But where the drive for energy efficiency is enforced by means of prohibitive legislation or pricing it is met with some resistance.

So, when smart electricity grids are introduced in order to charge consumers more for energy consumed at peak times, and MS governments introduce in-car meters and charges for car use, public feeling against "surveillance state" measures gathers strength and concerns are raised over perceived moves to calculate the worth of a human being by means of his carbon footprint. This manifests as civil unrest, and MS law enforcement agencies find themselves increasingly required to abstract resources from combating OC in order to police public disorder.

Some private citizens inevitably look to unorthodox and even illegal means to maintain their lifestyles: in this context black markets for both foreign goods and liquid fuels flourish. More specifically, there is a market for fuel stolen or diverted from authorised use by e.g. agriculture and the emergency services. This impacts on the effectiveness of these sectors – including the responsive capacity of law enforcement – and renders employees in these professions vulnerable to corruption. Looking ahead, increased fuel losses prompt an expansion of marking or dyeing, and higher penalties for diversion. Detection of diversion, however, remains a problem. By the same token, there is a market for devices which subvert demand limitation measures, such as smart energy meter or vehicle charge "scramblers".

In order to enforce demand limitation, energy efficiency and environmental protection, penalties are introduced or made more severe. Where a criminal offence is established (e.g. environmental crime) investigation and prosecution falls to law enforcement in MS and, if appropriate, at EU level: for civil or

administrative transgressions such as energy wastage or failure to meet green construction regulations, fines are imposed. Over time, however, the authorities come to deal with such a high volume of infringements that some MS establish law enforcement agencies dedicated to policing offences relating to energy production and consumption.

Those who accept the restrictions placed on their energy consumption inevitably experience lifestyle change. In the short-term at least, electricity, gas and petrol take larger shares of household and company budgets, encouraging reductions in consumption and an uptake of energy efficient technology. This manifests in small changes which impact on traditional perceptions of productivity e.g. prolonged travel times as a result of increased public transport use, a reduction in long distance travel for face-to-face business meetings. Facilitated by ever faster broadband internet connections – themselves increasingly energy efficient – individuals and commercial concerns exploit online and "virtual" presences to their full potential, until such time as research and development in aviation and automotive industries produce viable long-distance transport alternatives.

The more commerce is conducted online, the more data there is liable to compromise. Energy-related regulations therefore indirectly provide increased opportunities for internet facilitated organised criminality such as identity theft and – at a commercial level – cyber-espionage. The energy sector itself is vulnerable, e.g. to hacking into smart grids for the purposes of extortion or power diversion. Accordingly, the number of cybercrime investigations of this type is even higher than projected on the basis of technological developments alone.

Many OC groups experience the same constraints on mobility, etc. as other members of society: in this regard, policing them becomes more cost effective, as offline surveillance is replaced by online monitoring. Better resourced and better connected OC groups with ready access to illicit fuel supplies, however, have a commercial advantage in so far as they are able to travel comparatively unhindered and transport goods over long distances. In this regard they are able to provide services such as haulage which can no longer be fulfilled by legitimate business. In some MS, the impact of regulation is such that OC has more fuel at its disposal, and is therefore more mobile, than law enforcement.

Discussion and Conclusions

Ultimately, there is no "preferred" scenario for law enforcement – for instance, regulatory diversity within the EU leads to OC exploitation of national differences, whilst strong EU regulation prompts OC exploitation of external borders. Engagement in this exercise has, however, highlighted a number of different dynamics with the potential to affect interaction between Organised Crime and the energy sector at all levels, and the responses of EU law enforcement. It is now the intention to prepare for these by monitoring indicators of events described in the scenarios, and disseminating updates to law enforcement on their implications. More detailed discussion of the challenges and opportunities facing law enforcement remains classified. In demonstrating the value of scenarios to Europol, this exercise paves the way for further use of futures methods in the EU's fight against Organised Crime.

References

A select review of literature consulted during this exercise is available on request:
victoria.baines@europol.europa.eu

PREPARING TODAY'S AIRPORT SECURITY FOR FUTURE THREATS – A COMPREHENSIVE SCENARIO-BASED APPROACH[6]

Mara Cole & Andreas Kuhlmann
Bauhaus Luftfahrt, Economics and Transportation, Munich, Germany

ABSTRACT *– Airports, as part of the critical infrastructure of a country, have repeatedly been the target of terrorists' attacks. Security measures meant to render these threats harmless have mostly been introduced in response to specific occurrences, thus allowing the potential attackers to always remain one step ahead. As this approach seems inappropriate for dealing with future security threats, this paper provides a proactive approach to identify future threats and their coverage by airport security processes. To meet the requirements of a complex and critical system such as airport security a standard scenario process has been enhanced. This approach is presented in this paper.*

Introduction

Mobility, in particular air transport, is vital to the economic stability and growth of a nation. Air transport symbolises national self-confidence and self-conception, which made commercial aviation a preferred target for attacks of terrorists and other offenders. Airports are part of the critical infrastructure of a country and form the gateway for most terrorists' attacks on the air transport system. In the past political and related scientific approaches to cope with airport security matters were primarily reactive ones (Salter, 2008; Sweet, 2002). New security measures have regularly been introduced in a political ad-hoc process as a consequence of specific security incidents. The well coordinated terrorist attacks on September 11 are the most prominent example (ACRP Synthesis 3, 2007). The liquid ban after the transatlantic aircraft plot in 2006 is another example for this costly and often inefficient process of reactive action.

A precondition to overcome this reactive procedure would be to apply an anticipatory approach, which allows exploring the different characteristics of potential threats and to adapt the security processes accordingly. This would not only require an in-depth understanding of the many interlinked and complex airport processes, but also a systematic assessment of threat aspects or elements as well as a related analysis of possible and plausible future threats. Future research methods could in principle fill

[6] This article has been developed in course of the research project „SiVe", which is funded by the Federal Ministry for Education and Research as part of the German research program for civil security, which in turn is part of the high-tech-strategy of the Federal Government of Germany.

the methodological gap for this purpose. The use of the well established scenario technique can give new insights into possible future threat situations and thus is an important prerequisite for any assessment of current and future security measures.

The typical scenario building process is, however, insufficient for these purposes as it only results in a small amount of plausible future scenarios with a rather global focus (see next section). Furthermore, such an approach allows dealing with only a relatively small amount of elements in order to keep the process manageable. This is not appropriate for analysing a clearly defined system, which has to deal with a large variety of possible threats and whose processes are to be improved at a very detailed level. This scope requires an approach for the development of a very high number of standardised scenarios which show a detailed level of abstraction.

In this paper we propose a method, which allows generating the required large variety of consistent scenarios and analysing them in a systematic way. A matrix-based method adapted from system analysis and complexity management methods is applied in order to analyse the airport security system. The combinations of different threat aspects forming a valid threat scenario and their link to related security measures have been assessed and implemented in a matrix. Drawing upon such a database, structurally consistent scenarios can be produced in a standardised form. Analysing the resulting scenarios enables the user to better anticipate possible future threats, identify weak points in the security structures and thus to proactively improve the respective processes.

First, the standard scenario approach with its advantages and shortcomings in context of airport security will be described. Next the enhanced approach, which allows including a high level of detail and complexity of the respective system without compromising the manageability for decision makers, will be introduced. This includes system "capture", scenario building and related analyses. The last section concludes the results and provides an outlook for further research tasks.

The Standard Scenario Approach

In order to deal with prospective challenges in a proactive way, future research or foresight methods are increasingly gaining acceptance and relevance for companies and politics alike. The scenario process is one of the most prevalent techniques in the toolbox of future research methodology[7], which is justified by a variety of strengths of this method. Scenarios broaden the scope of a decision maker by providing a range of possible outcomes and insight into the underlying drivers of change. Furthermore they uncover already well developed trends or predetermined outcomes such as demographic developments and they help to avoid biased and lopsided group results by facilitating contrarian thinking. Godet described scenarios as useful in a fivefold way, as they "stimulate the imagination, reduce inconsistencies, create a common language, structure collective thought, and enable appropriation by decision makers" (Godet, 2000). However, scenarios are also prone for misinterpretation and abuse (Roxburgh, 2009). Some have described scenarios as counterproductive for developing a clear vision and therefore not suited for leadership tasks. Such a position neglects the fact that a goal can also be robust under several different sce-

[7] The Millennium Project of the American Council for the United Nations University has published the most comprehensive documentation of related methods (Glenn and Gordon, 2009).

narios. Decision makers, however, confronted with scenarios when they are actually searching for a one-dimensional vision or prognosis, therefore often choose one or two scenarios, which are closely related to their own image of reality. Ignoring the outer scenarios leaves leaders exposed to any kind of dramatic change. The potential of scenarios can therefore only be exploited if they are correctly applied and understood.

The procedure. In the 1970s scenarios entered the field of strategic planning, both in public and private sectors, with the methodologies developed and made popular by consultancy groups such as Battelle (Godet and Roubelat, 2000). The Battelle approach (e.g. Von Reibnitz et al., 1982) was structured in eight steps, where a problem specification (1) is followed by environmental screening (2) which then requires a specification of the relevant parameters and characteristics (3). This is followed by a clustering of assumptions (4), an interpretation of selected scenarios (5), an analysis of wild cards (6) and implications (7), which is then concluded by concrete action planning (8). 30 years later de Jouvenel (2000) provided a comprehensive review of scenario methods and described the prospective procedure in a similar way but condensed it to five basic steps: defining the problem and choosing the horizon (1); constructing the system and identifying key variables (2); gathering data and drafting of hypotheses (3); exploring possible futures, often with the help of tree structures (4); and outlining strategic choices (5). In the following these steps will be referred to as the standard scenario process. The system analysis (in step 2 and 3) also includes an assessment of the interrelations within the system, which is generally implemented by a cross-impact analysis (Gordon and Hayward, 1968). Apart from similarities in the different standard processes described above, it is obvious that every scenario generation process varies with the specific topical context, the experience and the tools of the respective moderator.

Characteristics of standard scenario problems. Before starting the scenario generation process the following question has to be asked in order to choose the appropriate methodological steps: For what purpose are scenarios generally well suited and what are the relevant features in the respective system or topical context? In cases of large uncertainty and thus numerous and quite different possibilities for future developments in the respective environment, scenarios cannot be built reliably at any level of detail. But even if this is not the case, it is problematic to structure “the unknown”. A reasonable and helpful way to approach this problem is to identify and describe the scenarios by means of a small amount of decisive variables. Scenarios can thus be characterized by the two most important driving forces, resulting in an illustration of scenario-axes (van’t Klooster and van Asselt, 2006) with the four quadrants representing four related scenarios. Such a structure, which allows making seemingly unrelated data operationally useful, proved to be quite valuable in environments, where few decisive variables characterise an economic sector or certain political developments sufficiently. However, even for issues where many variables are needed to describe the environment[8] the number of resulting scenarios rarely exceeds four. This is mainly due to simplicity reasons in order to avoid overwhelming the decision maker (de Jouvenel, 2000).

Airport security. In the context of airport security it is neither sufficient to use a small amount of descriptive variables, nor is a small number of scenarios adequate to cover the possible varieties of future

[8] The choice of used variables is mostly based on an uncertainty-impact-analysis, where a high value for both of these characteristics is required for including a variable in the further analysis.

threats. Here a clearly defined complex security system (characterized by a variety of utilized processes, technologies and involved actors) has to deal with a large variety of threat aspects and therefore many variables or critical uncertainties. An approach for dealing with airport security in a proactive way would therefore require a process, which includes advantages of scenario planning without compromising the specific requirements of the airport security system. Such requirements include the development of numerous standardised scenarios, which still offer a high level of abstraction. This is necessary as scenarios – in this context – serve to identify as much security threats as possible and not just an idea of the most plausible lines of development. These requirements are not in line with the standard scenario approach delineated above. The next chapter describes an approach, which allows to fulfil these requirements in a prospective and therefore proactive way and thus to overcome the shortcomings of standard scenario planning in the context of airport security.

The Enhanced Structural Complexity Scenario Approach

System coverage, data gathering and structuring

As mentioned above most scenario processes approach the topic in question in a structured way, following clear steps. The procedure may vary in detail from one scenario project to another but the basic steps mostly stay the same. This chapter will demonstrate how the adaptation of standard scenario methods helped to overcome the constraints faced when dealing with large, complex systems on a very detailed level. The procedure shall be demonstrated by drawing on examples from a scenario process conducted at Bauhaus Luftfahrt concerning airport security, which was performed by means of methods of structural complexity management, originating from product development methodology (Lindemann et al., 2009).

The first step of the standard scenario process (see previous chapter) is conducted to define the problem as well as to choose the horizon. Environmental scanning (Gordon and Glenn, 2009) can help to detect important influencing factors as well as to define the limits of the system in question. In the case described in this chapter expert discussions as well as literature reviews helped to identify potential influencing elements of the airport security system. During this process the borders of the system were clearly defined or, to put it in de Jouvenel's words, the horizon was chosen.

Once the system's borders were defined, the variables influencing airport security were compiled – a procedure corresponding to step two of the standard approach. To be able to analyse interdependencies within the airport security system from an integral point of view, security measures as well as elements of threat scenarios were gathered. To escape the danger of subjectivity, elements were collected by experts from different backgrounds and with different interests in the process. Structuring the collected elements was the next step in the conducted scenario process. The terms were clustered and structured hierarchically. In this first version 210 elements constituted the system on the lowest hierarchy level, structured by up to seven hierarchy levels and subsumed under 15 top level categories.

Following a standard scenario process the next step would have been to transfer the elements to a matrix to be able to carry out a cross-impact analysis of all gathered elements. By transferring the collected terms to a matrix the elements serve as row headings and as column headings – both in the same

order. Diagonal matrix cells thus represent self-reflexive dependencies. Since the system shows a very high level of detail this would have required specifying 44.100 relations (Figure 1).

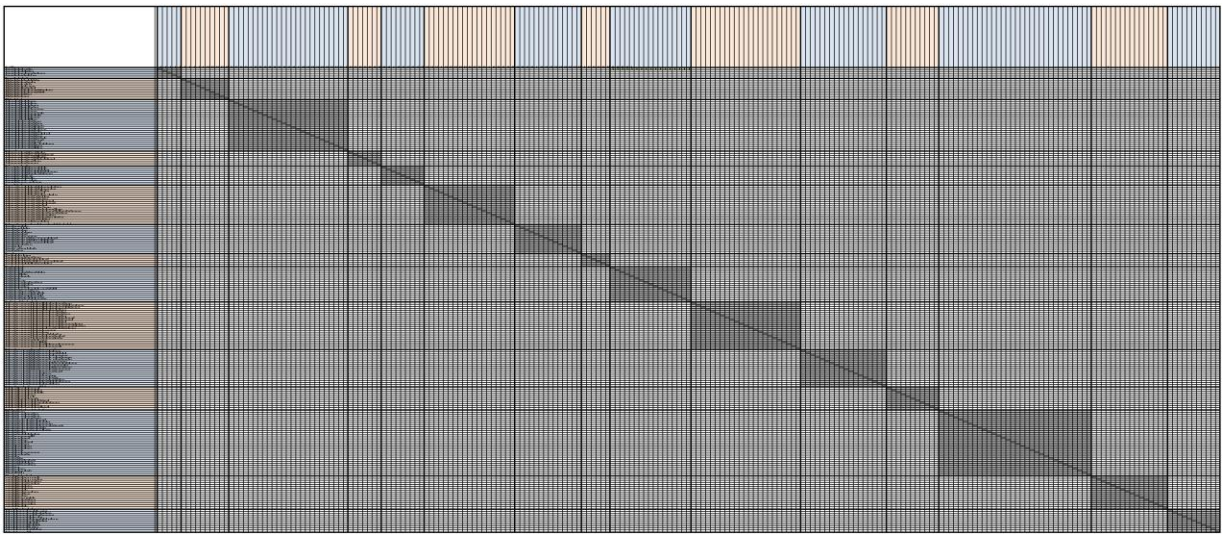


Figure 1. Multiple Domain Matrix on element level.

Since this is an impossible task concerning time resources[9] another way had to be found to approach the cross-impact analysis. At this point it was necessary to alter the standard scenario process and adapt the approach to the specific requirements of the airport security system. Thus an intermediate step was introduced to reduce the relations to the logically necessary connections: This is generally necessary if a system consists of too many single elements (and thus element interrelations) to be considered within a reasonable timeframe. To gain a more general impression of the system it is vital to change the level of abstraction. Up to this point the focus has been laid on the element level, the perspective is now broadened, focussing on the highest level (the "domain level") of the system. On this level of abstraction it can be verified which of the domains are directly linked to each other and which of them are not connected at all. The latter domain-pairs can later be excluded when performing a cross-impact analysis on the element level. This interim step reduces the considered element connection significantly to a feasible amount.

After identifying the domain-linkages, the direction and specific quality of each relation was discussed and named. With the help of a flowchart these connections were illustrated (see Figure 2). The arrows in Figure 2 represent the direction as well as the quality of a relation between two domains (e.g. "Potential Offender" *has* "Intention"; "Tool/Weapon" *is suitable for* "Target").

[9] If seven experts would have discussed each element-pair for only one minute this would have resulted in approximately 650 person days of work.

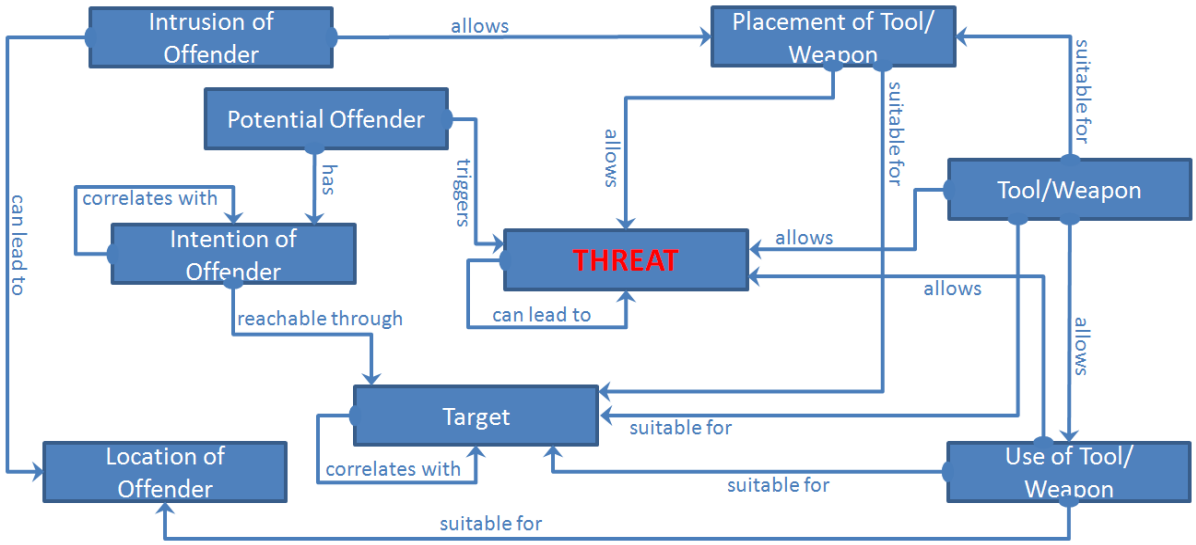


Figure 2. Detail of flowchart (showing 9 out of 15 domains).

After both the quality of the logically necessary interrelations and their direction of influence are specified, domains can be transferred back to a matrix design. Figure 3 shows the result for those domains of airport security, which are relevant in the context of this paper. Each filled matrix cell represents an arrow from the flow chart und thus the connection of one domain to another. In the matrix cells each type of connection is specified. Just as in the element matrix (Figure 1), the domains in the rows influence the domains in the column heading. This representation method makes it possible to document the direction as well as the specific kind of relation in a very clear way and thus allows for an intuitive access to the data. The presented section of this domain matrix can be subdivided into two major areas: the red represents the elements necessary to form a valid threat scenario and the blue represents the preventive and reactive (i.e. emergency) countermeasures an airport can apply.

	Potential Offender	Intention of Offender	Tool/ Weapon	Use of Tool / Weapon	Approach of Offender	Insertion of Tool	Target	Location of Offender	Threat	Security Measure (Preventive)	Security Measure (Emergency)
Potential Offender		has							triggers		
Intention of Offender		correlates with					reachable through				
Tool/ Weapon				allows		suitable for	suitable for		allows		
Use of Tool/ Weapon							suitable for	suitable for	allows		causes
Approach of Offender						suitable for		can lead to	allows		
Insertion of Tool							suitable for		allows	is influenced by	causes
Target							correlates with				causes
Location of Offender											renders possible/ inhibits
Threat									can lead to		demands
Security Measure (Preventive)			counteracts		counteracts	counteracts	influences	complicates access			
Security Measure (Emergency)		influences									demands

Figure 3. Detail of matrix on domain level (showing 11 out of 15 domains).

After the domain's relations have been reduced to the logically necessary ones, the standard scenario process can be picked up again. According to de Jouvenel (2000) a cross-impact matrix is often employed at this stage to analyse the relations between elements. It is typically used as "a schema for collating and systemizing [...] expert judgments, so as to make it possible to construct a conceptual substitute, however imperfect, for a whished-for but nonexistent theory of how events affect each one another in a multidisciplinary context." (Helmer, 1981). At this point the level of abstraction has to be changed back to the lowest hierarchy level of the system, the element level. Each matrix cell in the domain level represents a sub-matrix on the element level. For the following cross-impact analysis only those element relations are considered that belong to a domain interrelation that is marked as logically necessary in the domain matrix.

To ensure a certain level of quality and to overcome the impending subjectivity the determination of the connections has to be carried out by a certain number of researchers with different scientific backgrounds. In most cases binary decision (indicated by 0 and 1) sufficed to document the relationship of two elements. In some cases a more detailed differentiation was necessary and the relation was specified by a weighted value (+2, +1, 0, -1, -2), indicating positive or negative influences. For example a terrorist could have the intention to cause commercial damage, a high loss of human lives and thus demoralize the population. He could do this by attempting to smuggle explosives or a knife through the hand luggage check. This is the point where the airport can render the whole threat scenario harmless. Security measures always address single aspects of threat scenarios and never the scenario as a whole. By detecting elements of the scenario one hopes to render the whole potential threat unsuccessful. If, for example, the explosives are detected during the hand luggage check the whole scenario falls apart because the offender cannot complete the scenario without a weapon.

In a standard scenario process the next step would be to collect data concerning the past, present and possible future development of the considered variables. As a consequence of the very high level of abstraction of the considered airport security system the elements themselves are not subject to development. It is their interaction within the system that lets the system as a whole evolve. Thus the complexity and high detail does not allow for approaching the compilation of scenarios with the help of plausible projections. Consequently, another way has to be found to extract the information gathered during the cross-impact analysis to generate consistent scenarios. This process, which is completely beyond the scope of the standard scenario process, will be described in the following section.

The Scenario Building Process

The specified connections in the scenario-part of the matrix (illustrated by the red area in Figure 3) build the base for generating structurally consistent and thus plausible scenarios. Assuming that the matrix comprises all possible threat elements and correct interconnections between them, one could theoretically claim that all possible threat scenarios are covered by this approach. All different shapes a scenario can assume are documented through different combinations of the interlinked elements. The elements of a historic or fictive threat scenario then can be traced within the detailed system matrix (see Figure 1). Two results arise from mapping scenarios on to the documented structure: By mapping historic scenarios the quality of the documented system can be scrutinized and by mapping fictive scenarios on to the matrix the plausibility of the scenario itself can be validated regarding its structural consistency.

To verify the consistency of fictive scenarios one has to take a close look at the system on element level and check the interlinkage of the different element pairs one by one. Since the system does not only consist of threat scenario elements but also includes security measures, the relation between the scenario and potentially effective counter-measures can be traced. Again the connection of each element of the threat scenario to each element of the security measures has to be assessed. Because of the high structural complexity it is very time consuming to trace each connection. To make the system more easily accessible and to overcome these problems, the domains of the system were connected via an underlying process logic derived from the partitioning process and connected by the Boolean algebra operators AND and OR. This logic was applied to the whole dataset (the single matrix elements) in a tool based on MS Excel called “scenario builder”.

The “scenario builder” helps to compile threat scenarios and offers a clear representation of the scenario-specific countermeasures. It allows generating (threat) scenarios by successively choosing consistent elements from different domains until a scenario is completed. The sequence is based on the underlying logic (starting with the “potential offender”, as illustrated in Figure 2) and every successive choice or step only allows choosing from a reduced selection of elements in the next domain, according to the logical link from the previous choice. The scenario builder thereby guides the user through the process of compiling elements to form a consistent scenario. Besides creating scenarios in a very time-efficient way, this approach has the advantage of also producing scenarios that might seem to make no sense from a rational point of view but that are at the same time structurally consistent – e.g. scenarios a mentally disabled person might pursue. After the scenario is compiled, the scenario builder automatically lists the security measures that are connected to the elements of the scenario. This helps to evaluate

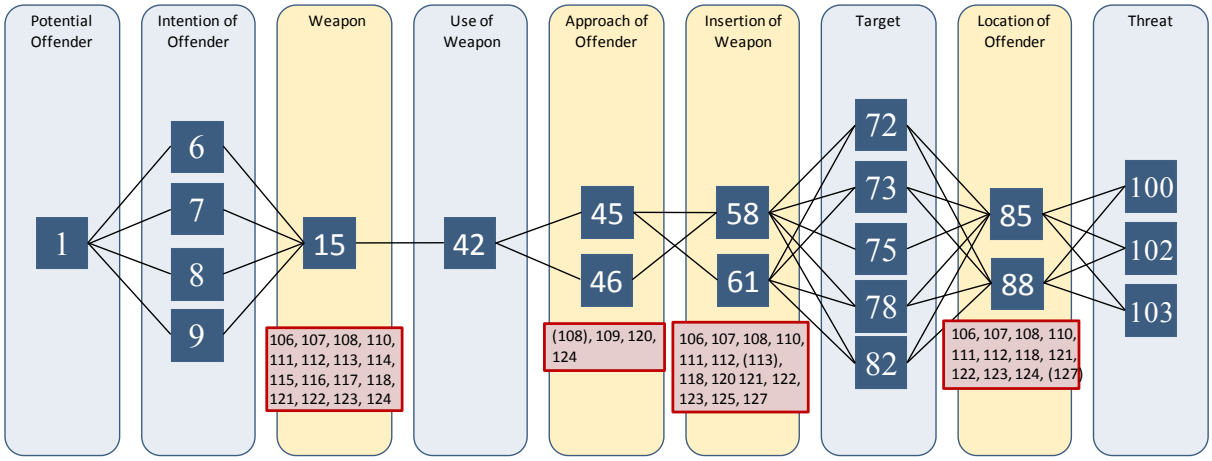
the effectiveness of existing security measures because the scenario and the related measures are directly opposed.

The System Analysis

The content of the matrix allows analysing many structural aspects of the security system and their relation to specific threat elements. One possibility is to analyse the risk coverage by preventive security measures (Cole et al., 2009) but single threat aspects or elements are not the relevant perspective, as their combination (or the scenario) creates the valid threat. The scenario builder renders the broad space of all structurally consistent scenarios accessible in a rather intuitive way. To gather a certain amount of scenarios in order to analyse them, for example with respect to the related security measures, is still a time-consuming activity. The scenario building process has been automatised in order to be sure to base the evaluation of the function of the security measures in relation to different scenarios on a broad data base. Through the automatic analysis the span of the space of all structurally consistent scenarios can be fully exploited. The first analysis of the airport security system, which had to run under certain restrictions[10] in order to match the available calculating capacity, resulted in more than 220.000 scenarios. With this large (and theoretically complete) set of scenarios it is possible to analyse structurally weak points in the airport security system. For this purpose the scenarios can be sorted by the number of related security measures, which are potentially addressing the respective threat elements. By clustering similar scenarios, where in principle only a small amount of countermeasures are able to address the threat, one can identify threats which are dangerous from a structural point of view.[11] Thus, focusing on the system itself, one can identify points in the system, which are so far insufficiently protected or where processes can at least be ameliorated in order to address more threat aspects.

Figure 4 illustrates how the different parts of (standard) threat scenarios can be opposed to relevant counter-measures and consequently be visualized. This example shows a cluster of similar scenarios, where a suicide bomber tries to smuggle explosives into the security zone of an airport to reach a specific target. The columns depict the nine domains of the threat scenarios. The numbers in the blue squares represent the scenario elements, while the ones in the red boxes indicate the elements of preventive counter-measures, which are part of the airport security system. When the terrorist tries to conceal the weapon on his body (item 58), the most relevant counter-measure is the passenger control (item 111), while concealing in the hand luggage (item 61) is, amongst others, addressed by the hand luggage check (item 113).

[10] These restrictions included the limitation to one threat element per domain, which significantly reduced the possible combinations and therefore number of threat scenarios.
[11] At this point in the analysis we neglect the differences in actual effectiveness of security measures, the focus here is on structural links between threat elements and security measures.



1: Terrorist, 6: Economical damage, 7: Human lifes, 8: Attention, 9: Fear, Demoralization, 15: Explosives, 42: Manually – calculating own death, 45: Street, 46: Rail, 58: Concealing weapon on body, 61: Concealing weapon in hand luggage, 72: Aircraft flying, 73: Aircraft at ground level, 75: Fuel depot, 78: Restricted area, 82: People, 85: On-board, 88: Restricted area, 100: Hijacking, 102: Sabotage, 103: Renegade

Figure 4. Threat scenario cluster with respective security measures.

Similar analyses can identify where redundancies in the system are very large, which might indicate a bad cost-benefit performance.

Discussion and Outlook

In the past new airport security measures have regularly been introduced in political ad-hoc processes, often as a consequence of specific security occurrences. A precondition to overcome this reactive procedure would be to apply an anticipatory approach. Scenario planning methods could in principle be applied to address this problem. However, the typical scenario building process is insufficient for this purpose since a large database of plausible scenarios is needed to be able to systematically improve the airport security system. Thus an approach merging elements from standard scenario process, system analysis and matrix-based complexity management has been developed and are described in this paper.

This approach allows combining the advantages of a prospective foresight method, which is generally vague in terms of tangible developments in specific sub-systems, with the accuracy of an in-depth system analysis of airport security. Two adaptions of the standard scenario process are central: first, the logical reduction of possible links between elements for the cross-impact analysis, which is necessary to handle large complex systems. The second major extension is the introduction of the “scenario builder”, allowing for a time-efficient analysis of the complex data. This kind of extended scenario analysis allows demonstrating effects of a specific scenario on other affected stakeholder or systems (in this case on airport security). This automatised approach is valuable, when a large variety of scenarios has to be analysed. This in turn allows to better optimise the system in concern because the interrelations are documented and thus evaluable, for example concerning structurally weak points in the system. Further analysis of the documented database still remains to be done. Consequently, as a central result of the project, implications for a proactive structure of airport security measures and processes will be derived.

For a general overview on the complete airport security analysis of the whole “SiVe” project, which includes simulations as well as cost-benefit-analyses, see Breiing et al. (2010). A more specific descrip-

tion of how the scenario builder is interconnected with simulation and risk quantification modules and how aggregated risk values are derived is given by Maurer et al. (2010).

References

ACRP Synthesis 3 (2007) *General Aviation Safety and Security Practices*. FAA.

Breiing, Marcus – Cole, Mara – d'Avanzo, John – Geiger, Gebhard – Goldner, Sascha – Kuhlmann, Andreas – Lorenz, Claudia – Papproth, Alf – Petzel, Erhard – Schwetje, Oliver (2010) Optimisation of Critical Infrastructure Protection: The SiVe Project on Airport Security, *Lecture Notes in Computer Science,* Vol. 6027, 73-84, Springer.

Cole, Mara – Kuhlmann, Andreas – Schwetje, Oliver (2009) *Aviation Security –*

A Structural Complexity Management Approach, 13th Air Transport Research Society World Conference 2009, Paper No. 96.

de Jouvenel, Hugues (2000) A Brief Methodological Guide to Scenario Building, *Technological Forecasting and Social Change*, Vol. 65(1), 37-48.

Glenn, Jerome C. – Gordon, Theodore J. (eds.) (2009) *Futures Research Methodology*. Version 3.0. UNU Millenium Project.

Godet, Michel (2000) The Art of Scenarios and Strategic Planning: Tools and Pitfalls, *Technological Forecasting and Social Change*, Vol. 65 (1), 3-22.

Godet, Michel – Roubelat, Fabrice (2000) Scenario Planning: An Open Future, *Technological Forecasting and Social Change*, Vol. 65(1), 1-2.

Gordon, Theodore J. – Glenn, Jerome C. (2009) Environmental Scanning. Futures Research Methodology. Version 3.0. UNU Millenium Project.

Gordon, Theodore J. – Hayward, H. (1968) Initial Experiments with the Cross-Impact Matrix Method of Forecasting, Futures, Vol. 1(2), 100-116.

Helmer, Olaf (1981) Reassessment of Cross-Impact Analysis, *Futures*, Vol. 13(3), 389-400.

Lindemann, Udo – Maurer, Maik – Braun, Thomas (2009) *Structural Complexity Management*. Springer.

Maurer, Maik – Cole, Mara – d'Avanzo, John – Dickmanns, Dirk (2010) *Airport Security: From Single Threat Aspects to Valid Scenarios and Risk Assessment*, American Journal of Engineering and Applied Sciences, in press.

Roxburgh, Charles (2009) The Use and Abuse of Scenarios, *McKinsey Quarterly*, November 2009.

Salter, Mark B. (eds.) (2008*) Politics at the Airport*. University of Minnesota Press.

Sweet, Kathleen M. (2002) *Terrorism and Airport Security*. Edwin Mellen Press Ltd.

van't Klooster, Susan – van Asselt, Marjolein B.A. (2006) Practising the Scenario-Axes Technique, *Futures*, Vol. 38(1), 15-30.

Von Reibnitz, Ute – Seibert, Siegfried – Geschka, Horst (1982) *Die Szenario-Technik als Grundlage von Planungen*. Battelle-Institut.

COMBAT SIMULATION AS TOOL FOR EVALUATION OF FUTURE WEAPON SYSTEMS AND SOME RISKS IN SCENARIO BASED WARGAMING

Esa Lappi & Bernt Åkesson
Finnish Defence Forces Technical Research Centre, Electronics and Information Technology Division

ABSTRACT *– In the Finnish Defence Forces Technical Research Centre (PVTT) combat simulation models are used in order to choose optimal combinations of weapons. In the defence analysis different tools are used. In this paper we describe the methods and tools used in the military analysis and discuss the sources of errors in the future weapon evaluation and estimation process on technical, tactical and operational levels.*

In military analysis the scope of the simulations vary from platform level technical analysis to tactical and operational questions. The technical level analysis is basic science and engineering, for example calculating probabilities of detection of targets in different weather conditions using different sensor systems. In the analysis we can predict the trend of the technological improvements and also explore physical limits of system of interests. The technical and small scale combat analysis can fail, however, if completely new technology is invented in the near future.

Operational planning and brigade level analysis pose a more challenging problem. The operational level analysis is based on scenarios, which are simulated using computational combat models. These are often man-in-the-loop simulations, which are based on the tactical and technical models, and where the wargaming is based on predictions of future warfare and a vision of how the forces will be used. A worst case situation in operational level wargaming is using the wrong assumptions when predicting the concept for the use of forces. A completely new doctrine may emerge for the forces and their use, in which case defence forces have been optimised for the wrong type of war.

Introduction and Background

The time span of defence planning is decades. This means that defence planning includes assumptions about the future and acquired systems are intended to be used for several decades. Therefore, in acquisitions it is important to evaluate the capabilities of current and future systems with regards to future threats. In this work the applicability of Finnish computation and simulation methods to weapons procurements, motivated by potential battles 10-15 years in the future, is evaluated. In addition, the research process itself is studied and its functionality is evaluated.

Currently the basis for the analysis are scenarios derived from the threat models (Facts about National Defence 2008), in which Finland is subject to an armed attack and is forced to use military power. These scenarios are restricted, but in this paper only the research process and simulation tools are studied.

Since the life span of the systems used by all parties is measured in decades, we assume the newest systems, which are currently in use and under procurement, to still be in use in 15 years. This means that a large number of the systems are known, but they can still have been upgraded e.g. by installing better communication equipment, fire control systems or using more powerful ammunition. In addition to these known weapon systems, some completely some new weapons or weapon systems could have been developed by the year 2025 through technology and new innovations. Furthermore, the use of current systems and capabilities could have been changed on either tactical or operational level.

In the study of the use of weapon systems, the basis is formed by an assumption about the situations where the systems are used. Thus, the research depends on the scenarios derived from the threat models. Simulation software tools, which estimate the outcome of battles, are used to support the estimation of how the scenarios unfold. In this paper the simulation methods and their application, which support decisions concerning the defence solution of the future, are described. The usefulness of the assessment methods is discussed by making a brief comparison based on historical events as to how the methods would have worked in light of the events during May 1940.

Material and Methods

In Finland the development of future technologies and its effect on the outcome of battles is estimated by producing an Estimation and prognosis of military technology (Estimation and prognosis of military technology 2025, parts 1 and 2 2008), which contains descriptions of all fields of military technology and a prognosis of technological development. This provides the foundation for assessing developing technologies in the defence forces, although naturally other sources are used as well to support the analysis.

Aside from the survey of technological alternatives is the military political analysis of Finland's surroundings which is left out of the technical analysis. The technical and tactical analysis starts with a crude assumption of the military threat to Finland, based on the threat models (pressure, attack), and of the different alternatives. (Facts about national defence 2008)

The different threat models and the series of events related to them result in scenarios, which can be analysed using computer simulation. These national level scenarios are further refined into smaller scenarios and even further into combat technical level evaluations. The practical simulation starts at the combat technical level, where the capabilities of different systems are evaluated in different situations. In this study the combat technical and tactical level simulation models are described. The results from the higher resolution models provide input to the lower resolution/large scale model.

Wargames and simulations are used when developing Army tactics. Major General Arto Räty presented a chart of the development process in a recent article (Räty 2009), shown in Figure 1.

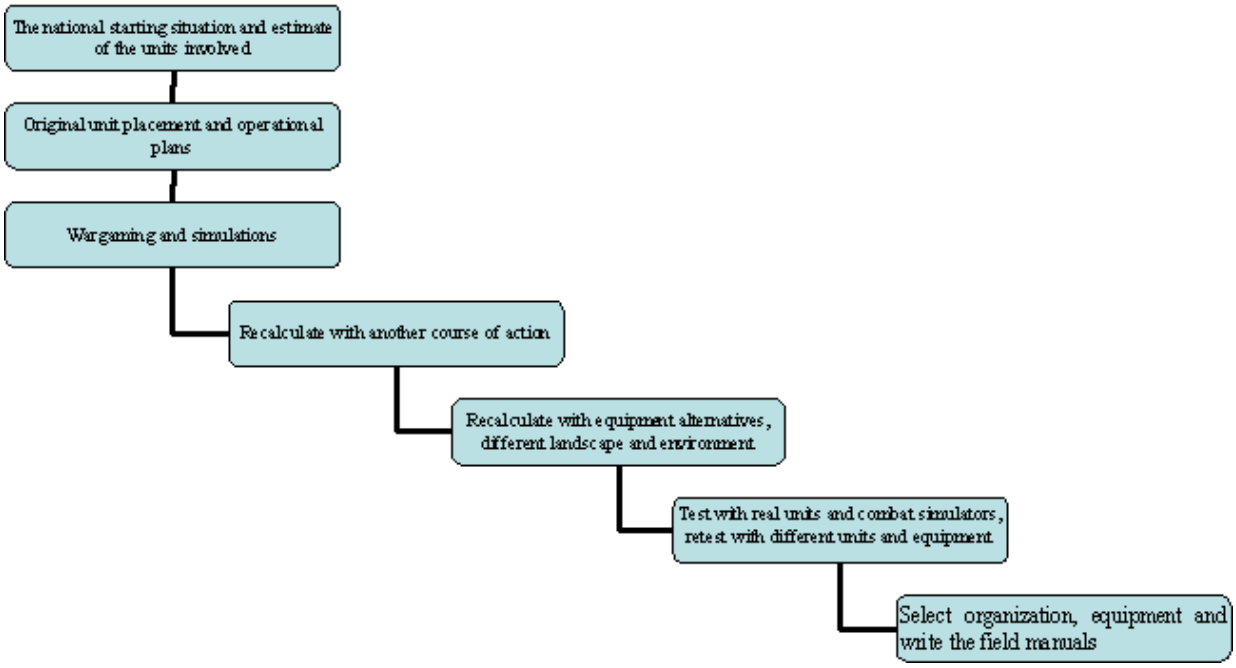


Figure 1. *Wargames and simulations are a part of the process when developing the tactics, organizations and equipment of new Army troops. The results that are obtained are verified by exercises (Räty 2009).*

A suitable simulation software tool for the combat technical level is e.g. FLAMES (Ternion Corporation 2010). It can be used to examine situations within a company, comparing tactical alternatives or changes at the platform level, e.g. how a better or more accurate gun changes the situation. After the results have been obtained by FLAMES, they can be transferred to brigade level analysis tools, such as Sandis (Lappi 2008). This multi-level simulation process is, however, very labour intensive.

FLAMES (FLexible Analysis, Modeling, and Exercise System) is a commercial OA-tool, which is used for comparative analysis on system and platoon-battalion level. The software is based on component-based physical and mathematical system and action models. FLAMES can be used to automatically analyse the effect of different system, parameter and tactical alternatives through high-resolution simulation, where units are modelled on platform level (individual tanks, aircraft etc). Because of its generality the software is suitable for Army, Navy and Air Force simulations.

The inputs are:

- system parameters
- troops and their equipment
- action logic (tactics) for the units
- unit actions (routes and missions) in the scenario
- digital map material (ESRI/DTED).

FLAMES produces, among others, the following output:

- casualty distributions for different unit and weapon types
- distributions of units destroyed by different weapons

- 2D and 3D visualization of the simulation
- other interesting information, such as average detection or firing distance.

Sandis is a combat modelling tool based on probability calculus and fault logic analysis. It is developed by PVTT and it is used for comparative analysis of cost effectiveness and tactical alternatives on platoon-brigade level.

The inputs of the tool are:

- weapon and communication characteristics
- units and their equipment
- fault logic for the units and operation success
- map
- user actions for the units at company or platoon level.

As output, Sandis gives, as functions of time,

- operation success probability
- probability of each unit being beaten
- unit strength distributions
- killer-victim scoreboard
- ammunition consumption
- radio network availability
- medical evacuation logistics and treatment capacity analysis.

The use of simulation systems is time consuming, so the simulations are focused on the most important cases. Figure 2 shows an estimate of the time needed for Sandis simulations as a function of scenario size. The other simulation models and methods are also needed for the analysis.

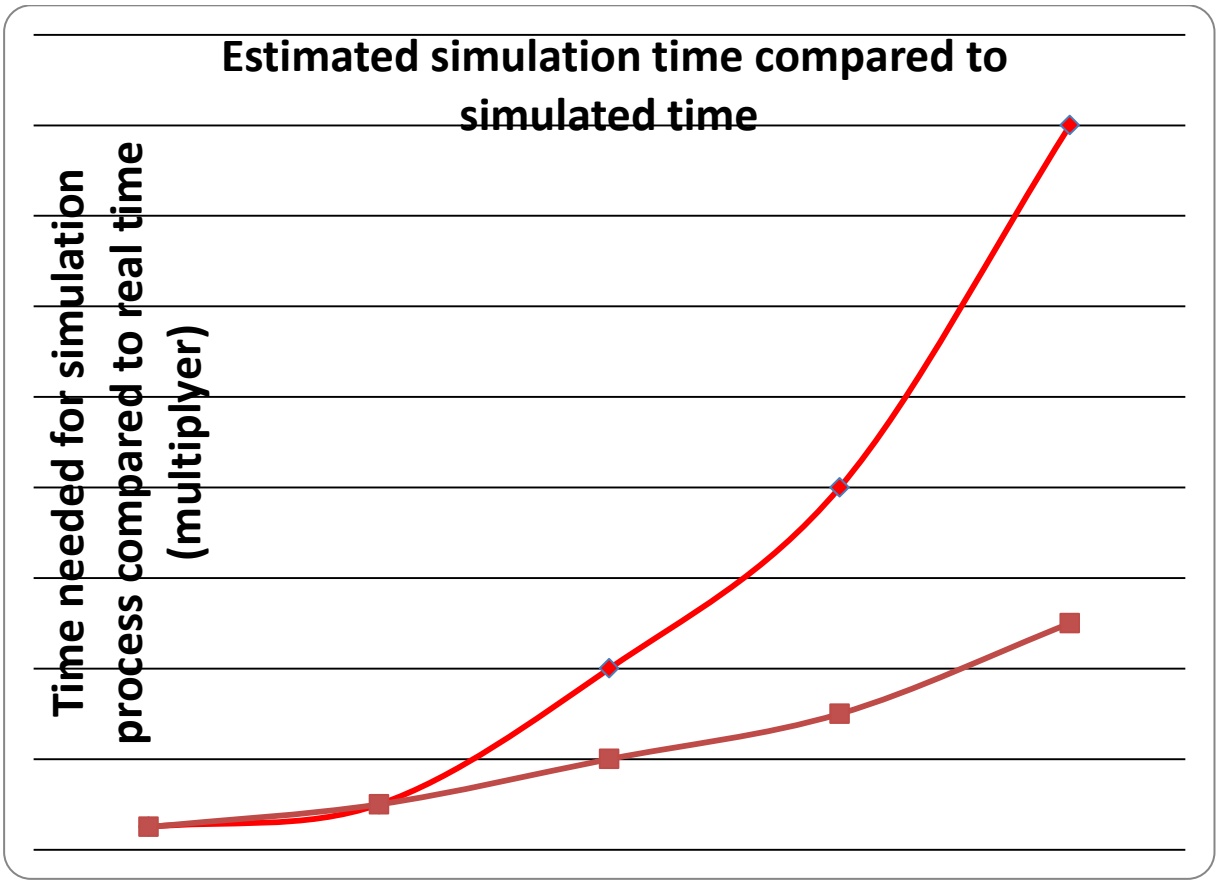


Figure 2. *The time needed for the simulation process as a function of the scenario size. The scale on the horizontal axis represents the approximate size of the scenario. Dots start from platoon level and end with brigade level. The upper line represents the first simulation and the lower a variation of it. For example, a brigade level battle lasting a week requires 4 man-weeks of work for the first simulation and then a man-week for each variation.*

Results

The suitability of the presented method is discussed through a historical example: How would this method have worked in France in May 1940. However, this is not a study in military history, but an example to emphasise how the method can be applied. In this study several possible reasons for the outcome of the battle are considered, as described by the contemporary Tapio Hiisivaara in his book "Saksan voitto lännessä 1940" ("Germany's victory in the west 1940"), published in 1941 (Hiisivaara 1941). This example is chosen because it contains different types of combat and the surprise caused by a new type of warfare.

In the work by Hiisivaara the main points of the German attack are noted to be, among others, the significance of manoeuvre warfare and activeness, that are closely associated with the use of air support to ground forces, armoured and light units and the concentration of armoured forces at a very narrow break point, emphasis on deep penetrations, use of paratroopers, direct fire using artillery and the use of anti-aircraft guns for antitank defence and destroying nests (Hiisivaara 1941, 258-260). Combined arms

warfare is also emphasized (Hiisivaara 1941, 266). The command and control (C2) systems required for combined arms warfare are described in (Hiisivaara 1941, 129).

These factors can be analysed with the available simulation software. In FLAMES duels between individual tanks and tank companies can be played as well as duels between antitank weapons and armoured units. These analyses would have showed that the rate of fire, the ability to fire at moving targets and the hit probability of weapons are significant for the outcome of the battle. This information could have directed the effort towards acquisition of systems that would have been more effective for the battlefield and towards noticing essential factors. The technology for firing at moving targets was already available in anti-aircraft defence and during the war the Germans used 88 mm anti-aircraft guns for antitank defence. The quality and need for such weapons or similar ones would have been discovered in wargames played using simulation tools.

In Sandis it is possible to evaluate the state of communications and their significance for warfare. That way the importance of more powerful radios and C2 systems could have been evaluated through simulation, although partly as a man-in-the-loop simulation. A typical situation is depicted in Figure 3. In a wargame only units with some form of communication between them are able provide fire support to each other. The concentration of armoured units and its effect on the situation would have been possible with Sandis, if the tank duels and the duels between tanks and antitank weapons had first been analysed in FLAMES and the results transferred to Sandis. This way the comparison of concentrated and dispersed use of tanks would have been possible.

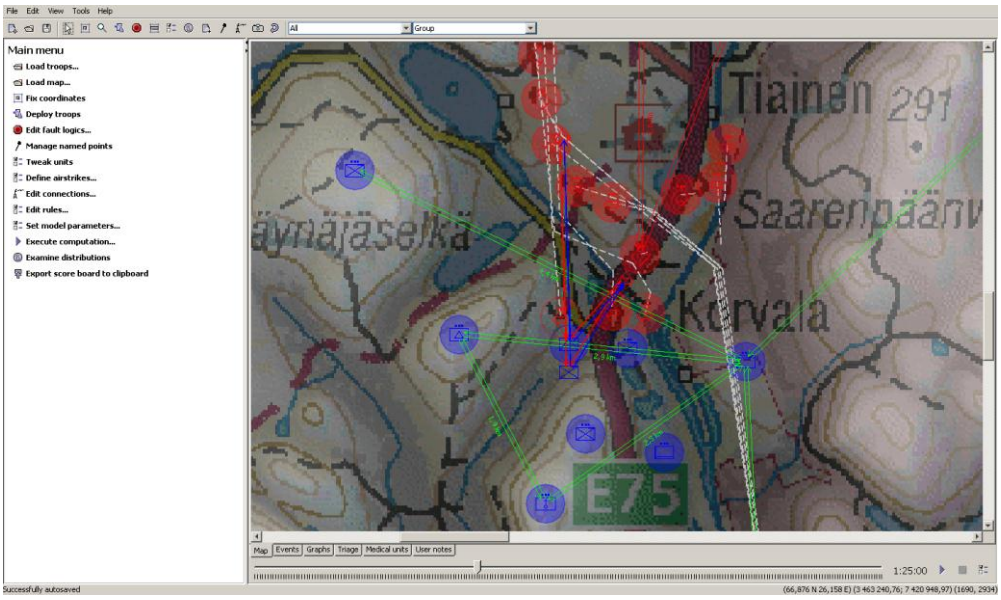


Figure 3. A close-up from a battalion-level scenario in Sandis. The red and blue circles represent platoons. The green lines represent functioning radio links.

The movement of civilians and their casualties in the warzone could have been included in Sandis, but the actions of civilians are based on assumptions made by the user and as such would only serve as bookkeeping based on an enlightened guess. Even then moving civilians would be visible on the map in urban areas and on roads, and it would be possible to take into account their effect on warfare, provided that the estimate of their behavior is in the right ballpark.

The panic of troops and civilians and the use of psychological weapons are completely left out of the analysis. There are no computational models for describing their effects, although troops and civilians can be moved on the map.

There are several ways of modelling air combat, but air combat simulators are not studied any further in the scope of this paper, although FLAMES would be suitable for this type of studies. The effect of aerial bombardment on different targets can be studied using both Sandis and FLAMES. However, duels between an individual target (tank) and an aircraft can only be solved using FLAMES. On the other hand, the average effect of an air strike to units of platoon size or larger could also be examined using Sandis.

It is especially worth noting that only if the possibility of enemy armoured forces had been considered in the beginning of the development process, would such a large force be included in the wargame and as an optimization alternative for the systems. Simulation of an armoured division would have proceeded in two phases: details using FLAMES and the whole using Sandis. Thus, simulation of concentrated forces and dispersed tanks would have required a significant amount of personnel resources. When allocating the limited simulation resources such an alternative could still have been left out.

As a result, we notice that simulation tools would have shown the effectiveness of antitank troops and the technical execution of the plans on a rough level. The Germans could have tested their blitzkrieg-concept and assured themselves of its effectiveness, whereas the French would not necessarily have played any game containing operational level German armoured forces. If such a scenario had been played, the strategic level surprise in May 1940 could have been avoided.

Discussion and Conclusions

The example discussed shows that computational methods could have exposed some unexpected issues about the battles of May 1940, so the approach following the current development cycle seems largely like a workable development method for the military.

The deficiencies are also significant. The computational models would not have predicted panic, although they could have been used to estimate the civilian movement on the roads and thereby estimate the slowdown of movement.

The biggest risk lies in that so-called Red teaming (Chua, Choo, Sim & Tay 2008; Lauren, Silwood, Chong, Low, McDonald, Rayburg, Yildiz, Pickl & Sanchez 2009) is not considered or the amount of tactical and operational alternatives is too small. If in the Red alternatives significant modes of operation have been ignored, the simulation and optimization process can still lead to optimization of the defence system for the wrong type of threat and mode of operation.

Finally, it should be noted that the simulation process described in this paper is labour intensive and the analysis in the example would have required several man-years of work, if multiple German attack alternatives had been played against multiple French defence alternatives.

References

Chua, C.L. – Choo, C.S. – Sim, W.C. – Tay, Victor (2008) Automated red teaming: an objective-based data farming approach for red teaming. *Proceedings of the 2008 Winter Simulation Conference S. J. Mason, R. R. Hill, L. Mönch, O. Rose, T. Jefferson, J. W. Fowler (eds.),* 1456-1462.

Hiisivaara, Tapio (1941) *Saksan voitto lännessä 1940 (Germany's victory in the west 1940)*. WSOY.

Kari, M. – Hakala, A. – Pääkkönen, E. – Pitkänen, M. (eds.) (2008) *Sotatekninen arvio ja ennuste 2025, osa 1: Teknologian kehitys (Estimation and prognosis of military technology 2025, part 1: Technological advancement)*. Publications 14. Finnish Defence Forces Technical Research Centre.

Kari, M. – Hakala, A. – Pääkkönen, E. – Pitkänen, M. (eds.) (2008) *Sotatekninen arvio ja ennuste 2025, osa 2: Puolustusjärjestelmien kehitys (Estimation and prognosis of military technology 2025, part 2: Development of defence systems)*. Publications 15. Finnish Defence Forces Technical Research Centre.

Lappi, Esa (2008) Sandis Military operation analysis tool. 2nd Nordic Military Analysis Symposium, Stockholm.

Lauren, M. – Silwood, N. – Chong, N.E. – Low, S. – McDonald, M. – Rayburg, C. – Yildiz, B. – Pickl, S. – Sanchez, R. (2009) Maritime force protection study using MANA and Automatic Co-Evolution (ACE). *Scythe: Proceedings and Bulletin of the International Data Farming Community*, Issue 6, 2-6.

Public Information Division of Defence Command Finland (2008) Facts about National Defence.

Räty, Arto (2009) Maavoimat kohti 2020-lukua (The Army towards the 2020s). *Sotilasaikakausilehti,* Issue 6-7, 9-15.

Ternion Corporation (2010) FLAMES. http://www.ternion.com.

EDUCATING SOLDIERS AND SECURITY SECTOR ACTORS FOR HUMAN SECURITY ORIENTED ACTIVITIES

Juha Mäkinen
Department of Leadership and Military Pedagogy, National Defence University of Finland

ABSTRACT – *A new kind of soldiership, akin to the security sector actorship, is emerging in the national security sector in Finland. An efficient and good national security sector should have some shared aspects like for example some ends and objects of the activities but also some mediating means. The analysis done in the paper shows how human security -oriented activities are mediated in Finland at the moment for example by such concepts as human security and action competence. These concepts are operational for the 21st century education of soldiers and civilians facing new kinds of global threats collectively.*

Introduction and background

In the Nordic countries, soldiership has got a new flavour in our 'postmodern' times (Moskos et al. 2000), with primacy given to international missions (Stoltenberg 2009; Bailes et al. 2006) instead of old-fashioned territorial defence and some comprehensive internal security activities. By comprehensiveness, I mean that both civilian and military resources and personnel are needed for internal security activities, as the duties of the Finnish Defence Forces also highlight at the moment (Finnish Parliament 2007). At least in Finland we should keep our soldiers also nationally oriented, being able to think by themselves while keeping in mind fundamental questions, such as how to maintain one's ethical consistency and to be an ethical subject by justifying killing and respecting human dignity and human security at the same time.

It follows that instead of just being 'hired guns' and 'traditional warriors', the (Finnish) soldiers are national security actors[12] in our forthcoming comprehensive national security age. Both soldiership and the emerging security actorship have to be reinterpreted when more justifiable ethical-moral grounds for the activities of the comprehensive national security sector have to be established.

The soldiers are in the security business and are acting on a broad field of the security sector that has been under a global transformation process (i.e. Security Sector Reform, SSR). Security, and more specifically human security, is a widely shared interest, and soldiers are actively seeking new kinds of means

[12] A new, more comprehensive national security strategy is needed for national (strategic) security actors, replacing the strategies/policies of security and defence policy, the strategy for securing the functions vital to society, and also the internal security programme.

and ways for collaboration with the representatives of the other branches of government[13], as well as with the security sector in general.

Already after the Second World War[14], military establishments have been heavily engaged in human security-related activities in the peacekeeping and in many kinds of duties in assisting civilian authorities. This shift in orientation has been accelerated also by academic studies and debates. At least since the 1980s, the so called 'interparadigm debate' (Raitasalo 2008) between the traditional realist, or positivistic, interpretations and the emerging anti-positivistic interpretations has been going on. Instead of taking an 'either-or' stand in these debates, the present paper focuses on the meaning, dynamics and application of (security) concepts, and debates that have often taken place across these categories (Fierke 2007, 3). This means that the most enlightening debate for the human oriented security studies seems to be the debate over the traditional orientation to security versus critical security studies (CSS) (Fierke 2007; Booth 1991; see Limnéll 2009, 57–60). In other words, this paper has the emansipatory interest that is shared by critical security studies and military pedagogical studies. The subjects to be emancipated are the soldiers (i.e. citizen soldiers) but also the other security sector actors, including all the citizens of Finland.

The military pedagogists of the Department of Leadership and Military Pedagogy at the Finnish National Defence University feel the need to enhance educational considerations within the wide field of comprehensive crisis management and among human security researchers and educators. For this purpose, a new kind of course for MMSc students (i.e. MA students) was held this winter, called 'Security and Comperehensive Crisis Management', and this paper reflects on the progressive inquiries done before, during and after the innovative and future-oriented course.

A brief and critical introduction to the (too) various kinds of security strategies of Finland

Based on the premise that the Finnish security sector already has some shared and mediating concepts, at least in its strategies, a qualitative content analysis is done in this paper. Through the content analysis we can see how widely the *focal* concepts (i.e. human security; action competence) are shared or not within the branches of the Finnish government. Also the possible differences in the conceptual meanings of the focal concepts can be identified. For a start, it is assumed that the strategies and policies in question construct *a hierarchic constellation* where the more normative strategies, such as the Finnish Security and Defence Policy (FSDP, 2009) and e.g. Finland's Comprehensive Crisis Management Strategy (2009) *should* form a clear basis for *coherent political guidance* of the several branches of the government. The 'coherency check' can be done by comparing the most normative strategies/policies to several

[13] According to the Strategy for Securing the Functions Vital to Society (=SSFVS 2006) each ministry, within its mandate, shall steer and monitor the implementation of tasks and the development of required capabilities related to securing the society's vital functions. The Ministry of Defence is responsible for the coordination of total defence activities.

[14] Cf. Henk (2007, 225) who claims that after the early 21st century the military establishments have been heavily engaged in human security- related activities. Interestingly, Henk's interpretation neglects the long historical roots of e.g. UN-led peacekeeping operations, as well as the soldier's role as an actor of internal security.

security oriented "sub-strategies"[15]. The analysis is done in a future-oriented manner due to the fact that the potentially identifiable lack of coherence in the strategies/policies can be to a large extent avoided in the forthcoming security strategies/policies.

According to the FSDP (2009, 71, 82), Finland follows a comprehensive approach which recognizes the interrelationship between internal and external security. Finland will be defended by focusing the resources of the entire society on national defence efforts, in line with the principles of the comprehensive defence approach and the Strategy for Securing the Functions Vital to Society (SSFVS, 2006).

The FSDP (2009, 129) continues that in the Comprehensive Approach (CA), the goal in crisis management is to coordinate different activities *coherently* while respecting the independent *role* of each actor. The FSDP claims also that the impact of the activities must be assessed in its entirety, and along with this, the policy runs into difficulties. Firstly, all the impacts (consequences; both intended and unintended) have to be assessed holistically, and secondly, the impacts have to be linked back to the actors having 'independent roles'. The position 'actors having static and independent roles' is an example of the 'old-fashioned' functionalist sociological interpretation, and sociologically an extensively and convincingly criticized position. Also when interpreting from the angle of the cultural-historical activity theory, the actors participate in collective activities having a shared object and outcome (i.e. 'consequences') being potentially related to human beings and their basic needs (i.e. safety; human security). Instead of a static independency position, the security sector actors should favour more *dynamic*[16] interpretations of their basic premises, values and their position in the security-oriented networks, e.g. due to the continuous cultural evolution of their operational environments.

According to the FSDP (2009, 110), the deterrence of Finland demands that the Defence Forces are capable of repelling an attack requiring e.g. *a comprehensive situation picture* and an early-warning capability, constant readiness in the chain of command, highly capable key troops and systems in every service, good operational mobility across the nation, and capability of cooperating with other authorities and key actors of the business sector.

But what kinds of threats are the Defence Forces and the other (*European*) security sector actors facing? According to the FSDP (2009), the threats are wide-ranging and interdependent. Logically, it follows, like the FSDP claims, that traditional security policy instruments and military defence will not suffice; fresh approaches are needed in order to respond to new kinds of threats.

Let us return to the issue of what the deterrence of Finland, Europe and the globe demands? As stated, *a comprehensive situation picture* and early-warning capability with constant readiness to act with *appropriate means* is needed for the evolving security sector in Finland, and even more so on a European, and also on a global level.

A recent analysis made by Jarno Limnéll of the FSDP in 2004 (2009, 189) clearly shows how rapidly the security strategies are evolving in Europe as well. For example the European Security Strategy (2003) does not discuss environmental, or human, security threats (cf. European Union 2008). On the

[15] The Internal Security Programme is an example of a "sub-strategy".
[16] By dynamic I refer simply to the "non-static" nature of the phenomena in question and additionally also to such ongoing debates as the debate on agency versus structures, Latourian discussion about the actants, and the "subjectless" sociological theories (see Mäkinen 2006).

other hand, the FSDP (2009) emphasizes that long-term global trends, such as climate change, need to be countered by a comprehensive approach.

The Advisory Board for Defence Information (ABDI) has a long tradition of polling the opinions of Finns on the Finnish foreign and security policy and defence policy. In addition, since 2007, citizens have been asked to provide their views on how they think security will develop over the next five years, and to assess factors which affect the security of Finland and their personal *sense of security*. When comparing the ABDI polls done in 2007 and 2009 it can be seen that in 2009 a deep, global crisis of the international economy, getting 48 % share of the answers (41% in 2008), was seen as the most likely threat. The result is understandable in the midst of a severe global economic crisis. The second most likely threat in the ABDI poll of 2009 was an environmental disaster caused by global warming, getting 46 % (37 % in 2008) of the answers. The number of those seeing the environmental disaster as an influential source of a security threat has risen by 9 % in a year, maybe partly because now it has been proven that we humans have an influence on climate change (IPCC 2007). This trend should be notified both in the next FSDP and in the next European Security Strategy, although the fundamental question of 'what threatens us' remains partly unanswered. In a way our situational picture is a non-comprehensive one, giving no real support for comprehensive security planning nationally or internationally.

According to Finland's Comprehensive Crisis Management Strategy (2009), the objective of crisis management is to strengthen human security[17] and comprehensive crisis management through shared training and research. For these purposes, Crisis Management Centre (CMC) Finland and Finnish Defence Forces International Centre (FINCENT) have intensified their training cooperation by founding the Finnish Centre of Expertise in Comprehensive Crisis Management. However, (academically) educational co-operation within the emerging national security sector has to be established as well. High quality (national/international) *human security education* has to have some shared concepts and dimensions. One major candidate to act as a mediating means within the security sector is the concept of human security.

Human security – an end itself but also a mediating concept within the security sector

In the course of the profound and complex contemporary developments, the paradigm of human security might be the 'third step' coming after the first step to the 'postmodern warfare' and the second step to 'fighting against terrorism' (Toiskallio 2007, 9). In the 1970s, the so called 'human rights regime' emerged as a result of the development of the human rights law, the Conventions and the Helsinki Agreement of 1975, and the proliferation of human rights activists concerned about human rights abuses (Kaldor 2007, 8). Another complementary and central explanation for the emergence of the human security has been offered by Sabine Alkire (2003; cf. CMC 2009) who has claimed that due to the mis-

[17] Interestingly both the Strategy for Securing the Functions Vital to Society (2006) and the Internal Security Programme (2008) do not mention the concept of human security at all. It is possible, and actually justifiable to assume, that the forthcoming SSFVS and ISP strategies deal with human security and do it comprehensively and coherently.

match between the security threats, and the national and international responses to these threats, the human security approach has got its pivotal position within the global security sector. The 'mismatch' feeling has been shared also by soldiers, the seminal book of general (ret.) Rubert Smith (2005) being a prime example of this point.

Instead of aiming to analyze and show the most appropriate definition of the concept, the famous 'right answer' for the 'question' of the human security (see Alkire 2003; Commission on Human Security 2003; CMC 2009), the intent in this paper is to show the main *dimensions*[18] of the human security oriented activities to be shared by the main security sector organizations and actors. One of the main premises of the paper is that the dimensions emphasized by the human security approach suggests that we should enable our students, both military and civilian ones, to shift their orientation along the dimensions (cf. the key educational dimensions; Mäkinen 2006) proposed in this article.

The seminal report of the UN, the Human Development Report (1994), sets the stage for those interested in finding out the main dimensions of the human security approach. Instead of 'adding more cooks to the soup of the conceptual mess of human security', a clarification is sought after by a multidimensional framework already potentially identifiable in the Human Development Report of 1994.

According to the Human Development Report (1994) the threats to human security are no longer just personal or local or national, they are becoming *global*[19]. Against the awakening awareness about the global security situation, the report stresses that a sharable new paradigm of sustainable human development and security has to be sought for. The needed framework has to bring *humanity together* through more equitable sharing of global economic opportunities and *responsibilities* (ibid). Of course the global orientation is closely intertwined with the 'old-fashioned' national/local orientation, and this kind of conclusion may seem surprising, but we have to *reinterpret the local/national orientation for it to become a glocal human security orientation.*

The orientation of the international community often seems to be a reactive one, and especially for soldiers, this kind of orientation has meant overemphasis on post-conflict situations and on phases after open conflict (e.g. Koskela 2008, 7). Also the Human Development Report (1994, 3) challenges the traditional interpretation by stressing that it is important to develop some *operational indicators* of human security as an *early warning system* allowing us to help in avoiding to reach a crisis point. The main focus of the global community, including all security sector actors, should be on *the whole spectrum of conflict resolution responses*[20] (Ramsbotham et al. 2005, 12; Human Security Study Group). The special focus of the attention should be, instead of 'post-conflict' situations, preventive peace building means of overcoming structural and cultural violence when heading towards a 'positive peace' (Webel & Galtung (ed.) 2007) and 'better peace' (Liddell Hart 1954: 1991). Interestingly, Johan Galtung, the founder of peace studies and a peace researcher, and Sir Basil. H. Liddell Hart, a military strategist and a theorist of art of war, share the very same 'grand strategist' object – peace[21]. It seems that especially soldiers, as

[18] In other words the intent is to construct a multidimensional framework for human security-oriented activities.
[19] It follows that the first dimension of human security is the dimension between local and global. Therefore instead of "globalness" and "globalization", the emphasis of the paper is on the glocalness meaning an emphasis both on the global and on the local (i.e. local human agency).
[20] The whole spectrum of conflict resolution is the second dimension of human security.
[21] E.g. in 1994 NATO launched the Partnership for Peace program, and since 2004 the Partnership Action Plan on Defence Institution Building (PAP-DIP) has been operational. For additional information see http://www.nato.int/).

well as all security sector actors, have to be *educated* for 'whole spectrum' operations including also peace building operations and activities.

Neither peace nor war are ontological facts. Both are *potentially* socially constructed, and it is our responsibility to choose our side in this debate. According to the Human Development Report (1994, 13), human beings are born with certain *potential capabilities*. The purpose of development is to create an environment in which all people can expand their capabilities. One option, elaborated later in this paper, is to conceptualize these human potential capabilities as *action competence*. By emphasizing action competence we can agree with the Human Development Report that at the global level, sustainable human development requires no less than a new *global ethic* and *glocally shared responsibility* (Heinonen 2002; Heinonen & Romppanen 2010; Mäkinen 2010).

Let us now turn the attention to the Kaldorian interpretations about the question of adopting the human security approach in Europe. The first reason to adopt the human security approach (Human Security Study Group 2004) is based on morality, like emphasised in the Human Development Report (1994). All human life is equal, and it is not acceptable that human lives become cheap in desperate situations (i.e. be it in Rwanda, Srebrenica, or anywhere else). The second reason (ibid.) is legal, meaning that we have not only a right, but also a legal obligation, to concern ourselves with human security worldwide. The third reason (ibid.) for adopting the human security approach is 'enlightened self-interest'. The Europeans, or anybody else, cannot be secure while some people in the world live in severe insecurity. In a way we all are interconnected in the front of emerging security threats.

It is often understood that the human security 'paradigm' argues for the importance of simultaneous progress in a variety of domains (i.e. economic, food, health, environmental, personal, community, and political) (CMC 2009, 16-18), but instead of this traditional 'linear and unsystematic' kind of thinking, a more holistic (Toiskallio 2007, 8–9) and *systematic* way of thinking is needed[22]. This is a shared challenge for all security sector actors and not just for soldiers. The demand for holistic and systematic thinking goes in parallel with the 'utility of force' (i.e. the means) debate (Smith 2005). The situation is really challenging when both comprehensive situational awareness (i.e. awareness of the global and shared threats) and understanding of the means to counter these threats systematically are lacking.

According to the human security approach, in line especially with its European branch, a set of selected principles (Human Security Study Group 2004) should, and could, guide the actions of the security sector actors on all the levels of the *epistemic infrastructure* (Mäkinen 2006). In other words, the proposed principles are intended to be applicable both at the grassroot level (i.e. the soldiers and the civilians in the field) and at the "grand strategic level" (i.e. the UN, NATO, EU, OSCE etc).

The proposed set of complementary human security principles are the following (Human Security Study Group 2004; 2007):

- the primacy of human rights
- legitimate political authority
- multilateralism
- bottom-up approach

[22] The third dimension means shifting our thinking from linear towards more systematic ways of thinking.

- regional focus
- use of legal instruments
- appropriate use of force.

At this phase, only a short analysis of the proposed principles can be done. Traditionally, it has been assumed that the interests of states (i.e. natural resources, economical advantages), or the interests of "the military-industrial complex" (see Mäkinen 2010), override the needs to promote e.g. human rights and security. Contrary to this kind of traditional interpretation, the *hypernorms* should and could constrain the local *authentic norms* (Donaldson & Dunfee 1994; e.g. globally destructive overemphasis on self-interests (i.e. freedom) over interests of our humanity). One proposed candidate for such a hypernorm is *human dignity*[23] (Mäkinen 2010). At this phase, the proposed hypernorm is just a "potential" one, waiting to be checked in e.g. crisis management realities. In other words, the emphasis on "reality checks" means also emphasis on case studies, and more precisely, on *hierarchic/networked case studies*. By hierarchic/networked, or *systemic*, case studies I refer to studies whose unit of analysis is neither only soldiers/security sector actors on the field nor only a specific mission (e.g.. ISAF in Afganistan or KFOR in Kosovo), but instead the whole epistemic infrastructure from the individuals up to the "grand strategic level", according to the bottom-up principle.

The meaning of multilateralism should be interpreted more comprehensively than 'acting with a group of states' (Human Security Study Group 2004). Multilateralism means a commitment to work with international institutions, but it also means commitment to common ways of working and to *agreed rules and norms*. Additionally, multilateralism means coordination of collective efforts and activities[24]. Finally, the regional focus needs to be explained, although it is closely linked to the above-mentioned bottom-up (i.e. epistemic infrastructure) approach. The emphasis on regional issues means that not only local-global interaction is needed for stability, well-being and peace. The activities at a regional level play a crucial mediating role between the national and international/global levels. Interestingly, the regional approach is not applicable somewhere in Africa only, or in the former Soviet Union, but also here in Finland with its neighbours. The fundamental question, in the case of Finland, is the regional cooperation between the Nordic countries and with our Eastern neighbours (i.e. the Russians; see e.g. Heusala, Lohiniva & Malmi 2008). This question is even more pivotal in the case of all kinds of security institutions (including military institutions), because the ultimate end is not war but peace.

For soldiers, and for all security sector actors, the use of force, and especially ethically justifiable use of force is the fundamental and paradoxical question[25]. In 2004, the Human Security Study Group proposed a 'Human Security Force' to be composed. A minimum use of force should be the norm for such a Force, meaning that this kind of an attitude is more akin to the traditional approach of the police, who risk their lives to save others, even though they are prepared to kill *in extremis*, as human security forces should be.

---

[23] The debate over the similarities and differences of human security, human development and human rights is an ongoing one among human security researchers and practitioners, but here the intent is not to deal with these issues. Only the focus on human individuals and on their needs (i.e. security and many others according to e.g. Maslowian human hierarchic needs) is the focal point to be emphasised in this military pedagogical article.
[24] The premise of this article is that the security activities should share e.g. some objects, ends and means in order to achieve an appropriate level of coordination and coherence.
[25] For more about the paradoxes of the soldiers, see Mäkinen 2006.

Effectiveness, and the impact assessment of human security activities (CMC 2009), is more than just the capability to act, or to react. The preventive, more peace building oriented approach requires that Finland, and also the EU, will continue discussing about the strategic direction of Finland and the EU on a political level. But even more than traditional political discussions, a more ethically-morally oriented strategic debate should be going on. Systemic case studies are needed on an international, as well as on a collective and on an individual level (e.g. Human Security Study Group 2007; CMC 2009; Athanasiou 2007; see Mäkinen 2010 for additional case studies).

Is there any need for action competent human agents in the future?

In the comprehensive field of national security, action competence is a practically mediating concept (Finnish Government 2008; Defence Command 2007). The concept of action competence also acts as a boundary object (Star 1989) between the military and e.g. the civilian national security -oriented activity systems.

Traditionally, action competence has been a philosophically oriented social construction used in the military educational context. In the near future, the concept of action competence will be elaborated further as a behavioural scientific concept. This means that the boundaries between philosophically oriented human sciences (i.e. the position of traditional military pedagogy) and behaviourally oriented psychologies and social sciences will be discussed, and crossed, with the assistance of a *mediating model* (Figure 1; Toiskallio & Mäkinen 2009, 102).

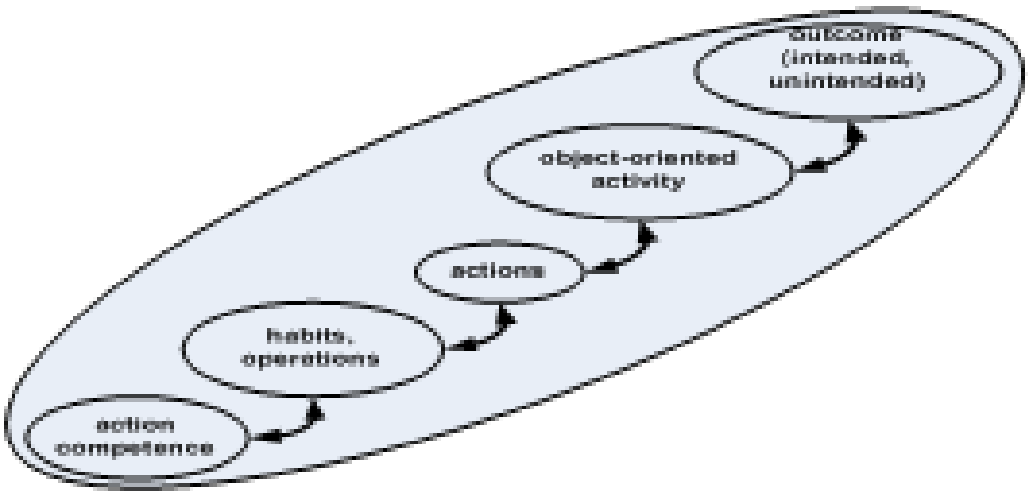


Figure 1. Action competence in its context.

The core of action competence features the concept of identity; namely, in our case, the identity of soldiers. For us this means that we keep asking and partially answering what it actually means to be a soldier in a democratic state, say, in Finland. To be a good, even a great soldier, means, among other things, that one is able to solve the fundamental paradox of being a soldier: how is it possible to maintain one's ethical consistency and be an ethical subject by justifying killing and respecting human dignity at the same time?

Discussion and conclusions

Even a brief analysis like this shows clearly how the ambiguous concept of human security can be made understandable and sharable by utilizing dimensional, principled and systematic thinking. Education seems to be the main instrument for us to enhance the shift of minds, orientations and ways of acting, and the dimensions emphasize the main focal points of our shared interests. Education needs some shared concepts, and human security and action competence are justifiable candidates for this.

References

Advisory Board for Defence Information (ABDI) (2009). http://www.defmin.fi retrieved 15.3.2010.

Alkire, S. (2003). *A Conceptual Framework for Human Security*. Centre for Research on Inequality, Human Security and Ethnicity, CRISE.

http://www.crise.ox.ac.uk/pubs/workingpaper2.pdf retrieved 15.3.2010.

Athanasiou, E. (2007). Human Security at Test: The United Nations Peacekeeping Operation in the Democratic Republic of Congo. *Human Security Journal*, Vol.5, pp.72-80.

Bailes, A.J.K., Herolf, G. & Sundelius, B. (2006). *The Nordic Countries and the European Security and Defence Policy*. UK: Oxford University Press.

Booth, K. (1991). Security and emancipation. *Review of International Studies*, Vol. 17, pp.313-326.

CMC (2009). *Training manual: Human Security in Peacebuilding*. Kuopio: CMC.

Defence Command (2007). *Kenttäohjesääntö – yleinen osa: puolustusjärjestelmän toiminnan perusteet*. (Finnish Doctrine for Military Operations). Helsinki: Edita Prima. (in Finnish)

Donaldson, T., Dunfee, T.W. (1994). Toward a unified conception of business ethics: integrative social contracts theory. *Academy of Management Review*, Vol.19 (2), pp.252-284.

European Union (2003). *European Security Strategy*. http://www.consilium.europa.eu retrieved 15.3.2010.

Human Security Study Group (2004). *A Human Security Doctrine for Europe: The Barcelona Report of the Study Group on Europe's Security Capabilities*.
http://www.lse.ac.uk/Depts/global/Publications/HumanSecurityDoctrine.pdf retrieved 15.3.2010.

Human Security Study Group (2007). *A European Way of Security: The Madrid Report of the Human Security Study Group comprising a Proposal and Background Report*.
http://www.lse.ac.uk/Depts/global/PDFs/ retrieved 15.3.2010.

European Union (2008). *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World*. http://www.consilium.europa.eu retrieved 15.3.2010.

Commission on human security (2003).
http://www.humansecurity-chs.org/finalreport/Outlines/outline.pdf retrieved 15.3.2010.

Fierke, K.M. (2007). *Critical approaches to international security*. UK: Polity Press.

Finnish Government (2006). *The Strategy for Securing the Functions Vital to Society*.
http://formin.finland.fi retrieved 15.3.2010.

Finnish Government (2008). *Internal Security Programme*. http://www.intermin.fi retrieved 15.3.2010.

Finnish Government (2009). *Finnish Security and Defence Policy*. Helsinki: Prime Minister's Office Publications.

Finnish Government (2009). *Finland's Comprehensive Crisis Management Strategy*. http://formin.finland.fi retrieved 15.3.2010.

Finnish Parliament (2007). *Act on the Defence Forces*. http://www.finlex.fi/fi/laki/kaannokset/2007/en20070551.pdf retrieved 15.3.2010.

Heinonen, R. (2002). Values Memory, Global Ethic and Civil Crisis Management in Toiskallio, J., Royl, W., Heinonen, R.E. & Halonen, P. (eds.) *Cultures, Values and Future Soldiers*. Helsinki: Finnish National Defence College.

Henk, D. (2007). Human Security and the Military in the 21st Century in Toiskallio, J. (ed.). *Ethical Education in the Military*. Helsinki: Edita Prima.

Heusala, A.-L., Lohiniva, A. & Malmi, A. (2008). *Samalla puolella – eri puolilla rajaa: rajaturvallisuuden edistäminen Suomen ja Venäjän viranomaisyhteistyössä*. (On the same side – on different sides of the border: enhancing border security in co-operation with Finnish and Russian officials). Tampere: Juves Print.

Kaldor, M. (2007). *Human Security*. UK: Polity Press.

Koskela, M. (2008). Preface in Eronen, O. (ed.). *Needs of Comprehensiveness: Building Blocks for Finnish Crisis Management*. Helsinki: Edita Prima.

Liddell Hart, B.H. (1954: 1991). *Strategy*. Second Revised Edition. US: Meridian.

Limnéll, J. (2009). *Suomen uhkakuvapolitiikka 2000-luvun alussa*. (Finnish threat perceptions in the early 21st century). Helsinki: Edita Prima. (in Finnish)

Moskos, C.C., Williams, J.A. & Segal, D.R. (eds.) (2000). *The Postmodern Military: Armed forces after the Cold War*. US: Oxford University Press.

Mäkinen, J. (2006). *The Learning and Knowledge Creating School: Case of the Finnish National Defence College*. Helsinki: Edita Prima.

Mäkinen, J. (2010). Creating a Unified Framework for Future-Oriented Education of Military Ethics in Annen, H. & Royl, W. (eds.). *Educational Challenges Regarding Military Action*. Frankfurt am Main: Peter Lang.

Polanyi, M. (1966). *The Tacit Dimension*. London: Routledge&Kegan Paul.

Raitasalo, J. (2008). *Turvallisuusympäristön muutos ja Suomen puolustus*. (The changing nature of the security environment and the defence of Finland). Helsinki: Edita Prima. (in Finnish)

Ramsbotham, O., Woodhouse, T. & Miall, H. (2005). *Contemporary Conflict Resolution: The prevention, management and transformation of deadly conflicts*. Second Edition. UK: Polity Press.

Smith, R. (2005). *The Utility of force: the art of war in the modern world*. New York: Allen Lane.

Star, S.L. (1989). The Structure of Ill-Structured Solutions: Boundary Objects and Heterogeneous Distributed Problem Solving in Gasser, L., Huhns, M.N. (Eds.). *Distributed Artificial Intelligence. Volume II*. UK: Pitman Publishing.

Stoltenberg, T. (2009). *Nordic Cooperation on Foreign and Security Policy*. http://formin.finland.fi retrieved 15.3.2010.

Toiskallio, J. (ed.) (2007). *Ethical Education in the Military*. Helsinki: Edita Prima.

Toiskallio, J. & Mäkinen, J. (2009). *Sotilaspedagogiikka: sotiluuden ja toimintakyvyn teoriaa ja käytäntöä*. (Military Pedagogy: Theories and practices of the soldiership and action competence). Edita Prima: Helsinki. (in Finnish)

United Nations (1994). *Human Development Report*. http://hdr.undp.org/en/reports/global/hdr1994/ retrieved 15.3.2010.

Webel, C. & Galtung, J. (eds.) (2007). *Handbook of Peace and Conflict Studies*. UK: Routledge.

TREND AND BENCHMARKING ANALYSIS OF EUROPE-AN PRISON POPULATION 1993-2007: STATISTICAL ANALYSIS ON EUROPEAN TRENDS WITH BENCH-MARKING PRISON POPULATIONS IN THE U.S.A. AND IN THE RUSSIAN FEDERATION

Research Director, Dr (Adm.Sc.), MSc (Econ.) Jari Kaivo-ojaa
[a]Finland Futures Research Centre, University of Turku, Finland

Development Manager, Dr (Psychology) Arja Konttilab
[b]Criminal Sanctions Region of Western Finland, Turku, Finland

ABSTRACT *– The development of prison population is one key issue in the security policy of a society. From a general security research perspective, this kind of international statistical analysis provides many important empirical insights for security policy in EU Members States, in U.S.A. and in the Russian Federation. This article provides trend analyses of European26, U.S.A. and Russian Federation prison population in the years 1993-2007. A lot relevant observations and findings are presented concerning prison population trends in different countries and in Europe. Three alternative trend shapes of prison population development are identified.*

Introduction

This article will address a trend and a benchmarking analysis of European prison population. Prison population studies have been used in the planning of security policy, criminal policy and prison size management (Barnett 1987). Earlier research has indicated that the enlargement of EU means greater opportunities for crime, but it is also an incentive for the process of approximating law and building institutions (Loader 2002). From this European policy perspective, it is interesting to analyze trends in prison population generally and especially in prison population of violent offenders during the enlargement process of the EU. The prison population study monitors prison population trends in today's enlarged Europe and beyond. Similar types of crime comparisons between countries have been provided by

[26] Country sample of Europe is including the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, France, Germany, Greece, Hungary, Ireland, Italy, Liechtenstein, Luxembourg, Macedonia, Malta, Montenegro, Netherlands, Northern Ireland, Poland, Portugal, Romania, Scotland, Serbia, Slovenia, Slovakia, Spain, Switzerland and Turkey.

Stollmack 1973, Blumstein, Cohen & Miller,1980, Gilinskiy 2006, Hofer 2003 and Vieraitis, Kovandzic and Marvell 2007, Holmes 2009).

The amount of prison population is a good measure of the general security climate in different countries. Empirical database of the study covers years 1993-2007. In the study, historical development of the prison population in Europe, U.S.A. and Russian Federation are analyzed. We also report prison population trends of South Africa, Turkey and Canada. This study analyses critical changes in the prison population during the years 1993-2007. These data sets consist of comprehensive national-level data of the Eurostat (Eurostat 2010). Because of some problems of Eurostat data (ibid.), we have added UN demographic data to some databases (United Nations 2010). Criminal policy is considered a part of security policy of a country. What might be the optional level of prison population? It has been proved in earlier criminal and security research that severe prison sanctions increase recidivism compared to interventions based on cognitive-behavioral models of social change (McGuire 2003). In this article, we discuss conceptual and theoretical issues of security and criminal policy in section 2 (security policy) and section 3 (criminal policy). In section 4, we shall report the results of nationwide and regional benchmarking analyses. In the benchmarking analysis, conventional statistical analyses are presented. Trends in prison population are analyzed in Section 4. In the benchmarking analysis, special attention is paid to prison population of Turkey compared to European prison populations. Second key part of the statistical benchmarking analysis is a comparison of the prison populations in the Europe -, in U.S.A. and in the Russian Federation. We shall also provide an analysis of prison population in relation to total population and in relation to total criminality statistics.

Thus to make a summary, the article provides updated "big picture" of prison population trends in Europe, in U.S.A. and the Russian Federation. From a general security research perspective, this kind of international statistical analysis provides many important empirical insights for security policy in EU Members States, in U.S.A. and in the Russian Federation. In the study, linear trend analyses are provided and expected linear BAU -scenarios are reported. The provided analyses are useful when criminal policy professionals and policymakers are planning prison capacities and social policy programs for the prisoners in different European countries and abroad in U.S.A. and in the Russian Federation. This study is not analysis special prisons of terrorists, which exist in Europe (Bures 2006).

Conceptual issues of security and security policy research

The role of the prison has changed over the last decades. Liebling (2006) noted that dramatic changes have been that the prison population has grown and its composition has altered. Security climate and the environment of criminal policy have also changed. We live in dynamic societies where values and policies are in change. Whereas some societies, favor severe criminal punishments, in some other societies less severe criminal punishment policies are favored. It is clear that prisons are needed especially for violent psychopathic offenders (Konttila & Holmalahti 2009). There are many factors which affect the size of prison populations. Such factors are (1) juridical laws, changes in penal policies, and normative systems, (2) employment rate, (3) demographic changes, (4) social norm structures, (5) sex related norms and values, (6) political decisions, (7) technical security innovations, (8) goals and means of prison service, (9) courts and their decisions (Lavenex 2004, Louks, Lyner & Sullivan 1998, Blom-Hansen

2005, Lerch & Schwellus 2006, Deams 2008, Fábián 2010, Ochsen, 2010). There is no obvious single explanation for crime rates.

Security is a challenging concept. To clarify key aspects of security, we must use two associated concepts; objective security and subjective security. Objective security is real dimension of security without any reality biases. Subjective security reflects a subjective dimension on security, which is not based on real facts and the objective reality where an individual lives and exists. In Figure 1, four dimensions of security are identified: Ideal security situation is in depicted in B where people have high level of objective security and subjective security. The most problematic situation forms C, where both subjective security and objective security are on low levels. A is a special situation where people have very high subjective security level but actually they are in danger (objective security level is low). People who faced the September 11 attacks were in this kind of situation in New York before airplanes came and destroyed the twin towers. D is also a special situation where people have very low subjective security level but they are not in danger in any way (consider people suffering from phobias). Security that people feel can be in any space of Figure 1.

Criminal policy is connected to security policy and security concerns. One key motivation of criminal policy is the argument that people experience higher subjective security and partly higher objective security when criminals are in prisons. These aspects of security are very important for policymakers. Especially sentence lengths vary much in different countries. Criminal policy is a political issue in different countries but also inside the EU (see e.g. Loader 2002).

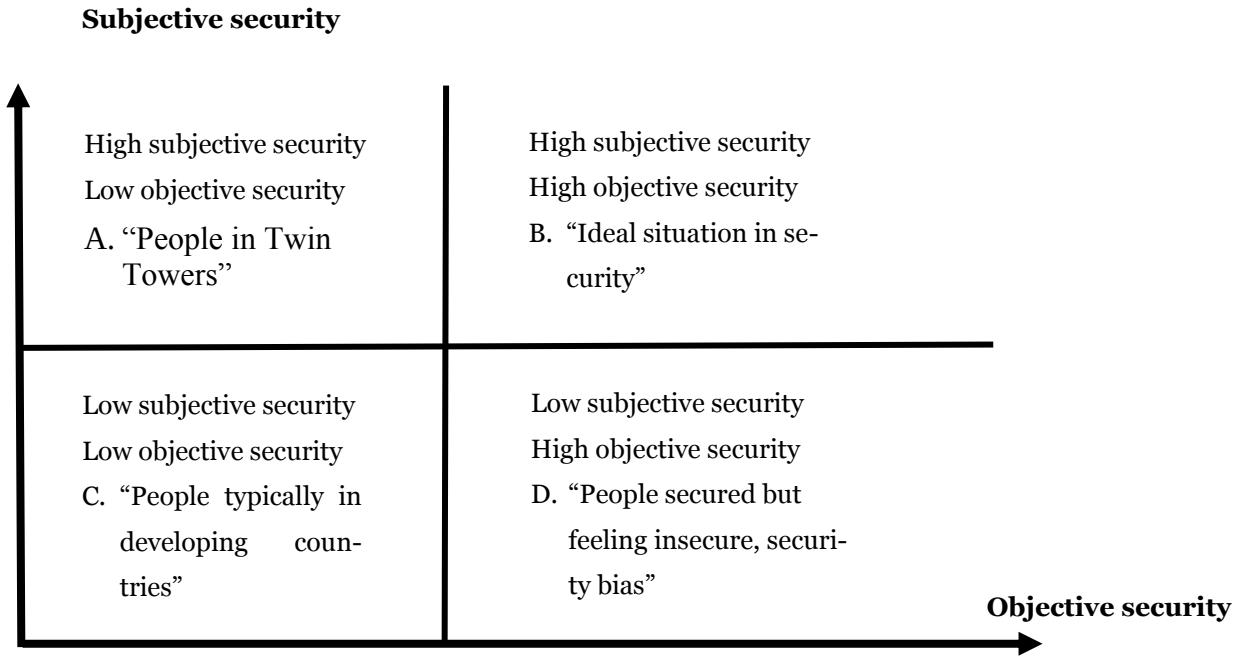


Figure 1. Objective and subjective security

Criminal policy concepts

Modern criminal policy in Europe has emphasized the importance of rehabilitation as a goal connected to the execution of sentences. For example, the main goal of Finnish prison service is to reduce the recidivism, re-offending of the prisoners by using different rehabilitative methods depending on the risks and needs of the prisoner. According to research, many different cognitive-behavioral programs have been indicated to be effective in this respect (Allen et al. 2001; Andrews 1995). At the same time, however, there is a demand for more and longer prison sentences emphasizing the punitive role of crime policy. Death penalty as a form of sentence has been abandoned in most countries. Today it is used for example in many U.S. states and in China but no longer in Russia.

Contemporary Russian criminal legislation and police methods, criminal justice and prisons are very strict, unjust and repressive (Gilinskiy 2006). Russia has faced problems in maintaining control except through repression. It has never been a democratic state. Considerable social and economic inequality has always characterized Russia which has even increased in recent years. Economic inequality is one important criminogenic factor (that is a factor maintaining or leading someone to commit a crime) in a society. In addition, there are also cultural factors that have created a specific Russian mentality that is characterized by intolerance. These are the main factors that explain the high rate of violence in Russia (Gilinskiy 2006).

Criminal policy of the United States has increasingly relied on the mass incarceration to reduce crime and it has been asked whether they should continue to expand prison capacity indefinitely (Mauer 2001). On the other hand, large amounts of inmates in closed prisons are very expensive for society. Nowadays many American states are put in a difficult situation and as a result of the economic recession they try to save money by releasing non-violent prisoners on probation much earlier. There are several factors which contributed to the rise in the use of incarceration since 1980; Firstly, American culture of individualism and free market liberalism (see e.g. Milton Friedman 1962). American emphasis on individual approaches to social welfare created a receptive climate for harsh prison policies (Mauer 2001). It is not amazing that a very large part of the prison population consists of poor and black males or immigrants. Secondly, there is the politicization of crime and growing conservative political climate which supports the “Getting tough” attitude on criminals (Mauer 2001). Prisoner rates are to a great degree a function of criminal and social policies of a country but the connection is complicated.

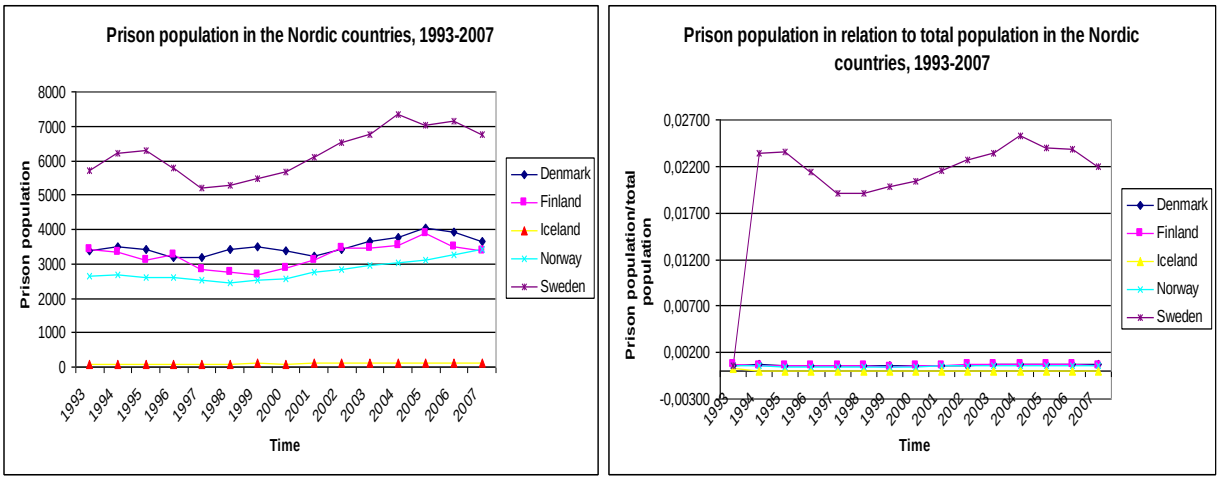
There are different ways to define the concept of ***prison population***. In this article, the definition of Eurostat is used: prison population is the “total number of adult and juvenile prisoners (including pretrial detainees) at 1 September. Including offenders held in Prison Administration facilities, other facilities, juvenile offenders' institutions, drug addicts' institutions and psychiatric or other hospitals. Excluding non-criminal prisoners held for administrative purposes (for example, people held pending investigation into their immigration status)”. The ***criminality*** of a country means the total recorded offenses against the criminal code including homicide, violent crime, robbery, domestic burglary, theft of a motor vehicle and drug trafficking. Most analyses are based on the total crime rates. ***Total crime statistics*** include offences against the penal code or criminal code. Less serious crimes (misdemeanors) are generally excluded (Eurostat 2010).

Criminality and prison population trends in a comparative international setting

Prison population trends during the years 1993-2007 in te Nordic countries

Basically, the Nordic countries are quite similar economically and socially and have had same kind of crime trends, so it is interesting and easy to compare their prison populations. In Figure 2, we can see that the situation in Sweden differs very much from the other Nordic countries. The amount of prisoners in Sweden is much higher than in Denmark, Finland and Norway and the trend is quite steady during the period of nearly twenty years. The difference grows even bigger when the prison populations are examined in relation to the total populations of these countries (Figure 2). At this point it is interesting to examine the crime rates (Figures 2 and 3). The crime rates of Sweden from 1996 to 2007 show an increase of 11 % in total criminality whereas the crime rates of the other Nordic countries has not increased, for example in Denmark it has decreased about 15 % and in Finland nearly 9 %. The amount of homicides has also decreased in Finland and Denmark but increased in Sweden. Other violent crimes have increased in these Nordic countries but the biggest growth is in Sweden. These results seem to show the ineffective and detrimental form of punishment (Eurostat 2010).

In addition to looking at the means between the countries, it is interesting and useful to examine the standard deviations which are shown in Table 1. It is striking that the smallest standard deviation is in Sweden and the biggest one in Iceland. The standard deviations of the other Nordic countries show that the amount of prisoners does not vary very much.



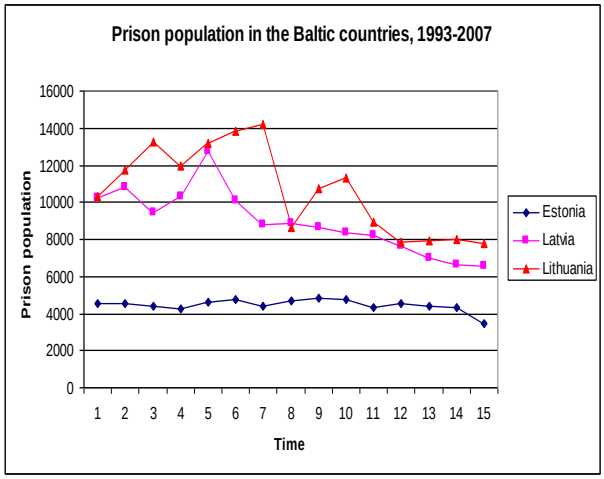
Figures 2 and 3. Prison population in the Nordic countries, 1993-2007. Prison population in relation to total population in the Nordic countries.

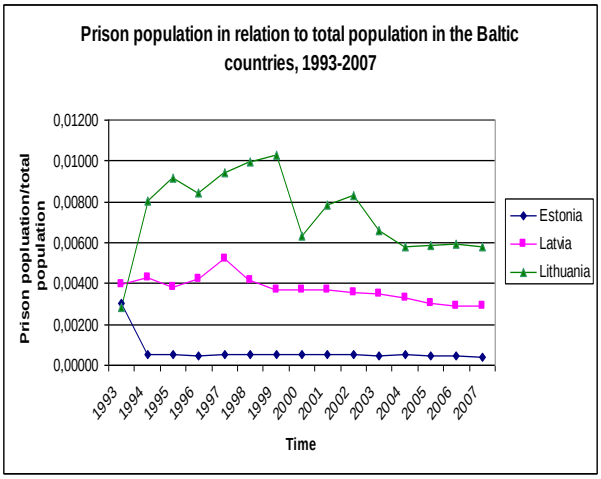
Table 1. *Prison population in relation to total population in the Nordic countries. Basic statistical analysis.*

	Min	Max	Range	Average	Median	Var	Standard deviation
Denmark	0,00060	0,00075	0,00015	0,00066	0,00065	1,72617E-09	4,15472E-05
Finland	0,00052	0,00074	0,00023	0,00063	0,00064	3,9394E-09	6,27646E-05
Iceland	0,00001	0,00036	0,00034	0,00004	0,00002	7,65384E-09	8,74862E-05
Norway	0,00048	0,00065	0,00017	0,00055	0,00053	2,95883E-09	5,43952E-05
Sweden	0,00065	0,02523	0,02458	0,02067	0,02191	3,41279E-05	0,00584191

Prison population trends during the years 1993-2007 in Baltic countries

Figures 4 and 5 show that the amount of prison population in Estonia is at a very low level in comparison to Lithuania and Latvia even though the amount of prisoners is decreasing in both Lithuania and Latvia. The rate is very high in Lithuania when the prison population is examined in relation to the total population. Lithuania has the biggest average and standard deviation of the prison population (Table 2). It is amazing how Estonia has been able to keep the rate of prisoners so low, when at the same time the total crime rate has increased over 40 %. The prison populations of all three Baltic countries have decreased during the years 1993-2007 although especially drug trafficking crime has increased explosively during the years 1996 – 2007 (Eurostat 2010). So the growth in crime rates in Estonia and Latvia cannot be seen in prison population trends.





Figures 4 and 5. Prison population in the Baltic countries, 1993-2007. Prison population in relation to total population in the Baltic countries

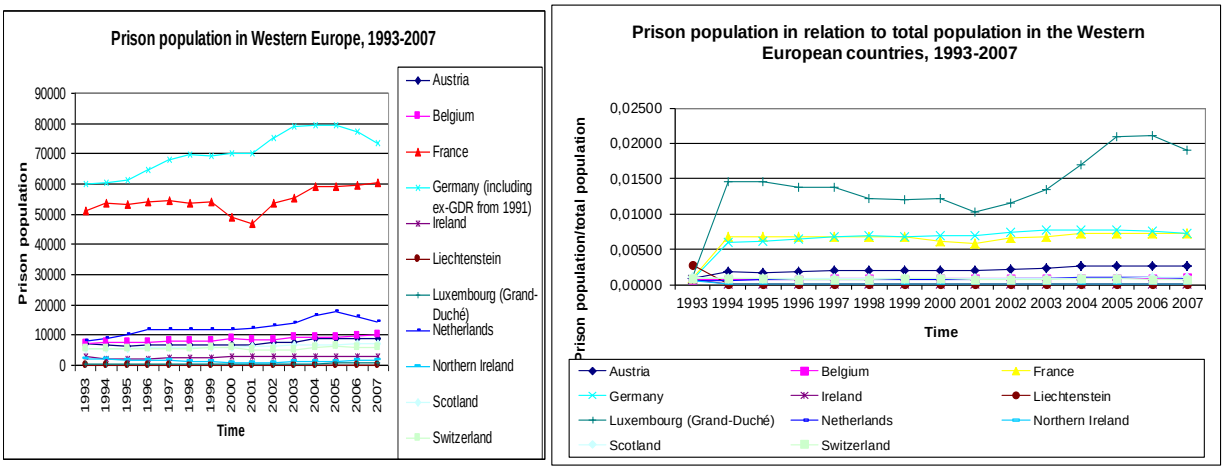
Table 2. *Prison population in relation to total population in the Baltic countries. Basic statistical analysis.*

	Min	Max	Range	Average	Median	Var	Standard deviation
Estonia	0,00038	0,00302	0,00263	0,00067	0,00051	4,24025E-07	0,000651172
Latvia	0,00287	0,00523	0,00236	0,00373	0,00367	3,72102E-07	0,000610002
Lithuania	0,00281	0,01030	0,00749	0,00738	0,00786	4,08509E-06	0,002021161

Prison population trends during the years 1993-2007 in Western Europe

Figure 6 indicates that Germany and France have the greatest number of prison population whereas the other Western European countries have much lower rates. The Netherlands had its highest amount of prison population in the year 2005 which was nearly 20000. The situation becomes quite different when the prison populations are examined in relation to total populations. The Prison population in relation to total population is clearly highest in Luxembourg and the amount grew quite steadily since 2001 until 2006. At first it seems amazing. There have been steadily growing migration in Luxembourg during the years 1961-2003 so that in the year 2007 there were 37 % immigrants of the population and 5000 illegal immigrants (Wikipedia/Luxembourg). Alcohol consumption is also quite high in Luxembourg (WHO 2004): it sells the most alcohol in Europe per capita. However, the visiting foreign customers of the neighboring countries (Germany, France and Belgium) also contribute to the high level of alcohol sales per capita. Level of education has not been very high because the only university was build not until in 2003. The situation of Luxembourg is also so central that it is quite easy for the professional offenders to come to the country.

Next after Luxembourg are performing Germany and France, which have had the amount of prisoners quite at a same level during this checking period (Figure 7). The averages, medians and standard deviations of all the Western countries are shown in Table 3.



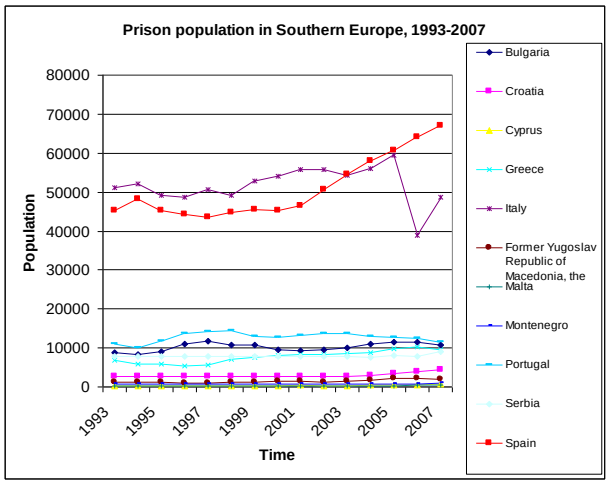
Figures 6 and 7. Prison population in the Western Europe, 1993-2007. Prison population in relation to total population in the Western Europe

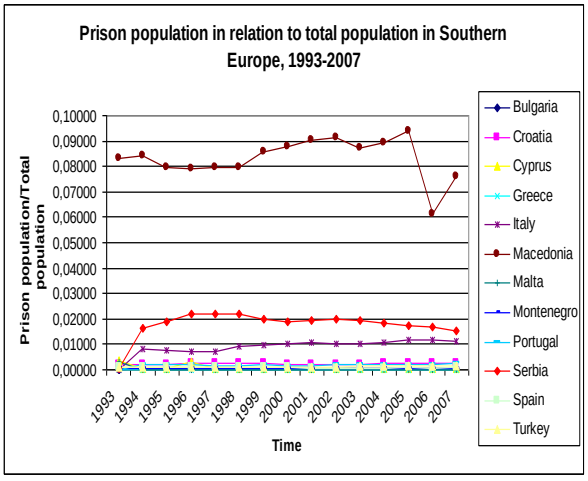
Table 3. *Prison population in relation to total population in Western Europe. Basic statistical analysis*

	Min	Max	Range	Average	Median	Var	Standard deviation
Austria	0,00091	0,00263	0,00172	0,00206	0,00196	2,02806E-07	0,00045034
Belgium	0,00072	0,00097	0,00025	0,00083	0,00084	6,25931E-09	7,91158E-05
France	0,00089	0,00729	0,00640	0,00640	0,00679	2,48034E-06	0,00157491
Germany	0,00074	0,00779	0,00705	0,00658	0,00688	2,94407E-06	0,001715829
Ireland	0,00002	0,00079	0,00076	0,00008	0,00004	3,79472E-08	0,0001948
Liechtenstein	0,00001	0,00278	0,00277	0,00020	0,00002	5,07798E-07	0,000712599
Luxembourg (Grand-Duché)	0,00105	0,02109	0,02003	0,01384	0,01377	2,3698E-05	0,004868057
Netherlands	0,00053	0,00108	0,00055	0,00080	0,00077	2,34836E-08	0,000153244
Northern Ireland	0,00005	0,00051	0,00045	0,00011	0,00009	1,21324E-08	0,000110147
Scotland	0,00080	0,00111	0,00031	0,00089	0,00086	6,65762E-09	8,15943E-05
Switzerland	0,00068	0,00083	0,00015	0,00078	0,00079	1,9596E-09	4,42674E-05

Prison population trends during the years 1993-2007 in Southern Europe

Figure 8 indicates that Spain and Italy have the biggest number of prisoners and that the number of Spanish prisoners has been growing steadily from the year 2001. Again, the situation changes quite radically when the prison populations are examined in relation to total populations: then Macedonia has much more prisoners than the other Southern European countries (Fig. 9). Understandably the numbers are so high when we think the situation in the times of former Yugoslavia, which was the name of Macedonia before. Total criminality (total recorded offences) increased in Spain during the years 1996-2007 about 30 % and in Italy about 20 %.





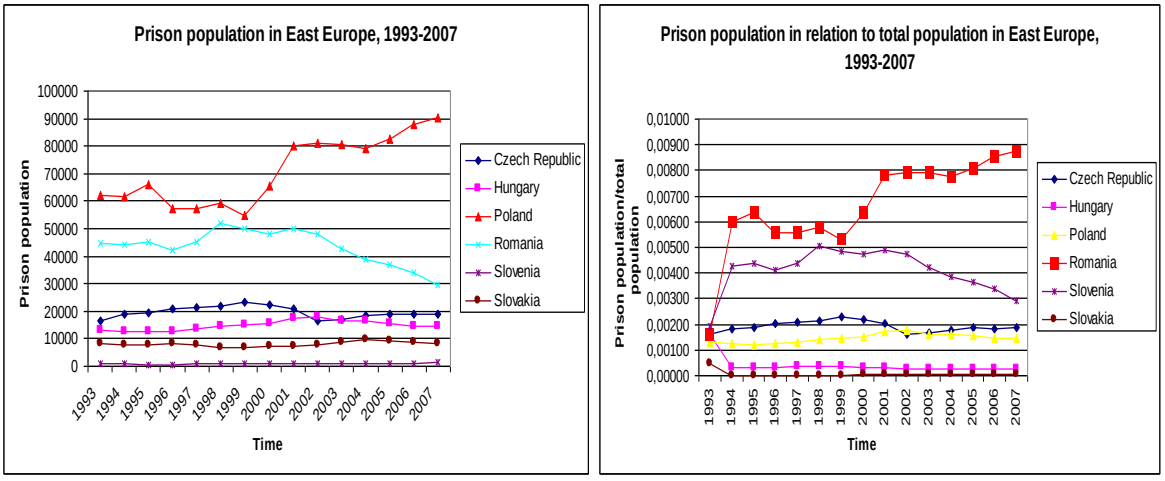
Figures 8 and 9. Prison population in Southern Europe, 1993-2007. Prison population in relation to total population in Southern Europe

Table 4. *Prison population in relation to total population in Southern Europe. Basic statistical analysis.*

	Min	Max	Range	Average	Median	Var	Standard deviation
Bulgaria	0,00023	0,00029	0,00005	0,00027	0,00028	1,59023E-10	1,26104E-05
Croatia	0,00180	0,00258	0,00078	0,00226	0,00234	6,54818E-08	0,000255894
Cyprus	0,00031	0,00364	0,00333	0,00078	0,00033	1,16388E-06	0,001078832
Greece	0,00002	0,00015	0,00013	0,00008	0,00006	1,52906E-09	3,91032E-05
Italy	0,00012	0,01185	0,01173	0,00903	0,01024	8,37971E-06	0,002894772
Macedonia	0,06137	0,09411	0,03274	0,08329	0,08402	6,44345E-05	0,008027109
Malta	0,00002	0,00309	0,00307	0,00023	0,00002	6,25061E-07	0,000790608
Montenegro	0,00031	0,00060	0,00029	0,00042	0,00042	7,83397E-09	8,85097E-05
Portugal	0,00007	0,00236	0,00229	0,00176	0,00181	2,4951E-07	0,00049951
Serbia	0,00048	0,02200	0,02152	0,01780	0,01896	2,6716E-05	0,005168755
Spain	0,00073	0,00085	0,00012	0,00077	0,00077	6,3852E-10	2,52689E-05
Turkey	0,00110	0,00151	0,00041	0,00124	0,00116	1,91001E-08	0,000138203

Prison population trends during the years 1993-2007 in Eastern Europe

The sample of Eastern Europe is limited for this trend analysis because the statistics of Eurostat consists of only six countries. Poland and Romania have had the biggest number of prisoners compared to the other Eastern European countries during the follow-up period but the prison population of Poland has increased its growth since the year 2000 while the prison population of Romania has decreased quite a lot (Figure 10). Interestingly the total crime rate has increased in Poland nearly 30 % and decreased in Romania over 10 % during the years 1996 -2007. However when the prison population is considered in relation to total population the prison population of Romania grows sharply (Figure 11).



Figures 10 and 11. Prison population in Eastern Europe, 1993-2007. Prison population in relation to total population in Eastern Europe.

Table 5. Prison population in relation to total population in East Europe. Basic statistical analysis

	Min	Max	Range	Average	Median	Var	Standard deviation
Czech Republic	0,00161	0,00227	0,00067	0,00192	0,00186	4,18244E-08	0,00020451
Hungary	0,00024	0,00161	0,00136	0,00039	0,00031	1,15131E-07	0,00033931
Poland	0,00121	0,00175	0,00055	0,00146	0,00146	3,16445E-08	0,000177889
Romania	0,00161	0,00877	0,00716	0,00662	0,00638	3,3457E-06	0,001829127
Slovenia	0,00194	0,00508	0,00314	0,00409	0,00425	7,12661E-07	0,000844192
Slovakia	0,00002	0,00049	0,00047	0,00006	0,00003	1,43516E-08	0,000119798

The prison population trends in the USA, Russia, South Africa, Turkey and Europe

The main trends of prison populations between U.S.A., Russia, South Africa, Turkey and Europe are presented in Figures 12 and 13. Figure 12 indicates that the prison population in USA has increased steadily and is expected to continue its growth. However, we know that in the year 2009 the growth stopped because of the economic depression (look at page 4). The situation is a bit different when the prison population is examined in relation to total population (Figure 13): the prison population has not increased so much. It seems that the prison population is related to the great number of immigrants. Canada has quite different criminal policy as compared to USA at least when the prison populations are concerned. Canada has a low rate of prison population – in fact it has the lowest average compared to the average prison populations of Russia, USA, South Africa, Europe and Turkey - and it is showing a downward trend, because the yearly average change was negative (Eurostat 2010).

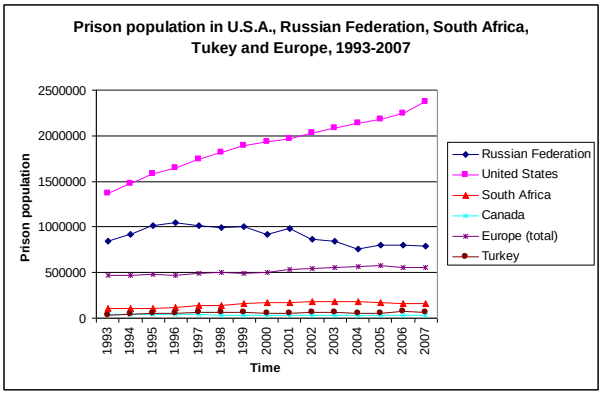
The criminal policy of USA differs also from that of Russia; Figure 14 indicates that the amount of prison population in relation to total population of USA is slightly increasing whereas the rate is decreasing in Russia. Kleyman (2011) nicely explains the moral climate and the prison-punishment system in Russia. After the collapse of communism, the Russian society changed dramatically. Many of the systems and infrastructures that provided social security were destroyed, law and order broke down resulting in the growing criminalization within the society. In Putin's era much of the political and financial power began to be controlled by people with a state security background. As a result in the 2000s crime in Russia has taken a sharp decline.

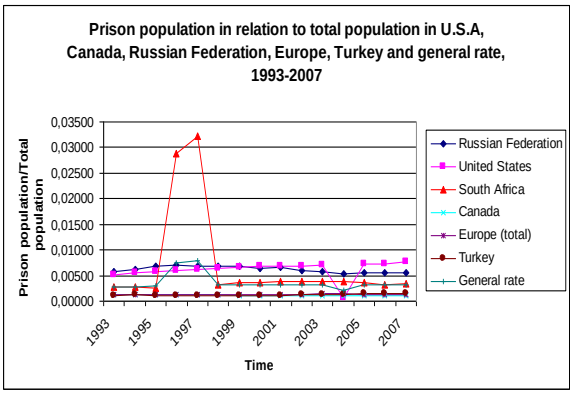
The number of prisoners in USA is huge: nearly 600 000 inmates return to their communities each year (see Farkas & Miller 2011, 342) and it has created the problem of recidivism because the reentry of prisoners is a difficult process. The study of Vieraitis, Kovandzic and Marvell (2007) demonstrated that although prison population growth seems to be associated with statistically significant decreases in crime rates, increases in the number of prisoners released from prison seem to be significantly associated with increases in crime. This is just what has happened in the USA.

Comparing the general European criminal policy to that of Turkey (Figure 16), we can see a difference: the amount of prison population in relation to total population is increasing in Turkey but not in European key countries. Turkey has a serious problem with a high rate of prisoners which is increasing explosively: yearly average growth is 6.7 % in 1993-2007. This means that it grows six times more than the total prison population of Europe (Eurostat 2010). One reason for this is that the Turkish political and economical system has been quite unstable until the end of 1980s, and the criminal policy of Turkey has been quite aggressive and punishing. Turkish society has been quite authoritarian where the army

has had great political power but in recent years some democratization process has been going on. Because of questionable human rights in Turkey there have also been much political prisoners. About 70 % of the Turkish population lives in urban centers and about 20 % of the population are of other ethnic groups than Turks – e.g. Kurds, Arabs and Romani people. There have been tensions between these ethnic groups. The assimilation rate has been quite low among these ethnic groups, but among the Turks the assimilation rate has been quite high. (Wikipedia/Turkey).

The results concerning the relation between criminality and prison population/total population in U.S.A., Russia, Europe and Turkey are presented in Figures 18, 20, 21, and 24. The trade-off analyses of criminality and prison population are more thoroughly analyzed elsewere (see Konttila & Kaivo-oja 2011). Interestingly, this study found three different kinds of prison population trends. These trends have different background criminality policy settings. First, one basic trend is: when total criminality increases, prison population increases. This is the case especially in Turkey. The 2nd basic model is: when criminality increases, prison population does not increase. The aggregated trend of European countries resembles this trend model. The 3rd alternative trend model is: the criminality decreases by increasing prison population. This is a consequence of the criminal policy model of the U.S.A.. In the U.S.A., law offenders are straightforwardly locked in jail in order to reduce the total criminality – and this connection is quite linear. This trend reminds also the policy of Russian Federation but the connection is not as straightforward in Russia as it is in the U.S.A.

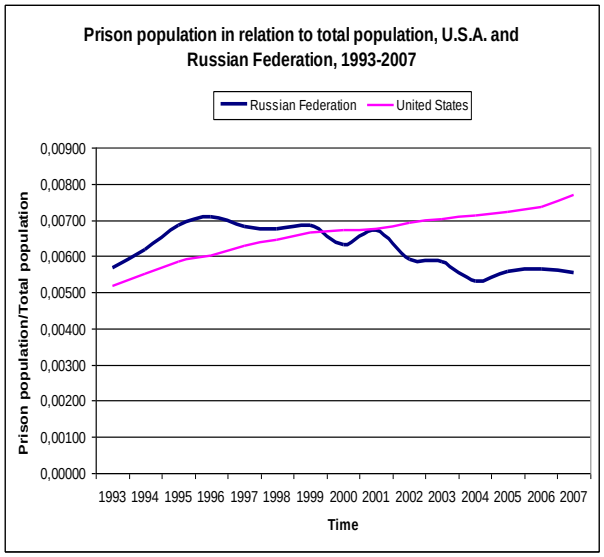


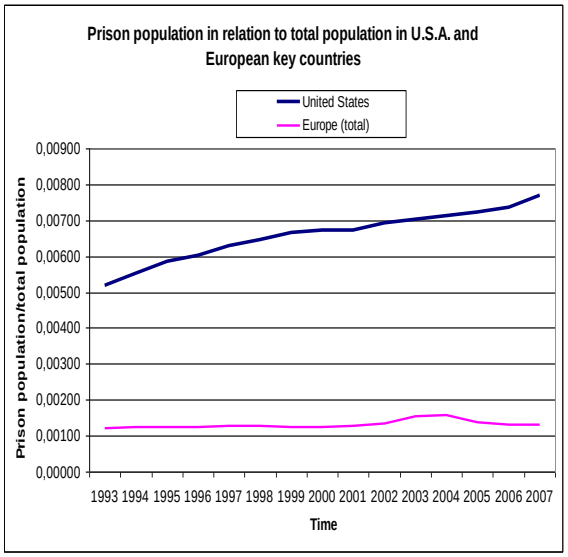


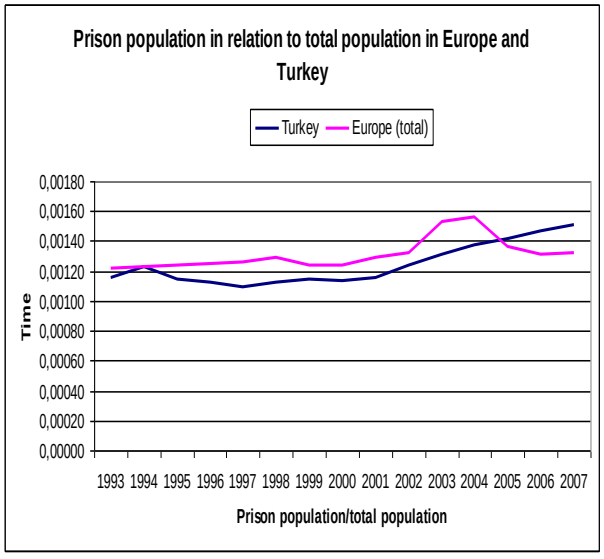
Figures 12 and 13. Prison population in the U.S.A., the Russian Federation, South Africa, Canada, Turkey and Europe, 1993-2007. Prison population in relation total population in the U.S.A., Russian Federation, South Africa, Canada, Turkey and Europe, 1993-2007

Table 6. *Prison population in relation to total population in in the U.S.A., the Russian Federation, South Africa, Turkey and Europe. Basic statistical analysis*

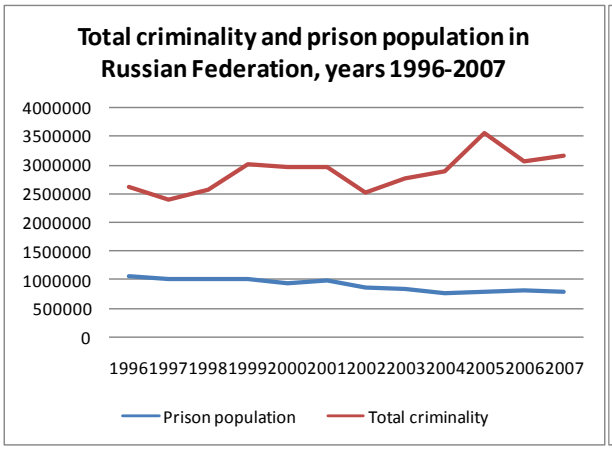
	Min	Max	Range	Average	Median	Var	Standard deviation
Russian Federation	0,00530	0,00709	0,00179	0,00620	0,00619	3,56553E-07	0,000597121
United States	0,00071	0,00770	0,00698	0,00616	0,00665	2,73742E-06	0,001654514
South Africa	0,00266	0,03224	0,02958	0,00705	0,00365	9,14614E-05	0,009563543
Canada	0,00105	0,00134	0,00029	0,00118	0,00116	1,09338E-08	0,000104565
Europe (total)	0,00121	0,00156	0,00034	0,00131	0,00129	1,07342E-08	0,000103606
Turkey	0,00110	0,00151	0,00041	0,00124	0,00116	1,91001E-08	0,000138203
General rate	0,00209	0,00798	0,00588	0,00365	0,00317	2,79874E-06	0,001672943

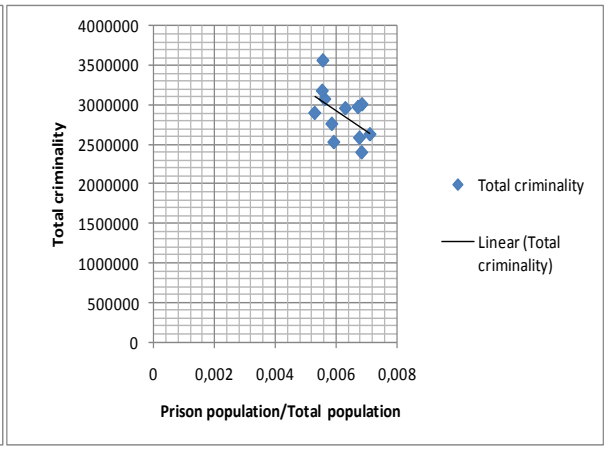




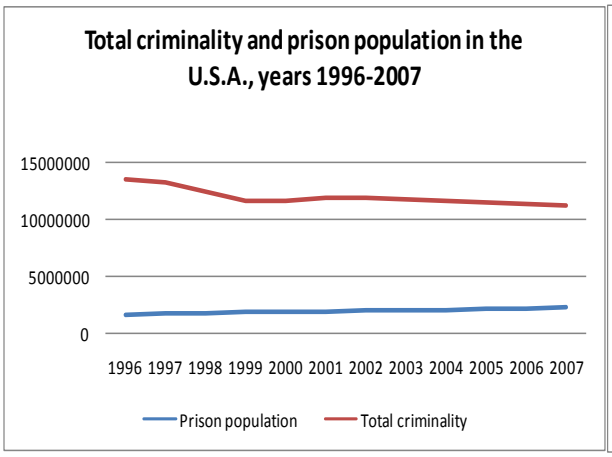


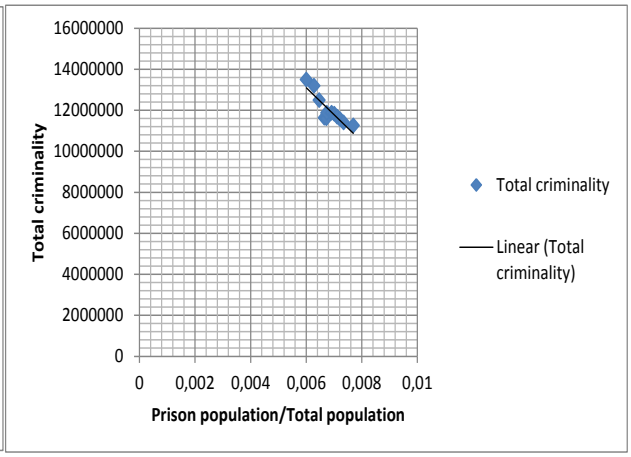
Figures 14, 15 and 16. Prison population in relation to total population in the U.S.A. and in the Russian Federation. Prison population in relation to total population, U.S.A. and European key countries and Turkey and European key countries.



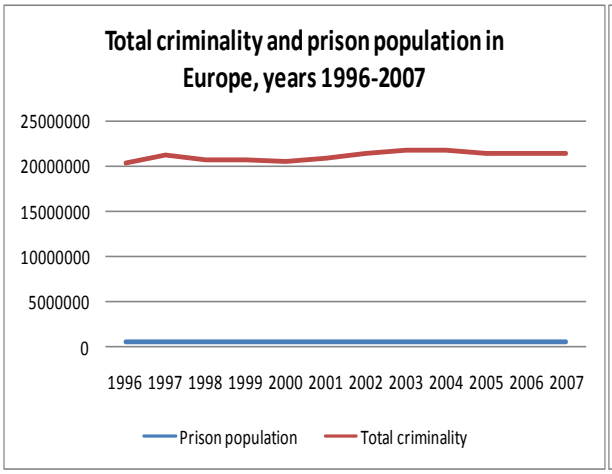


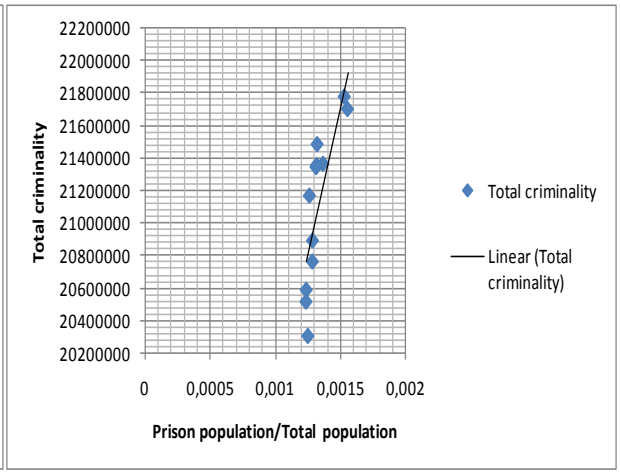
Figures 17 and 18. Total criminality and prison population/total population trade-off in the Russian Federation.



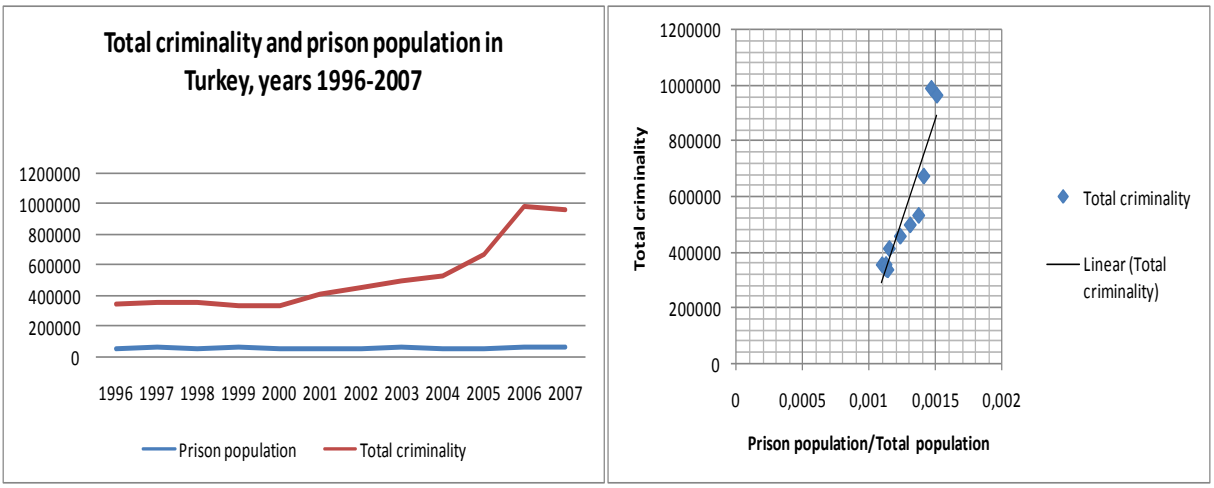


Figures 19 and 20. Total criminality and prison population in the U.S.A., years 1996-2007. Total criminality and prison population/total population trade-off in the U.S.A.





Figures 21 and 22. Total criminality and prison population in the U.S.A, years 1996-2007. Total criminality and prison population/total population trade-off in Europe



Figures 23 and 24. Total criminality and prison population in Turkey, years 1996-2007. Total criminality and prison population/total population trade-off in Turkey

Summary and security policy reflections

The trade-off relationship between total criminality and prison populations is a very complicated issue and varies between different countries as this study shows the issue. In this summary we do not repeat all the details of our research findings. There are some key findings which are summarized here.

First, our analysis tells that Turkey has a serious problem with a high rate of prisoners which is increasing explosively: yearly average growth is 6.7 % during the years 1993-2007. This means that it grows six times more than the total prison population of Europe. However, the rate of prisoners in Turkey may be changing to more positive direction, because of formal accession negotiations with the EU since 2005 and the Turkey has tried to change its policies towards the European model and standards. Increasing, quite alarming prison population/total trends were found also in Sweden, in Spain and also in Romania. Total prison population was increasing in a considerable way in the U.S.A., Poland, France and Northern Ireland. Generally, *it seems that a very high amount of immigrants is a very challenging security policy issues for the societies generally when the amount of criminality and prison population are considered*. The situation is quite different in the Baltic countries (Estonia, Latvia, Lithuania): the Baltic prison populations have decreased during the years 1993-2007, although especially drug trafficking crime has increased explosively.

In this comprehensive comparative trend analysis and security policy study we found three different kinds of prison population trends. These trends have different background criminality policy settings. First, Model Trend A, one basic trend is: *when total criminality increases, prison population increases*. This is the case especially in Turkey. The 2nd basic model, the Model B is: *when criminality increases, prison population does not increase*. The aggregated trend of the European member states reminds very much this kind of Trend Model B. However, it is to be noticed that the criminal policies varies quite a lot between some European countries. The 3rd alternative Trend Model C is: *the criminality decreases by increasing prison population*. This is a consequence of the criminal policy model of the U.S.A. In the U.S.A. law offenders are straightforwardly locked in jail in order to reduce the total criminality – and this connection is quite linear. This trend reminds us that the criminal policy of the Russian Federation,

but the connection is not as straightforward in Russia as it is in the U.S.A. One key scientific finding of this trend study is these three trend models. This finding implicates that *there are at least three different security policy models in the world* when we evaluate security policy from this perspective.

As a larger visual summary of prison population trends we can present baseline scenarios for large regions: U.S.A., Europe, the Russian Federation and Turkey till the year 2015. However it is to be noted that the statistical reliability of these statistics may vary between these countries. Last figure 25 indicates that in larger context prison population of the U.S.A. is going to grow unlike in Europe, Russia, the South-Africa, Canada, and even in Turkey. Thus the criminal policy of the U.S.A. differs quite a lot from the policy of the other larger countries/regions analyzed in this trend study. *Generally we can note that the changing demographic factors have also an influence on the criminality in the future*. For example, one key trend is that the population structure is coming older, which usually decreases the volume of criminality. *From this demographic perspective, we can expect a more secure world.*

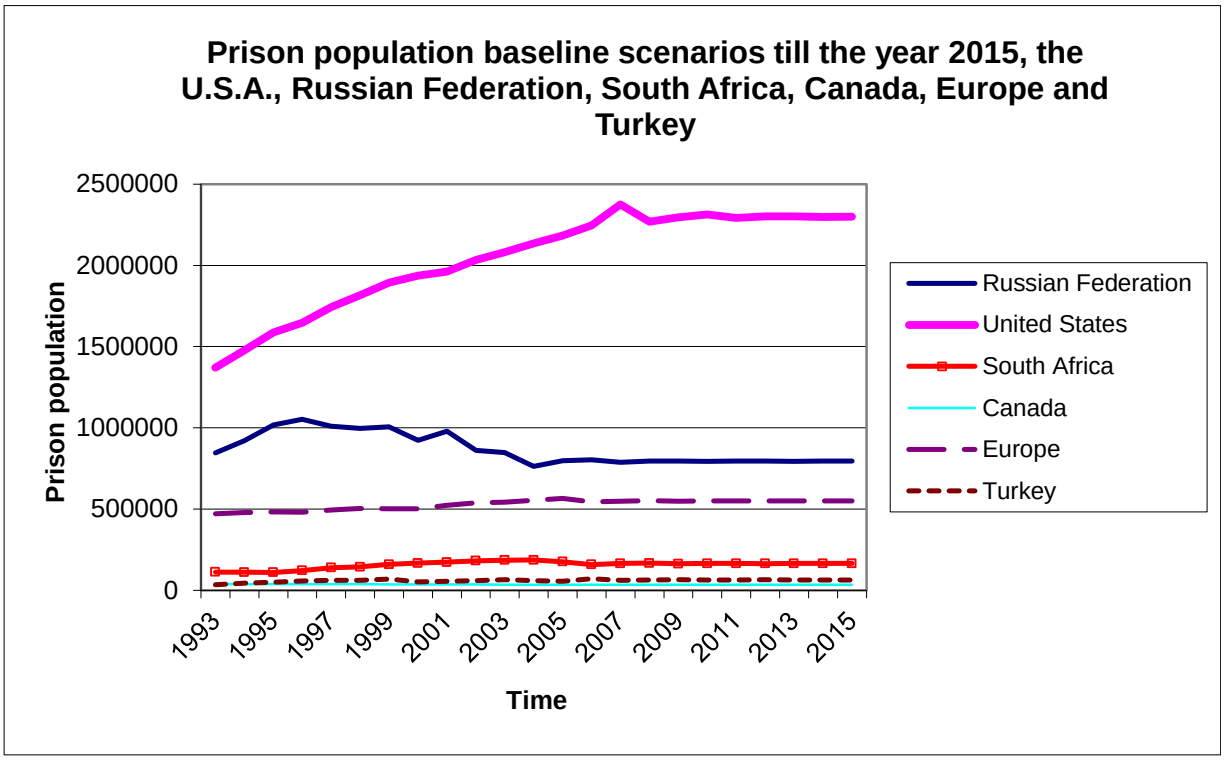


Figure 25. Prison population baseline scenario until the year 2015, the U.S.A., the Russian Federation, Canada, Europe, South Africa, and Turkey.

References

Allen, I.C., MacKenzie, D.I. & Hickman, I.J. (2001) The effectiveness of cognitive behavioral treatment for adult offenders: A methodological, quality-based review. *International Journal of Offender Therapy and Comparative Criminology* 45, 498-514.

Andrews, D.A.(1995) The psychology of criminal conduct and effective treatment. In J. McGuire (ed.) *What Works: Reducing Reoffending*. West Sussex, England: John Wiley & Sons.

Barnett, A. (1987) Prison populations: A projection model. *Operations Research*. Vol. 35. No. 1, 18–34.

Blom-Hansen, J. (2005) Principles, agents, and the implementation of EU cohesion policy. *Journal of European Public Policy*. Vol. 12, No. 2, 624-648.

Blumstein, A., Cohen, J. & Miller, H.D. (1980) Demographically disaggregated projections of prison populations. *Journal of Criminal Justice*. Vol. 8, 1-26.

Bures, O. (2006) EU Counterterrorism policy: A paper tiger? *Terrorism and Political Violence*. Vol. 18, 57-78.

Deams, T. (2008) Compatible victims? Prison overcrowding and penal reform in Belgium. International Journal of Law, Crime and Justice. Vol. 36, 153-167.

Eurostat (2010) *Crime and Criminal Justice. Database*. Crimes recorded by policy. Prison population. Web: http://epp.eurostat.ec.europa.eu/portal/page/portal/crime/introduction

Fábián, K. (2010) Mores and gains: The EU´s influence on domestic violence policies among its new post-communist member states. *Women Studies International Forum*. Vol. 31, 54-67.

Farkas, M. & Miller, G. (2011) Preliminary findings on the impact of reentry and reunification with family members. In I.O. Ekunwe & R.S. Jones (eds.) *Global Perspectives on Re-entry*. Tampere: Tampere University Press, 342-365.

Friedman, M. (1962) *Capitalism and Freedom*. Chicago: University of Chicago Press.

Gilinskiy, Y. (2006) Crime in contemporary Russia. European Society of Criminology, Vol. 3, 259-292.

von Hofer, H. (2003) Prison populations as political constructs: the case of Finland, Holland and Sweden. Journal of Scandinavian Studies in Criminology and Crime Prevention. Vol. 4, 21-38.

Holmes, L. (2009) Crime, organized crime and corruption in post-communist Europe and the CIS. *Communist and Post-Communist Studies*. Vol. 47, 265-287.

Konttila, A. & Holmalahti, T. (2009) Psykopaatti vankeinhoidossa. In H. Häkkänen-Nyholm.(ed.) *Psykopatia*. Helsinki: Edita, 246-270.

Konttila, A. & Kaivo-oja, J. (2011) Trade-off analyses of prison population and classified criminality rates in some European countries, including Turkey, the U.S.A., South Africa and Russia: integration or disintegration process in the global criminal policies? In I.O. Ekunwe & R.S. Jones (eds.) *Global Perspectives on Re-entry*. Tampere: Tampere University Press, 98-145.

Kleyman, M. (2011) Urban development, crime and re-entry: case Russia. In I.O. Ekunwe & R.S. Jones (eds.) *Global Perspectives on Re-entry*. Tampere: Tampere University Press, 78-97.

Lavenex, S. (2004) EU external governance in ´wider´ Europe. *Journal of European Public Policy*. Vol. 11, No. 4, 680-700.

Lerch, M. & Schwellus, G. (2006) Normative by nature? The role of coherence in justifying the EU´s external human rights policy. *Journal of Public Policy*. Vol. 13, No. 2, 304-321.

Liebling, A. (2006) Prison in transition. International Journal of Law and Psychiatry. Vol. 29, 422-430.

Loader, I. (2002) Policing, securization and democratization in Europe. *Criminal Justice*. Vol. 2., No. 2, 125-153.

Louks, N., Lyner, O. & Sullivan, T. (1998) The employment of people with criminal records in European Union. *European Journal on Criminal Policy and Research*. Vol. 6, 195-210.

Ochsen, C. (2010) Crime and labor market policy in Europe. *International Review of Law and Economics*. Vol. 30, 52-61.

Mauer, M. (2010) The causes and consequences of prison growth in the United States. *Punishment Society* 3, 9-20.

McGuire, J. (2003) Rikosten uusintariskin vähentämisessä käytettävät menetelmät – kansainvälisiä näkymiä. In R. Järvenpää & M. Kempas (eds.) *What works? Vankeinhoidon koulutuskeskuksen oppikirja* 1/2003. Helsinki, 68-106.

Stollmack, S. (1973) Predicting inmate populations from arrest, court disposition, and recidivism rates. *Journal of Research in Crime and Delinquency*, 141-162.

United Nations (2010) *World Populations by Country. Up to 2050*. United Nations. New York.

Vieraitis, L.M., Kovandzic, T.V. & Marvell, T.B. (2007) The Criminogenic effects of imprisonment: evidence from state panel data, 1974-2002. *Criminology & Public Policy* 6, 589-622.

Web: http://www.guardian.co.uk/world/datablog/2010/feb/01/united-nations-population-world-data.

Web: Luxembourg. http://www.en.wikipedia.org/wiki/Luxembourg, read 6.4.2011.

Web: Luxembourg. http://www.fi.wikipedia.org/wiki/Luxemburg, read 6.4.2011.

Web: Turkki. http://www.fi.wikipedia.org/wiki/Turkki, read 6.4.2011.

WHO (2004) *Global Status Report on Alcohol.* Department of Mental Health and Substance Abuse. Geneva: World Health Organization,

7. ENVIRONMENT, ENERGY AND CLIMATE CHANGE

CONTEXTUAL INSTABILITY: THE MAKING AND UN-MAKING OF ENVIRONMENT

Irina Comardicea & Achim Maas
Adelphi

ABSTRACT – *The environment and its resources are central to complex societies. Inadequate environmental governance may thereby lead to human suffering including armed conflict, while incapacity to adapt to environmental change has contributed throughout history to the collapse of complex societies. Environmental engineering technologies such as geo-engineering and synthetic biology add a new challenge by allowing modification from micro- to global scales at an unprecedented scope and pace. "Making our environment" is truer now than ever before, but unintentional and cascading consequences can also contribute to the unmaking of global society, if risks are not appreciated in advance.*

Introduction and Background

> *"International control of weather modification will be as essential to the safety of the world as control of nuclear energy is now" – Henry Houghton, chair of the MIT meteorology department, 1957*

Nobel-prize winner Paul Crutzen considered in 2000 the impact of human actions on the environment so profound as to constitute a new geological era, called the "anthropocene" (Dalby 2009: 99). While the exact starting date is debated, its defining quality is the historically unprecedented amount of environmental change as a consequence of human action. In the anthropocene the environment is no longer an independent background or simple context of human action: it has become a "matter of our own making" (Ibid.).

Modifying the environment according to some predefined specifications is not a new phenomenon, as illustrated by Houghton's quote above. Arguably, since agriculture has been invented, species bred and civilisation emerged, the environment has been constantly modified by, and for, humans (see Diamond 1999). What is different now, however, is the upsurge of the geoengineering debate in the past decade as well as advances in synthetic biology. The environment now seems to truly become a matter of our own making, as everything from microscopic scale to global weather systems could be consciously manipulated.

This paper will investigate how these types of manipulations affect our security in the long term. The environment and security interface on multiple levels: the role of the environment in questions of peace

and security has been repeatedly established (see e.g. UNEP 2009, WBGU 2007) and multiple studies have outlined how climate change may lead to future insecurity and instability by altering productive landscapes and negatively impacting human habitats (see WBGU 2007, Halden 2007, Carius et al. 2008). On the other hand targeting the environment in times of war or enlisting it as a weapon of war has an ancient history (Lockwood 2009), while fears of terrorist use of biotechnology have increased significantly with the anthrax attacks following the September 11, 2001 events (Monke 2004).

Against this background, the paper provides a conceptual overview to the potential implications of these environmental modifications from a security perspective. In section 2, the interface of security and the environment will be further elaborated in the context of the anthropocene and global environmental change. In sections 3 and 4, the emerging role, and potential risks, of geoengineering and synthetic biology as modification technologies will be highlighted. Although it is not an exhaustive review of the technologies, the paper discusses some policy conclusions in section 5.

Security and the Environment

Connecting security and environment via the term "environmental security" may be misleading – is it security of the environment or security from the environment? Without a clear reference object, the term security is meaningless (Buzan et al. 1998) as it depends strongly on the perspective and the reference object (cf. Dalby 1997). Security is additionally a term used to justify exceptional measures, such as sanctioning violence or cessation of rights, and labelling something a security issue may have significant consequences (Buzan et al. 1998). The term environmental security thus received much criticism, as it can distract attention from actual security concerns and/or may lead to the securitization or militarization of environmental politics (cf. Dalby 2002). From a terminological point of view, it is therefore more useful to keep security and environment apart.

At the beginning of the 21st century, the environment and security nexus can be discussed by studying two levels of interlinkages. The first is the interface level, where security and the environment are two distinct subjects. The second is the system level, where environment and security cannot be meaningfully separated. Each of these levels is reviewed below.

The interface level is useful to understanding how environmental issues and processes may lead to insecurity, which is here understood as violent conflict or related forms of human suffering. Past research shows that over 70 conflicts between 1980 and 2005 were related to renewable resources (Carius et al. 2006), while natural resources in general were implicated in approximately 40 percent of all armed conflicts since World War II (UNEP 2009).The studies focus in particular on ways in which either scarcity or abundance of resources may contribute to the outbreak, continuation or cessation of violent conflict (see e.g. Ross 2004; Homer-Dixon 1999). Indeed, in multiple conflicts in the past decades control over profitable resources such as diamonds, gold or oil has been a key driving factor. Additionally, violent conflicts may also be related to environmental destruction as a result of combat – which may be intentional, as in case of the use of Agent Orange during the Vietnam War – or unsustainable exploitation such as excessive logging to provide shelter to refugees (UNEP 2009).

Access to resources or environmental destruction however, is never the sole cause of conflict, but rather one aspect that may, to a lesser or greater degree, be implicated (WBGU 2007). Indeed, it can be argued that environmental and resource governance – the distribution of wealth from abundant re-

sources or allocation of scarce resources – are the actual core conflictive issues, and not the environment or resource availability per se. By comparing multiple cases across different regions, it becomes apparent that despite similarities in the respective environment/resource endowment, some tense situations escalate into violence while others do not (see e.g. Kahl 2005).

Yet the interface level is insufficient to grasp the deeper relationship between environment and security. Without agriculture, domestication of animals and cultivation of plants, there would be no complex society (see e.g. Diamond 1999), but it is unclear how to apply the term security in this context. Conversely, humanity has continued to shape the environment – thus the contemporary environment is in large part also the product of human action and rarely "natural" in a strict sense (cf. Dalby 2002, 2009). Climate change is the most clearly observable part of this process, and will leave no habitat or ecosystem untouched. It epitomises how societies and the environment are co-evolving, leading us to the "anthropocene" described above, where environmental change is largely driven by humanity (Dalby 2009).

The notion of the anthropocene and the view that security and the environment are constituent parts of a larger complex system are important to understanding how complex societies may collapse under environmental change: in contrast to the interface level mentioned above, security in this context is not only about human suffering or violent conflict, but about a form of "stability" – i.e. the continuation of the current socio-ecological patterns. Jared Diamond (2005) reviewed several historical examples where this pattern changed and societies ultimately collapsed; their way of living was inadequate for their (changed and changing) environment, the constituent parts mismatched and the pattern no longer stable. This may be the consequence of regional climate change or unsustainable development, as in case of the Easter Islands where ultimately no tree was left to sustain their culture (Ibid.). Interestingly, in most cases such societies collapsed because they focused on security and stability in a static sense, i.e. observing and preserving their practices and lifestyle when they were no longer viable. Or as Simon Dalby said: keeping things as they are when they no longer could stay as they are (cf. Dalby 2009).

The contrast then between the interface and systems levels is that in the former the connection between security and environment is spatially and temporally limited to a specific case. It is furthermore relatively direct, observable and traceable, as security relates directly to individuals or groups of humans, be it through frustration of their physical needs or as a result of armed conflict. Concurrently, a calamity such as a violent conflict is quite avoidable, as it is a result of ineffective, inequitable or uncooperative resource governance. This can all be changed and, consequently, terms such as "post-conflict reconstruction" apply and a positive, post-calamity situation can be created, all other things being equal.

On the complex systems level, however, insecurity may rather be seen as an existential challenge for a society, as it includes challenging its political, social, economic and cultural practices on a fundamental level. Post-calamity reconstruction would be impossible, because it would be unviable. Whatever the outcome of an event is when a society breaks down, the new society will look differently and adapt to the changed circumstances. Thomas Homer-Dixon (2005) coined the term "catagenesis" to describe this process: a combination of the terms catastrophe, which denotes the downfall of a society, and genesis, which denotes the creation of a new one after the downfall. This was the case on the Easter Islands, and is a process that has existed throughout history, with the rise and fall of civilisations.

The new quality of the anthropocene is that threats on the systems level are thereby globalised as well: a global society has been created, which interconnects every part of the world. Its demands are

equally staggering. Global population is likely to increase from seven to over nine billion by 2050. This, and currently further rising resource demands already create a series of interlocking resource challenges, where local events could have temporally and spatially dislocated impacts (cf. Lee 2009). A clear example for this is climate change, where activities by carbon-intensive societies will have disparate consequences around the world. The potential implications of such a change on a global scale have been outlined by multiple authors (see e.g. WBGU 2007, Halden 2007, Welzer 2008). The food crisis of 2008 exemplifies how loss of harvests and increased use of biofuels may affect food prices and lead to riots in distant countries (Maas et al. 2010). The global interconnectedness that comes with global society makes them also more susceptible to turbulences (Homer-Dixon 2005).

This global change may have impacts on both levels, with risks of increased conflict related to natural resources – among others due to governance systems incapable of anticipating the changes – or whole societies becoming unviable, as islanders may for example be forced to move thereby losing their collective identity.[1] On a global level some authors consider a "creeping social change" as adaptation to climate change inevitable (see Welzer 2008), while others already call democracy a failure and see a need for more authoritarian rule to cope with the challenges of climate change (see Shearmann/Smith 2007).

Changing Contexts: Making Environment

The aforementioned evolution of the environment is the sum and combination of intentional and unintentional modification events – such as agriculture or climate change. They have in common the incremental modification of the environment within certain parameters, such as livestock breeding over several generations and climate change resulting from two centuries of emissions. These changes are likely to increase and accelerate further, not least because of globally ongoing, carbon-intensive economic development. However, a new quality is now added, as technologies are becoming available to intentionally modify the environment *outside* of contemporary parameters. Of these, geo-engineering (or climate engineering) and bio-engineering signal challenges to come and will be discussed in greater detail below.

Geo-engineering and bio-engineering span two extremes of environmental modification, from large-scale, intentional manipulation of the non-living elements of the environment, in particular climate, to the engineering of biological resources. Geo-engineering is defined as large-scale (continental or global) intentional modifications to oceans, soils, and the atmosphere (ETC Group 2009). Techniques focus on managing solar radiation, removal (and storage) of carbon from the atmosphere, and weather modification (see e.g. Royal Society 2009).[2] In the last decade in particular these techniques have been proposed primarily to address the global problem of climate change, therefore large-scale impacts or benefits are desired. However, many assessments concede that most techniques that are able to deliver a high enough impact also carry with them high uncertainties of risk (Matthews and Turner 2009). Aside from

[1] In the Pacific island states, for instance, land is customarily owned and very closely connected to socio-cultural identity. Giving up land thus means giving up this identity as well (Carius/Maas 2009).
[2] Methods that might provide most benefits in the short-run include the injection of aerosol materials (such as sulphur) into the stratosphere, and increasing the reflectivity of the ocean by injecting bubbles on a large scale (MacCracken, 2009).

being technologically feasible[3], geo-engineering may be financially relatively 'cheap', compared with the scale of mitigation and adaptation costs: estimates for keeping global warming at <2°C has been estimated around US $6 billion per year (see Bickel/Lane 2009), while according to the UNFCCC costs for adaptation may be at least US $49 billion per year until 2030 (UNFCCC 2007).[4] It is important to note however, that such comparisons are difficult to make, since many costs may not be taken into account, and uncertainties and cascading effects may be overlooked.

Bio-engineering (or synthetic biology) on the other hand is applied in many different areas, from producing improved pharmaceuticals, food production, energy (biofuels) generation, to new plastics and materials (OECD 2009; EU 2005). Bio-engineering is defined as the making of things (improved or new) using biological pieces (Carlson 2010). The novel use and synergy of cells and organisms has been going on since the beginning of life on Earth, but what is now most interesting is the scale and intention of this genetic manipulation, which is unprecedented, and the scope of these endeavours: while parts of genes have so far been successfully introduced into organisms to encourage certain characteristics, scientists are now able to create an entire chromosome from scratch and endow it with tailored behaviours based on prior computer modelling (May 2009). The most recent feat of the J. Craig Venter Institute in fact successfully created an organism with no ancestor, whose DNA sequence was computer-designed.[5]

Bio-engineering is increasingly seen as future economic growth area, with some seeing already an emerging bio-economy (OECD 2009) on the horizon. However, the increase in the use of synthetic biology is not only driven by individuals empowered by a creative use of these technologies. There is in fact a growing demand for synthetic DNA and synthetic genes, a boom visible after the human genome was decoded in full in 1991, and highlighted by the size of the synthetic biology market, which was over US $200 million in 2008 (May 2009). Demand is driven by academic research institutions who use DNA parts, by companies who use synthetic biology to go beyond genetic engineering to increase the scope or efficiency of their work (i.e. creating designer enzymes), and by multinational biotech and pharmaceutical firms who are interested in these techniques for their own research and development work (May 2009). In contrast to the genetically modified organisms (GMO) which are mostly associated with transnational companies, synthetic biology has seen significant 'democratization' of its technologies and a move towards 'open source biology' (Schmidt et al., 2008). Skills can now diffuse through 'do-it-yourself' (DIY) blogs or groups, between amateurs, and bio-hackers. The DIY groups[6] – still a rather small community mainly active in the United States – were inspired by the International Genetically Engineered

[3] The unintentional modifications of the environment has already proven that human technologies and actions can have significant global impacts. Models and preliminary research also shows that new technologies such as ocean fertilization and increased desert reflectivity may indeed be feasible (see e.g. ETC Group 2009).
[4] It should be noted, that climate mitigation may have other benefits as well, such as reducing dependency on fossil fuel imports. Hence, making a complete simple cost-benefit analysis is difficult and has not been done yet.
[5] Please see the May 20, 2010 news in The Economist at
http://www.economist.com/node/16163006?story_id=16163006&CFID=138095936&CFTOKEN=20811879
[6] Examples include a woman who used a PCR machine purchased on eBay to decode her own genome in order to see whether she carried the gene for a disease her father has; or a computer programmer created glow-in-the-dark yoghourt in her San Francisco apartment and then moved on to a biosensor for the toxic contaminant in Chinese infant formula (Alper, 2009).

Machine (iGEM) project at MIT, which showcases the steadily accelerating ability of amateur scientists to create sophisticated biological project with very few resources[7].

Although there are clear differences in the scope, scale, and costs of geo- and bio-engineering, there are also several commonalities: they take an engineering approach to the environment, by dissecting their area of concern into basic components that can be separated, produced and assembled according to pre-defined properties, even though in both cases full understanding of the systems do not exist; both are converging technologies, combining areas such as chemistry, physics, engineering, biology, and information technology (see e.g. de Vriend in Torgersen 2009); both are working on environmental fundamentals, from climate to genes - together they cover the environment from the entire globe down to cells and viruses; at the same time, both are still very new technologies and their potential consequences are not fully known (Royal Society 2009; ETC 2007); their impacts may be unevenly distributed (in the case of geo-engineering, field testing may already have dramatic consequences (Royal Society 2009) and in the case of synthetic biology, while large-scale field tests are less of an issue, a community of so-called "bio-hackers" has emerged, i.e. people who conduct genetic engineering as hobby (Wall Street Journal 2009)); for both technologies international regulation has been called insufficient or absent altogether (House of Commons 2010; ETC 2009); concurrently both technologies – although viewed with fascination – received rather mixed or negative media attention, such as the focus on creating 'artificial' life (Torgersen 2009). Thus, the potential intentional and unintentional consequences of both technological areas require more scrutiny, which is discussed below.

Threats: Unmaking Environment

Bio- and geo-engineering both rely on the manipulation of elements that are part of a complex system (climate, biology), whose properties emerge not as a sum of its parts alone, but through interactions (cf. Gunderson/Holling 2002). As a result of these interactions a system develops equilibrium, i.e. fluctuations within certain parameters, which creates the stability of a system: it "behaves" along certain expectations, such as seasons or the Monsoon. Interactions are thereby networked, and changing one element has cascading impacts on all other parts of the system, to varying degrees. Geo- and bio-engineering both have the potential to upset this interaction of factors, by either introducing new elements or changing interactions within climate, biology, and the environment in general. As such, they may have cascading and unforeseeable impacts.

In the case of geo-engineering, solar radiation management may lead to significant and unpredictable changes in Monsoons (Royal Society 2009). Ocean fertilization may also carry with it potential side effects such as a decrease in oxygen and a resulting increase in methane emissions, or significant changes in the microbiological composition and productivity (Keith 2000). Thus, geo-engineering may fix one problem to create yet another problem, leading to a cascade of issues. Additionally, if they are chose as a solution to climate change global geo-engineering systems must be put in place and continuously maintained. If such systems should be crippled it could lead back to rapid global warming, with disastrous

[7] For more information on iGEM please see http://2010.igem.org/Main_Page

associated consequences given the little time left for adapting or building a new system (Brovkin et al. 2009).

A particular concern regarding synthetically created organisms is that they may leak into the environment from the safety and security of laboratories. If they then undergo mutations and become established in resident natural populations, they may cause unknown harm (Kaebnick 2009). The history of unintended damage caused by invasive species is an example of how unknown and potentially unstable consequences are proportional to our knowledge of the system upon which we are acting: the less complete our understanding of the system the greater the potential for "undesirable or unforeseen environmental" impacts (Matthews and Turner 2009).[8] The democratisation of biotechnology – including rapidly decreasing costs and availability of equipment and knowledge to a vast array of organisations, small companies and individuals – accentuates this concern.

A further concern, often cited by both supporters and sceptics of geo- and bio-engineering, regards dual-use: it is conceivable that states, non-state groups, or even individuals, could apply a number of environmental modification techniques for hostile purposes. For instance, the genetic makeup of the most dangerous agricultural pests have been decoded, which can help to gain insights to prevent catastrophic outbreaks, but can also be used to develop new pathogens (Casagrande 2000).[9] Additionally, nearly all of the materials and equipment used to cultivate biological warfare agents have commercial applications in the production of beer, wine, food products, animal feed supplements, bio-pesticides, vaccines, and pharmaceuticals (Tucker 1996).

Indeed, if terrorists chose to target agriculture, a pathogen could easily be found and synthesized to suit the target crops, or an entirely new organism could be created from scratch (Kaebnik 2009). Although most existing pathogens would need to go through a complex process of development, production, weaponization, and delivery in order to cause mass casualties (with the exception of the smallpox and 1918 influenza viruses) these processes would not necessarily be needed if agricultural crops were targeted (Vogel 2006). However, taking into consideration past examples and the still-significant technical obstacles for using these techniques, many studies seem confident that they could become a threat only at the state level; non-state actors thus, even those considering a bioterrorist attack, may still prefer to use traditional biological warfare agents (Kelle 2009). Bio-engineering security concerns thus may not be so much over individuals and non-state groups, but rather over the business industry. Several companies throughout the world are already working on producing synthetic DNA pieces (oligonucleotides), and as their size and complexity increases they will be theoretically able to manufacture any virus, including toxins and biological agents (Ibid.). These companies are already working together to create and check through databases before an order is placed, meaning they would receive an alarm if a potentially dangerous DNA sequence had been ordered. However, due to the increasing complexity of the genetic

[8] For instance, when the cane toad was introduced to Queensland, Australia in 1929, the intended effect was that it would act as an insect control. Unsuccessful in this respect, the toad now threatens a number of native species (Matthews and Turner 2009).

[9] Researchers in Brazil for example, have sequenced the genome of citrus variegated chlorosis (*X. fastidiosa*), whose strains cause disease in a variety of agricultural plants such as alfalfa, grapes, coffee, and stone fruit (Casagrande 2000).

parts able to be manufactured, it is becoming very difficult to pick out the dangerous sequences, and to create a detailed enough definition of what is dangerous (May 2009).

In the case of geo-engineering many technologies have military applications and concerns focus on states (or potentially also corporations): given its relative financial and technological feasibility, unilateral efforts may be attempted by single, less affluent countries to use technologies either as a global solution to climate change or for regional protection from climate change impacts (Ricke et al. 2009). However, the climate is indivisible and global, thus unilateral attempts would have major repercussions and could be considered as hostile acts. Gwynne Dyer (2008) explores the possibility that a country severely threatened by climate change may resort to desperate measures and even threaten countries with carbon-intensive economies into acting or fearing consequences. While protecting the environment and preventing climate change currently appear to be globally agreed-upon goals, the introduction of large-scale geo-engineering, climate variability and instability, and similar impacts may lead to creeping changes of values and perspectives (see Welzer 2008) – making the environment a target and a weapon alike: With environmental modification becoming pervasive politically, economically and increasingly accepted socially, it may also become a focus for military use and targeting – as did "cyberwar" before. A well-known example of environmental warfare using Agent Orange occurred during the Vietnam War, but a less well-known example of geo-engineering occurred at the same time: the United States carried out a campaign of cloud seeding during that war, with a budget of more than US $3 million per year. The negative public reaction to the war also extended to this effort, and lead to the international treaty of 1972, ENMOD, or the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (Keith 2000). Still, both geo-engineering and bio-engineering fall into gray legislative areas due to their dual-use purpose. The ENMOD treaty only has 75 ratifications and the past decade has seen deterioration and crises of several arms control treaties.

Discussion and Conclusions

The *anthropocene* is our new era in which direct human action is a major driving force in global environmental change. Historically, complex societies could only thrive on a suitable environment and would collapse if they were unable to adapt to environmental change. On a local level, inequitable and ineffective environmental and resource governance along with unsustainable development may also lead to conflicts over resources and very direct human suffering. A major challenge is thereby the inflexibility to change and adapt. Keeping things as they are even as they continue to change is impossible when the environment created by human action no longer supports current social, political and economic practices.

The fact that environmental modifications – such as geo-engineering and bio-engineering – are increasingly discussed, practiced and accepted pushes the anthropocene to a new level of potential instability by allowing changes outside of conventional parameters and on unprecedented scales. In the long-term, a major mismatch of geo-engineering and bio-engineering are their underlying intentions: geo-engineering focuses on nullifying climate change impacts, essentially a technology fix trying to keep the climate as it is; bio-engineering meanwhile is attempting the opposite, creating new organisms never seen before, engendering change. The major policy challenge is the view of environment as an external issue to be engineered, and not as an intimately co-evolving part of society. As a result, significant

threats of cascading, unexpected problems were discussed above, which may destabilise environmental processes and, by extension, societies.

Both ongoing, often unintended, environmental change as a result of human action, as well as intentional and targeted environmental manipulation, may lead to unpredictable environmental changes for which current societies are no longer prepared to adapt. This may also increase the risk of catagenesis: a calamity that leads to the collapse of the current complex global society, and the potential creation of a new society thereafter. Such events tend to significantly reduce social complexity and be accompanied by a violent release of energy as well (see Homer-Dixon 2005; Diamond 2005).

Governance, legislation and regulation of these modification technologies, such as via the ENMOD treaty, are currently insufficiently developed to accommodate the upcoming challenges. Furthermore, regulations have a tendency to be too rigid and inflexible: the Law of the Sea is a good example, as climate-induced sea-level rise is not covered and will raise serious future legal questions (Maas et al. 2010). Principles and codes of conduct[10] guiding behaviour may be more appropriate, as flexibility will be needed to adapt to ongoing environmental change. The precautionary principle should, however, be central to the debate – it is currently insufficiently discussed at international conferences such as the 2010 Asilomar International Conference on Climate Intervention Technologies.[11] To slow down the process and give more time for consideration and preparation, a moratorium on experiments have been suggested by a number of scientists to further research unintended consequences (e.g. ETC 2009). However, this requires a coordinated effort, particularly regarding monitoring and enforcement. Given the economic role of bio-engineering as an emerging sector, the Organisation for Economic Co-operation and Development as well as the G20 may be suitable fora for discussing these issues. The global nature and risks involved in geo-engineering, however, commands a debate within the UN General Assembly.

In conclusion a governance approach is needed, as it becomes clearer that trying to keep things as they are – an implicit key aspect of security – is not a sustainable option. Instead, it is likely that a transition will occur as a result of ongoing (and potentially accelerated) environmental change. The aim must be to identify where this transition may lead to frictions – where environment and security interfaces – and where it threatens to uproot societies. A set of social, political and economic practices that are capable to sustain rapid change and to adapt accordingly should be the focus of policy-makers.

References

Alper, Joe 2009: Biotech in the basement. Nature Biotechnology 27, no. 12: 1077-1078.

Baldwin, Daniel A. 1997: The Concept of Security. In: Review of International Studies 23:1, 5-26.

Bickel, J. Eric and Lee Lane 2009: An Analysis of Climate Engineering as Response to Climate Change. Frederiksberg: Copenhagen Consensus Center.

[10] However, a code of ethics in the bio-engineering community, similar to the one in the computer hacking community, provides no guarantee that dangerous intentional or unintentional products (such as malware for the computer hacking industry) would not result (Schmidt 2008).

[11] This conference mirrors the 1975 Asilomar Conference on Recombinant DNA, which focused on voluntary guidelines and a researcher-based code of conduct. For more information see http://www.climateresponsefund.org/index.php?option=com_content&view=article&id=136&Itemid=83

Brzoska, Michael 2008: Der konfliktträchtige Klimawandel – ein Sicherheitsproblem? In: Andreas Heinemann- Grüder, Jochen Hippler, Markus Weingardt, Reinhard Mutz und Bruno Schoch (eds) 2008: Friedensgutachten 2008. Münster: LIT, 195-206.

Buzan, Barry, Ole Wæver and Jaap de Wilde 1998: Security. A New Framework for Analysis. Boulder and London: Lynne Rienner.

Brovkin, Victor, Vladimir Petoukhov, Martin Claussen, Eva Bauer, David Archer and Carlo Jaeger 2008: Geoengineering climate by stratospheric sulphur injections: Earth system vulnerability to technological failure. In: Climate Change 92, 243-256.

Carius, Alexander and Achim Maas 2009: Climate Change and International Security. Technical Report. London: HTSPE.

Carius, Alexander, Dennis Tänzler and Achim Maas 2008: Climate Change and Security – Challenges for German Development Cooperation. Eschborn: GTZ.

Carius, Alexander, Dennis Tänzler und Judith Winterstein 2006: Weltkarte von Umweltkonflikten – Ansätze einer Typologisierung. Externe Expertise für das WBGU-Hauptgutachten: „Welt im Wandel: Sicherheitsrisiko Klimawandel". http://www.wbgu.de/wbgu_jg2007_ex02.pdf (3. August 2007).

Carlson, Robert 2010: Biology is Technology: the promise, peril, and new business of engineering life. Cambridge: Harvard University Press.

Casagrande, Rocco 2000: Biological Terrorism Targeted at Agriculture: The Threat to US National Security. The Nonproliferation Review.

Dalby, Simon 2009: Security and Environmental Change. Cambridge: Polity.

Dalby, Simon 2002: Environmental Security. Minneapolis: University of Minnesota Press.

Diamond, Jared 2005: Collapse. How societies choose to fail or survive. London: Penguin Books

Diamond, Jared 1999: Guns, Germs and Steel. New York: Norton.

Dyer, Gwynne 2008: Climate Wars, Toronto: Random House Canada.

ETC 2007: Extreme Genetic Engineering. An Introduction to Synthetic Biology. Available at http://www.etcgroup.org/upload/publication/602/01/synbioreportweb.pdf (22 April 2010).

ETC 2009: Retooling the Planet? Climate Chaos in the Geoengineering Age. Available at http://www.etcgroup.org/en/node/4966 (2 May 2010).

European Commission 2005: Synthetic Biology. Applying Engineering to Biology. Report of the NEST High-Level Expert Group. European Commission: Brussels.

Gunderson, Lance H. and C.S. Holling (eds) 2002: Panarchy. Understanding Transformations in Human and Natural Systems. Washington et al.: Island Press.

Halden, Peter 2007: The Geopolitics of Climate Change. Challenges to the International System. Stockholm: FOI.

Homer-Dixon, Thomas 2005: The Upside of Down. Catastrophe, Creativity and the Renewal of Civilisation. Washington et al.: Island Press.

Homer-Dixon, Thomas F. 1999: Environment, Scarcity and Violence. Princeton: Princeton University Press.

House of Commons 2010: The Regulation of Geoengineering. London: The Stationary Office.

Kaebnick, Gregory, E. 2009: Should moral objections to systhetic biology affect public policy? Nature Biotechnology 27, no. 12: 1106-1108.

Kahl, Colin 2005: States, Scarcity and Civil Strife in the Developing World. Princeton: Princeton University Press.

Keith, David, W. 2000: Geoengineering the Climate: History and Prospect. Annual Reviews of Energy and Environment 25: 245-84.

Kelle, Alexander. 2009: Ensuring the security of synthetic biology - towards a 5P governance strategy. Systems and Synthetic Biology 3: 85-90.

Lee, Bernice 2009: Managing the interlocking climate and resource challenges. In: International Affairs 85:6, 1101-1116.

Lockwood, Jeffrey A. 2009: Six-legged Soldiers. Using Insects as Weapons of War. Oxford: Oxford University Press.

Maas, Achim, Chad Briggs, Vicken Cheterian, Kerstin Fritzsche, Bernice Lee, Cleo Paskal, Dennis Tänzler and Alexander Carius 2010: Shifting Bases, Shifting Perils. A Scoping Study on Security Implications of Climate Change for the OSCE Region. Berlin: Adelphi Research.

Matthews, H Damon, und Sarah, E. Turner 2009: Of mongooses and mitigation: ecological analogues to geoengineering. Environmental Research Letters 4.

May, Mike 2009: Engineering a new business. Nature Biotechnology 27, no. 12: 1112-1120.

Monke, Jim 2004: Agroterrorism: Threats and Preparedness. CRS Report for Congress. Washington: Library of Congress.

OECD 2009: The Bioeconomy to 2030. Designing a Policy Agenda. Paris: OECD.

Ricke, Katherine, M. Graner Morgan, Jay Apt, David Vctor and John Steinbrunner 2008: Unilateral Geoengineering. Non-Technical Briefing Notes for a Workshop at the Council on Foreign Relations, Washington DC, May 05, 2008. Wahsington: Council on Foreign Relations.

Royal Society 2009: Geoengineering the Climate. Science, Governance and Uncertainty. Available at http://royalsociety.org/WorkArea/DownloadAsset.aspx?id=10768 (17 December 2009).

Schmidt, Markus. 2008: Diffusion of synthetic biology: a challenge to biosafety. Systems and Synthetic Biology 2: 1-6.

Schmidt, Markus, Helge Torgersen, Agomoni Ganguli-Mitra, Alexander Kelle, Anna Deplazes, und Nikola Biller-Andorno 2008: SYNBIOSAFE e-conference: online community discussion on the societal aspects of synthetic biology. Systems and Synthetic Biology 2: 7-17.

Shearman, David and Joseph Smith 2007: The Climate Change Challenge and the Failure of Democracy. Westport: Praeger.

Torgersen, Helge 2009: Synthetic biology in society: learning from past experience? Systems and Synthetic Biology 3: 9-17.

Tucker, Jonathan, B. 1996: Chemical/Biological Terrorism: Coping with a New Threat. Politics and the Life Sciences 15, no. 2: 167-183.

UNEP 2009: From Conflict to Peacebuilding. The Role of Natural Resources and the Environment. Nairobi: UNEP.

UNFCCC 2007. Investment and Financial Flows to Address Climate Change. Bonn: UNFCCC.

UNPD 2008: World Population Prospects. The 2008 Revision. Available at http://esa.un.org/unpp/ (4 January 2010).

Vogel, Kathleen 2006: Bioweapons Proliferation: Where Science Studies and Public Policy Collide. Social Studies of Science 36, no. 5: 659-690.

Wall Street Journal 2009: In Attics and Closets, 'Biohackers' Disvoer Their Inner Frankenstein. 12 May 2009, available at http://online.wsj.com/article/SB124207326903607931.html (22 April 2010).

WBGU 2007: World in Transition – Climate Change as a Security Risk. Berlin and Heidelberg: Springer.

Welzer, Harald 2008: Klimakriege. Wofür im 21. Jahrhundert getötet wird. Berlin: Fischer.

Wheelis, Mark 2004: Will the New Biology Lead to New Weapons? Available at http://www.armscontrol.org/act/2004_07-08/Wheelis (16 April 2010).

Wolinsky, Howard 2009: Kitchen biology. European Molecular Biology Organization 10, no. 7: 683-685.

NETWORKS OF POWER: DEVELOPMENT BANKS AND ENERGY SECURITY IN THE MEKONG REGION

Hanna Kaisti & Mira Käkönen
Finland Futures Research Centre, University of Turku
E-mail: hanna.kaisti@utu.fi

ABSTRACT *– Decisions and investments in energy sector are frequently justified in terms of achieving energy security. The concept energy security originates from the concerns generated by the first oil crisis (1973-74) and it basically refers to sufficient supply in affordable prices. Since then energy security has maintained to be a dominant energy policy objective and an important tool of justification for governments throughout the world. Less frequently there are questions raised on energy security for whom and with what kind of environmental and social consequences. In the era of climate crisis these questions are becoming more and more significant and especially in the development context issues related to pro-poor energy decisions are gaining importance.*

Development banks are major actors in defining and implementing global energy governance. They are involved in the financing of energy sector and defining priorities in most developing and transition countries where the energy demand is growing rapidly. This paper analyses, firstly, the development of World Bank's and Asian Development Bank's energy agenda and their understanding on energy-security-development nexus from 1980s to 2010. Secondly, the paper discusses how the banks energy agenda is implemented in practice in the Mekong Region in Southeast Asia. The focus is mainly on large-scale hydropower, which is the energy source with most regional relevance in the area.

Introduction

Energy policies, systems and technologies are the product of complex power play between divergent actors and their interests. The energy production and distribution choices are political but usually they are rendered technical and administrative. The pursuit of energy security has become a dominant energy policy objective and political tool for governments throughout the world. The way in which energy security is understood affects the way in which countries argue and formulate their energy policy. In its basic and most traditional form energy security refers sufficiency of supply in affordable prices. This understanding of energy security remains to be the core of energy security thinking, even though in the past decades the understanding of energy-security nexus has changed, mainly because climate concerns have entered into the energy agenda.

In the developing countries the development banks such as World Bank and Asian Development Bank (ADB) have become major actors in defining priorities in the energy sector of the recipient countries. Due to high investment costs in the energy sector, the development banks are powerful players in

building energy sector in many developing countries. Therefore, the energy policies that the development banks are promoting and the projects and programs they are financing have long term impacts on different levels, from local communities to states, regions and even the globe as a whole. This paper analyses the development of World Bank's and ADB's energy policy discourses and the implementation of their energy agenda in the Mekong region in Southeast Asia. The paper begins by examining the development of World Bank's and ADB's energy policies from 1980s to the present. The analysis focuses on the discursive turns in the development banks' energy policies.[1] By discursive turn we refer to major changes in their argumentation on how energy production and distribution should be organised and the reasoning why the selected solutions are superior to others. The latter part of the paper gives examples on how World Bank and ADB have implemented their energy policy in concrete energy programs and projects in the Mekong region. We will mainly focus on large-scale hydropower, which in the Mekong Region is the energy source with most regional relevance.

Energy-Security-Development Nexus

The pursuit of *energy security* is a dominant policy objective and political tool for governments throughout the world. The obvious reason for this is a strong link between energy and national security, as energy is vital for the functioning of the state. There is no internationally agreed definition of the term energy security, and the way in which countries, organizations and institutions have defined has changed over the years. In its basic and most traditional form energy security refers to security of energy supply, that is, *sufficiency of supply at affordable price*.[2] It is commonly thought that any longer interruption of a steady and plenty flow of energy would massively harm a nation's economic output, political stability and the personal wellbeing of its citizens. Therefore, a country is understood to have energy security if it is protected against shortages of affordable fuel and energy resources. (UNESCAP 2008, 3-4; Baumann 2008, 4) Energy security thinking is mostly centred on *national* energy security; how a state can guarantee the flow of cheap energy. Energy security is dictated by state's energy supplies, the infrastructure required for producing, distributing and storing the energy, and the associated costs to the consumers.

The first oil crises of 1973-74 often mark the beginning of the international energy security concern. In the early-1970s oil crises and Arab oil embargo was seen as a threat to energy security because oil supply was heavily dependent on the politically volatile Middle East. The International Energy Agency (IEA) was established during oil crises of 1973-74 to ensure reliable, affordable and clean energy to industrialized countries. The initial role was to co-ordinate measures in times of oil supply emergencies.[3] (Yergin 2006) Later the international discussion on threats to energy security shifted from concerns over

[1] Energy policy papers analysed in this research include: ADB's First Energy Policy, 1981; WB's Energy Policy, 1993; ADB's Energy Policy, 1995; WB's Energy Policy, 2002; ADB's Revision of Energy Policy, 2000; WB's Renewable Energy Policy, 2004; ADB's Third Energy Policy, 2009; WB's Energy Guidelines for East Asia and SEA (middle income countries), 2010.

[2] However, the way in which energy security is conceptualized depends on national and regional circumstances. For countries with their own resources, energy security involves the capacity to cope with changes in energy supplies using their own resources, while countries with fewer resources will be looking for reliable external supplies. Energy-exporting countries, on the other hand, will be looking for security in demand, from a stable energy market.

[3] As energy markets have changed, IEA's mandate has broadened to incorporate energy security, economic development and environmental protection. (Yergin 2006; IEA's web pages: www.iea.org)

oil embargo of oil exporting countries to anxiety over whether or not there are sufficient fossil fuel resources to meet the world's energy requirements in the decades ahead. (Yergin 2006) Widely fluctuating oil and gas commodity prices have impacts on all world economies, but particularly developing countries. Low income economies that import fossil fuels are particularly vulnerable to price increases, which can badly affect their balance of payments and increase their vulnerability. Furthermore, the energy demand is growing in the Global South, which makes the issue even more severe. There are several, often interrelated reasons for the growing energy demand, especially in the newly developed countries. Industrialization, urbanization, population growth, transfer of industrial production from the Western countries to Asia, rural electrification schemes all contribute to this development, even though the main drivers for increasing energy consumption vary from country to country.

While there is no doubt that states have certain minimum energy requirements, the rhetoric of energy security has often been used to pursue centralised industrialisation and large scale energy projects at the expense of other considerations. Large hydropower projects, gas pipelines and construction of nuclear power plants in the name of energy security and development are rarely vetted through a process of environmental or social impact assessment. (Simpson 2007, 539)

Three discursive turns in World Bank's and ADB's energy policies

In the global South development banks such as World Bank and ADB have become powerful actors in building energy sector. The reasons for this relate to high investment costs in energy infrastructure planning and construction, often low capacity and weak policy and governance framework in the recipient countries. Therefore the energy policies that the development banks are promoting have long term impacts on many developing countries and regions, and on global climate. World Bank and ADB are important creditors in Asia and the bulk of their lending goes to governments in form of project- or programme-based lending. They enjoy great leverage and influence by virtue of their superior credit rating and close cooperation with governments. The development banks' decisions on project lending, financial guarantees and promotion of best practices have enormous influence on the energy strategies and policy choices of the recipient countries, but it also has impact on global energy governance agenda. They have become part of global energy governance structure as economic and technical assistance projects and programs both reflect and shape global agendas on how countries should develop their energy structure and run their economies and what paths they should follow to promote economic development. (Florini 2009)

Besides lending, the development banks give technical assistance, training, policy dialogue, and evaluation, which are especially linked to transferring certain ideas, concepts, practices, and values to the recipient countries. Therefore it is important to analyse the energy discourses the banks are using.[4] Discourses frame certain problems, that is to say they distinguish some aspects of a situation rather than others. The ideas, concepts and categories that constitute a discourse can vary in character: they can be normative or analytic convictions; they can be based on historical references, or they can for instance

[4] There are numerous definitions for a discourse. For example, Maarten Hajer has defined discourse as an ensemble of ideas, concepts and categories through which meaning is given to phenomena. (Hajer 1993, 45; see also Hajer 1995; Hajer 2003)

reflect myths about nature. Discourse provides the tools with which problems are constructed. Discourse at the same time forms the context in which phenomena are understood and thus predetermines the definition of the problem. (Hajer 1993, 45; Hajer 2003) The development banks' energy discourses have gone through several changes in terms of what is defined to be the problem and how it should be solved. Also understanding of energy security has extended during the past three decades.

World Bank's and ADB's first policies reflected the fears that the first oil crisis of 1973-74 had caused. ADB's first Energy policy paper was published in 1981 and focused on overcoming the oil crisis. (ADB 1981) According to ADB there was a need *for large investments to meet the energy requirements* of rapidly growing economics in the developing member countries. ADB's response was to finance and build energy infrastructure in the client countries. As a result, the Bank's average annual lending in the energy sector increased rapidly from $0.5 billion in the early 1980s to $1.7 billion in the early 1990s. (ADB 1995) Most World Bank's and ADB's energy projects in 1980s and 1990s related to infrastructure construction such as building dams and extending transmission lines. However, at the discourse level in 1990s the development banks' energy discourse went through major changes. First, the banks began to push recipient governments to privatize the energy sector and increase regional electricity trade. This can be seen as first discursive turn. The World Bank's Energy Policy Paper from 1993 oriented its activities toward *liberalizing and privatizing energy markets*. The reasoning for privatisation was that the public sector had failed to deliver energy services. It began to promote greater use of private investment in the energy markets of developing and transition economies. (World Bank 2001, 2-3) In its second energy policy paper from 1995 also ADB started to encourage privatization and the private sector participation in funding of large scale energy investments in order to introduce elements of competition and to minimize energy monopolies. At the same time with the increasing privatization efforts ADB began to promote regional electricity trade between the neighbouring countries. ADB started to support the Build-Own-Operate-Transfer type[5] of projects in the private sector, as well as joint-venture projects between government utilities and private investors. (ADB 1995)

Second discursive turn took place in the late-1990s when especially World Bank strengthened its focus on *poverty reduction and sustainable development*. Energy was increasingly considered to be critical to poverty reduction, but more emphasis was given also to the negative impacts of energy production. Sustainable development discourse emphasized the environmental pillar, and also ADB began for the first time to integrate environmental considerations to energy development and paying more attention to environmental impacts of the energy projects. (ADB 1995) In 2000 ADB published another energy policy paper in which it again defined its goals and missions. Energy was now framed in terms of poverty reduction and environmental protection. Also global warming was discussed for the first time. The operational priorities that it defined particularly relevant to the energy sector were environmental protection, good governance, private sector development, and regional and sub-regional cooperation. It had adopted

[5] In Build-Own-Operate-Transfer (BOOT, or Build-Own-Transfer BOT) is a form of project financing a private entity receives a concession from the private or public sector to finance, design, construct, and operate a facility stated in the concession contract. This enables the project proponent to recover its investment, operating and maintenance expenses in the project. Large hydropower dams financed by private investors are usually built by BOOT agreement that usually lasts for 30 years. Research organizations and NGOs have criticized the BOOT e.g. because it mainly benefits the investors and leaves the communities to bear the consequences (changes in the river flow, impact on fishery etc.). See e.g. International Rivers (www.internationalrivers.org)

a poverty reduction strategy in its overall lending a year earlier, in 1999, and the energy policy paper reflected that change. Poverty reduction had been adopted as ADB's overarching goal. (ADB 2000, 9) This was a major change in the ADB's policy. The framework for poverty reduction comprised three pillars; pro-poor and sustainable economic growth, social development and good governance. (ADB 2000, 9) According to ADB, the energy sector operations would be designed to support ADB's approaches to poverty reduction because energy plays such an important role in meeting basic needs. (ADB 2000, 9) In 2001 World Bank published its new energy program titled Poverty Alleviation, Sustainability, and Selectivity. This energy program confirmed that energy issues remain at the core of the World Bank Group's activities for promoting economic growth and directly reducing poverty. (World Bank 2001) According to the World Bank, energy poverty in developing countries poses a persistent impediment to economic development. It is a serious equity issue as well. At the same time, the environmental impacts of conventional energy and traditional fuels are unsustainable at both the local and global levels. (World Bank 2004)

Third discursive turn in the banks' energy discourse took place in the early 21st century, when they began to emphasise the importance of *clean energy, low carbon solutions and climate-friendly technologies*. The reason given was that more than half of the global anthropogenic greenhouse gas emissions are caused by energy production and consumption, mostly fossil fuels. In twenty year's time, since the Kyoto base year 1990, global carbon emissions from energy have increased as much as 40%. (Jackson 2009) [6] Development banks began to fund some renewable energy programs. Clean energy became one of ADB's highest priorities, with over one fourth, or 27%, of the total approved loans in 2008 supporting projects with clean energy components.[7]

For the Asian middle-income countries, World Bank suggested that they should begin clean energy revolution: Countries need to transform the energy sector toward much higher energy efficiency and more widespread deployment of low-carbon technologies. According to World Bank, it is within the reach of East and Southeast Asian governments to maintain economic growth, mitigate climate change and improve energy security. (World Bank 2010) ADB established the Energy Efficiency Initiative in 2005 to promote greater investments in energy efficiency and renewable energy within the region, and to increase ADB's lending to these sub-sectors. In 2007, ADB published a report which discussed clean energy and low carbon alternatives in Asia. (ADB 2007) The report emphasized the human impact in climate change and the need for increased and urgent green house gas mitigation action in Asia. As a large proportion of the projected growth in green house gas emissions is largely linked to energy sector and transportation, the ADB underlined the importance of low carbon technologies, energy efficiency,

[6] There is also global interest in building low-carbon energy systems in developing countries as according to IEA over 70% of the increase in world primary energy demand between 2004 and 2030 comes from the developing countries. (IEA 2006, 68-70). Acknowledgement of the impacts of energy consumption on climate change has increased interest in so-called low-carbon energy solutions. Besides the development banks, climate change awakening has happened in many global and regional organizations. For example IEA has defined energy security and environmental protection as areas that need to be given particular emphasis by the governments; more environmentally acceptable energy sources need to be encouraged and developed. According to IEA, the solution lies in the clean and efficient use of fossil fuels together with the development of economic non-fossil sources, including nuclear energy and renewable energy. According to IEA, non-fossil fuels, particularly nuclear and hydro power, make a substantial contribution to the energy supply diversity of IEA countries as a group. (www.iea.org) Also other actors have redefined energy security to include also climate change. European Union defined in 2007 that the centre of new European Energy Policy was the meeting the EU's commitment in greenhouse gases mitigation. (EU 2007)

[7] More details about ADB's Clean Energy Program can be found at http://www.adb.org/clean-energy

and clean energy[8] investments. Again a year later, in 2008, ADB defined a strategic framework till the year 2020 in order to set a new strategic course. While the overarching goal had been since 1999 to reduce poverty, the mission of the Strategy 2020 was to help reduce poverty and improve living conditions in order to achieve "An Asia and Pacific Free of Poverty" (ADB 2008, i) ADB would pursue this mission by focusing on three complementing strategic agendas: inclusive growth, environmentally sustainable growth, and regional integration. For the next decade or so, it would refocus its operations to infrastructure, environment (including projects to reduce carbon dioxide emissions), regional cooperation, financial sector development and education. The new results will be monitored and assessed through Millennium Development Goals and other specified indicators. (ADB 2008)

The Table 1 shows the three major changes, or discursive turns, in World Bank's and ADB's energy policies from the 1980s to 2010, and in their understanding of security and insecurity relating to energy production and distribution. To summarise, it could be said that at the discourse level the conceptualisation of energy security has widened from the strict focus on sufficiency of supply and low price to include also other dimensions like environment and poverty reduction. However, despite of these changes, energy sufficiency and price still lie in the heart of energy security thinking of the development banks. The ways in which the sufficiency of supply and low price has been guaranteed include infrastructure construction (especially indigenous energy sources like hydropower), privatisation, and regional electricity trade. The inclusion of climate change considerations has not changed the agenda: the recipient countries are still expected to have economic growth but with less climate impact. According to the banks the combination of continuous economic growth, low climate impact and increasing energy security is possible for the middle income East and Southeast Asian countries. The solution lies in the efficient use of fossil fuels together with the development of economic non-fossil sources, such as nuclear energy and renewable energy. According to the World Bank, a low-carbon path produces substantial benefits for economic development through energy savings, better public health, enhanced energy security, and job creation. (World Bank 2010) From different renewable energy sources, hydropower is considered to have the best potential. Nuclear is also an option, even though the banks are not ready to fund it themselves. This in the World Bank vocabulary is called clean energy revolution. (World Bank 2010, 1) However, it is not clear how revolutionary it would be, as it does not really change the energy structure, except by opening a door for nuclear energy.

[8] Clean energy was in ADB context used as an umbrella term to describe both supply-side and demand-side energy related activities or technologies that result in reduction of greenhouse gas emissions compared to business-as-usual practices. (Carmody & Richie 2007)

Table 1. Energy related security/insecurity and three discursive turns in World Bank's and ADB's energy policies from 1980s to 2010

Discursive turns	Emphasis in energy policy	Source of insecurity	Solution increasing security
1980s - First framing of the energy and security	Energy infrastructure development and indigenous energy sources	Vulnerability	Building of energy infrastructure and use of indigenous energy sources
Early-1990s – First discursive turn	Privatisation and development of regional energy trade	Inefficiency	Privatization of energy sector, regional electricity trade
Late-1990s Second discursive turn	Poverty alleviation and sustainable development	Poverty and environmental degradation	Sustainable development and energy for all, capacity-building, renewable energy, regional cooperation
Early 21century - Third discursive turn	Increasing energy production with clean energy, low carbon technologies and climate revolution	Poverty; climate change; population growth and other reasons for growing energy demand	Climate-smart energy solutions: hydropower dams and other renewable energy and nuclear (for middle income countries)

Next we will look at how the development banks' energy policies are turned into practices in one particular area, Mekong region in Southeast Asia, where both banks during the past decades have been influential in the regional energy policy formations and where they have implemented several energy projects.

WB and ADB Shaping the Energy Policy in the Mekong Region

Mekong Region consists of Vietnam, Cambodia, Laos, Thailand, Myanmar (Burma) and Yunnan province of China. The region's name comes from the 4800 kilometers long Mekong River that runs through these countries and is the longest river in Southeast Asia. The history in the area has been turbulent not least because of the Indochina and Vietnam wars. In past decades countries like Vietnam, Cambodia and Laos have been going through a rapid economic transition and political transformations. Where Mekong River previously represented a division line between the capitalist and socialist worlds it is now seen as a uniting element enhancing regionalization. Over the past years, energy security concerns have moved up in the agenda of the Mekong countries. There are two main reasons, the increasing oil and gas prices and prediction of fast raising energy demand. Rapid industrialization and economic growth are increasing the use of energy especially in middle-income countries like China, Thailand and Vietnam. In order to meet the growing energy demand they have set goals to import more energy, develop their own energy infrastructure and increase energy efficiency. The estimations on demand increases have also been con-

tested. There are studies showing that many energy projects are largely justified by projections of over-estimated demand for electricity in Thailand, Vietnam and China (Greacen & Greacen 2004). The poorer countries in the region Laos, Cambodia and Myanmar (Burma) are trying to meet their own slowly growing energy needs and electrification objectives, but actually their energy sector development has been more strongly influenced by the demand of their energy-hungry neighbours and by the governments' hope to increase export revenues from the energy sector.

Table 2. *Built and planned large-scale dam projects in the Mekong Region (modified from Keskinen et al. forthcoming).*

	Existing	Under construction	Proposed
China	3	2	10
Thailand	10	0	0
Myanmar (Burma)	13	8	15
Laos	8	3	32
Cambodia	1	0	26
Vietnam	9	9	9
Total	**30**	**14**	**77**

In the Mekong Region the energy source with most regional relevance is large-scale hydropower. Hydropower's regional relevance is twofold: firstly hydropower is the main source of energy for the regional electricity grid that is funded and promoted by the development banks, and secondly the hydropower plants in the Mekong Basin have significant transboundary environmental and social impacts. The development of hydropower in Mekong Region dates back to the Cold War period. In the 1950's and 1960's Mekong Region was an important strategic area for the U.S. government which saw Southeast Asia as critical terrain for the spread of communism. Hydropower and irrigation development were interestingly perceived as issues of geopolitical security. The idea was that taming of the river could be combined to the taming of the spreading insurrections and communist ideas. The model of the inspiration for the several irrigation and dam projects of Mekong Region was taken from the Tennessee Valley which had become a sort of an American "export model for development" (Scott 1998). Backed by ECAFE (United Nations Economic Commission for Asia and the Far East) and with financial support and expertise from U.S. Mekong Committee was established in 1957. Under the Committee comprehensive plans and feasibility studies for the whole basin were developed. But because of the war and the series of conflicts in the 1960's, 1970's and 1980's only few development plans were actually implemented. The earlier plans have however now in recent years come closer to realization. The banks are not directly involved but just in few of them as the private financing is increasing in the region's hydropower sector. But more indirectly WB and ADB have been enabling the current boom of hydropower development (e.g. Middleton et al. 2009). As can be observed from Table 2 most of the proposed dam sites are located in the region's least developed countries i.e. in Cambodia and Laos.

Greater Mekong Sub-Region: regionalization and privatization emphasis

During the Cold War period the development banks mainly focused their attention to Thailand. Between 1970's and early 1980's World Bank funded several hydropower projects in Thailand (Hirsch 1996). This period was marked by the objective to increase Thailand's energy security by developing the energy infrastructure and indigenous energy sources. Starting in the late 1980s, as regional stability was largely restored, the World Bank and the ADB began to have a regional scope. Since then ADB and the World Bank have influenced the energy policies and especially the development of dams and electricity infrastructure in the Mekong Region.

In 1992 ADB launched the Greater Mekong Sub-region (GMS) program which has set a path towards regional economic integration and has attempted to orientate national policies towards private-sector led development and deregulation. In many ways the GMS programme has replaced the earlier Mekong Committee as the main framework for channelling economic development assistance to the region (Ratner 2003). The GMS program has emphasized the physical interconnectivity which would enable the cross-border trade in the region and has focused on the construction of major infrastructure projects such as transnational highways, railways and programs that encourage the integration of markets. Energy issues have played also a very central role. One of the core objectives of the GMS program has been the establishment of a regional power grid that would enhance the regionalisation of the energy market. Significant steps were taken forward in November 2002 when the governments signed an Inter-Governmental Agreement on Regional Power Trade.

The regional grid with its transmission lines is closely linked to the plans to encourage hydropower development. The grid extensions and new transmission lines are opening up previously inaccessible remote and mountainous areas for hydropower projects (Greacen & Palettu 2007). Many of the hydropower projects that would be powering the grid include controversial projects such as Tasang in Myanmar (Burma), Sambor in Cambodia and the already finalised World Bank and ADB funded Nam Theun 2 in Laos.

Power trade strategy of ADB, also supported by WB, has had a strong emphasis on market and trade. One of the justifications for the regional grid has also been the assumption that regional trade automatically enhances regional cooperation and mutual benefits. Some have claimed that the regional market emphasis has been too over-riding at the expense of national energy strategies failing to pay attention to meeting the basic domestic, commercial and industrial needs for electricity in these nations. (Yu 2003) As the poorer economies (Laos and Burma in particular) act as hydropower suppliers for their wealthier neighbours (Thailand and Vietnam) there has been criticism that they also have to bear the externalized environmental and social impacts linked to the large-scale dams. (Greacen & Palettu 2007) Some have also stated that dam promoters are taking advantage of the political non-democratic systems of Laos and Myanmar (Burma): the opposition that dams have faced in Thailand like in the case of Pak Mun dam (see e.g. Foran 2006) are far less likely in one party system of Laos or in the military junta led Myanmar (Burma).

Changing justifications of hydropower dams

During the 1990's the legitimacy of the dams has been under sever questioning and development banks' hydropower projects were severely criticised by their disastrous effects on nature and people (McCully 2001). Along with the establishment of the World Commission on Dams and its famous report (WCD 2000) problems related to large-dams have been quite widely acknowledged. Also the banks started to adopt stronger emphasis on sustainable development in their policies. This has made the justification of hydropower dams more challenging. World Bank funded Nam Theun 2 in Laos has been an attempt for the bank to show the world that large dams can be built sustainably and the project has included for example vast watershed conservation areas. But the successfulness of the project still remains to be highly debated (Stone 2010).

Also knowledge produced by experts in form of risk scenarios, models and impact assessments plays an increasing role in the legitimisation processes. In the regional level ADB and WB have "externalized" the issues of the impacts of the energy development on the Mekong River Basin to the Mekong River Commission (MRC) which is defining its role as a basin management organization. The Commission has been trying to balance conflicting ways of seeing the river basin either in terms of energy production and development engine, conservation and biodiversity region or source of food security and matter of social equity.

World Bank and ADB have been using results of the MRC's impact assessments in their own strategy papers. In their joint Mekong Water Resources Assistance Strategy for example they stated that *"The development scenarios modelling exercise [of MRC] have demonstrated that the Mekong river system has significant tolerance for development, including of hydropower and water diversion for irrigation* (World Bank and ADB 2006 p31)." But the actual studies they refer to are much more nuanced, careful and with much more emphasis on uncertainties than the bold interpretations of the banks (Käkönen and Hirsch 2009). The use of MRC's assessment results has been very selective also in that the banks have not been using the MRC's fisheries studies that have highlighted more explicitly the risks at stake with hydropower in terms of losses in fisheries, livelihoods and food security. There has been a growing body of studies highlighting the negative impacts of dams on fisheries. The flood pulse system has been recognised by ecologists as the key for the aquatic productivity sustaining the rich fisheries of the basin and the livelihoods of millions of people that depend on them. The tempering of the peaks of flood and drought by hydropower dams would be seriously damaging for the basin's fisheries. The dams are estimated also to block important routes of migratory fish. (Lamberts and Koponen 2008, Sarkkula et al 2009.) The attempts of WB and ADB to justify the dam development promotion by using selectively impact assessment studies has been directly challenged by various civil society groups (IRN 2006, IUCN et al. 2006, Middleton and Lee 2007, AMRC 2007). All in all it hasn't been an easy task for the banks to demonstrate how large-scale hydropower could be enhancing poverty alleviation and sustainable development.

Recently the increasing relevance of the climate change agenda has been re-shaping the dam debate in the region. The general discursive turn of development banks from poverty alleviation and sustainable development to clean energy and low carbon technologies has been manifested also in the Mekong Region. And within these frames the banks have attempted to use the climate change debate for greening

the hydropower projects. Hydropower is now increasingly presented as ”clean energy” and the environmental concerns on climate change mitigation and adaptation are over-riding the other environmental and social concerns. The current World Bank experts' vision that the regional grid assures that the region has access to clean, renewable energy produced by the large-scale hydropower dams principally in Laos but later possibly also in Cambodia. The smaller scale renewable options World Bank is funding are small off-grid programs that serve more as a complementary pre-electrification strategy rather than an alternative pathway. The main focus in Laos is still on large-scale hydropower development serving domestic needs but more importantly serving the need of its neighbors. Thus Laos is not anymore presented merely as the battery but the green battery of Southeast Asia. The energy security, regional trade and environmental issues in terms of climate change objectives are all presented in a win-win manner that paves the way for hydropower development. This is manifested well in a statement by a World Bank expert:

> *World Bank has an overall vision for the power sector in the Mekong Region. If you look at Laos, you don't only look from the country's point of view, but from the Greater Mekong Sub-Region's point of view. So first the World Bank is working closely with ADB, promoting regional power trade. For example, Laos has much more hydropower resources than others, so that the clean energy can be exported to Thailand and Cambodia, Vietnam. The overall priority is to provide renewable, affordable and sustainable electricity to sustain economic growth and poverty reduction in the country [Laos]. In order to achieve the first priority we need to develop the hydropower resources for export revenue earning. So far only about 7% of the potential is developed. It's more than double of the demand in this country. If you look the future and the 93% of the hydropower potential, the major target is for the regional market. From climate change point of view there is greater contributions from this point of view. (Interviewed World Bank expert in 2010)*

The concerns on environmental impact and on security of local natural resources and fisheries based livelihoods seem to have taken a backseat in this vision. Also the questions on e.g. emissions from the large reservoirs that especially many of the Mekong tributary dams involve have been so far left unanswered.

Also nuclear energy as part of main low carbon options?

Besides large hydropower, also nuclear power suddenly has come into favour among governments in Southeast Asia as a means of helping solve looming electricity shortages. While just four or five years ago nuclear energy did not feature in the medium- and long-term power development master plans of countries in the region, now Vietnam and Thailand have plans for nuclear power generation.[9] As yet, there are no commercial nuclear power plants in operation in the region (except in China), though there are small research reactors. (Symon 2008, 119) Vietnam and Thailand have plans to establish their first commercial nuclear power plants by 2020. In Vietnam the National Assembly ratified the Ninh Thuan nuclear power project in November 2009. The construction is planned to begin in 2014. (Foreign Press

[9] Here China is not included, even though the Yunnan province of China is considered to be part of the Mekong region. The mainland China has already now 11 nuclear power plants in operation and additional reactors are planned.

Centre, Vietnam, 8 June, 2010) In Thailand, the National Power Development plan from 2010 calls for five nuclear power plants. First two are planned to be build in 2020 and 2021. (The Nation 2 June, 2010) Pro-nuclear arguments are often framed in terms of climate change mitigation and reduced reliance on fossil fuels, including coal. The nuclear safety issues (e.g. radioactive waste, terrorism, tsunamis) are rarely discussed in public, and there is no strong civil-society opposition against nuclear energy. (Symon 2008)

But the new low carbon discourse has not been without emerging contestations. Especially in Thailand there has been civil society groups and activist researchers who have been raising up concerns related to the low carbon – nuclear nexus. A recent statement from and activist from Thai Working Group on Climate Justice is telling in this respect: *"We see now that we have to change our strategy and start discussing about energy democracy, sustainable livelihoods and sustainable communities because in the name of low carbon the government has started talking about four new nuclear plants."* (quoted in Kuronen 2010, p. 137)

Conclusions

During the past three decades from the early-1980s to present World Bank's and ADB's energy policies have gone through several discursive turns, i.e. major changes in their argumentation on how energy production and distribution should be organised. Despite the changes in the conceptualisation of security it remains to be a depoliticizing concept in the sense that it aims to present the solutions as serving everybody's interest in the technically best manner. The conceptualisation of energy security has widened from the strict focus on sufficiency of supply and low price to include also other dimensions like environment and poverty reduction. Despite of these changes, energy sufficiency and price still lie in the heart of energy security thinking of the development banks. The ways in which the sufficiency of supply and low price has been guaranteed include infrastructure construction (especially indigenous energy sources like hydropower), privatisation, and regional electricity trade. The inclusion of climate change considerations has not changed this part of the agenda as the recipient countries are still expected to have economic growth but with less harm on the climate. The solution lies in the efficient use of fossil fuels together with the development of economic non-fossil sources like hydropower and other renewables. For the middle-income developing countries the banks also see nuclear energy as an option.

The dominant discourses of the development banks have been continuously contested by NGOs and more critical researchers. Also the concept of energy security that still lies at the core of the energy policy objectives despite the different discursive turns has been challenged and questions on whose security is principally promoted have been raised. UN for example has demanded human security dimension to be included in to the energy security discussions. And more critical actors demand a conceptual change from energy security to energy democracy which implies that development of energy sources should be better attuned to basic local needs and projects that mainly foster energy exports and economic accumulation of metropolitan centers deserve serious questioning. This would mean that also the development banks would need to more rigorously aim at avoiding high environmental and social risk investments in large-scale plants and take smaller scale decentralized options more seriously.

In this paper we have looked at the influence of the development banks in one particular area, the Mekong Region where during the last WB and ADB have been active in attempting to shape the region's energy policies. The paper has brought into focus some aspects of the banks' discursive turns and their manifestations in Mekong energy policies. Between 1970's and early 1980's World Bank focused its support on Thailand by supporting and promoting hydropower as an indigenous energy sources relevant for countries energy security. In 1990's ADB, backed up also by WB, has supported regional economic integration through Greater Mekong Sub-Region programme in which hydropower development has been central as it has been planned to be the main source of energy for the regional electricity grid that lies at the core of the programme. The justification for the hydropower development has been however challenging especially in late 1990's and early 2000's as the banks' hydropower policies and projects have faced severe criticism. As a consequence the banks have adopted more emphasis on sustainability and they have had difficult times in trying to prove how large-scale hydropower could be enhancing poverty alleviation and environmentally sustainable development. A new opportunity for greening the hydropower has occurred however very recently as the climate change agenda has become more dominant and the banks have promoted hydropower as key low-carbon solution.

The case of Mekong highlights how despite the discursive shifts of the development banks the continuous preference for large-scale hydropower indicates that large-scale energy projects and centralised industrialisation have been in the banks' main focus throughout recent decades at the expense of other considerations. Unfortunately the communities most threatened by the energy plans, as in the case of hydropower development in Mekong Region, still remain as subaltern subjects – not heard enough in the debate. More sustainable and socially just energy futures in Mekong Region as well as in many other regions and countries of the Global South would require support for solutions that are better tuned for local needs. It seems that the concern for climate change is now increasingly used as a justification for paving the way for high risk hydropower or nuclear solutions. The role of the development banks in this as well as the unequal power structures underlying energy policy decisions in more general terms would deserve closer scholar attention and public debates.

References

ADB (Asian Development Bank) (1981) Role of the Bank in the Energy Sector in the Region. Working Paper No. 2. Manila: ADB

ADB (Asian Development Bank) (1995) Bank Policy for the Energy Sector. Manila: ADB

ADB (Asian Development Bank) (2000) Energy 2000: Review of the Energy Policy. Manila: ADB

ADB (Asian Development Bank) (2009) Energy Policy. Manila: ADB

Foran, Tira (2006) Rivers of Contention: Pak Mun Dam, Electricity Planning, and State-Society Relations in Thailand, 1932-2004, Ph.D. Thesis., University of Sydney.

Greacen, Chuenchom Sangarasri and Greacen, Chris (2004) Thailand's Electricity Reforms: Privatization of Benefits and Socialization of Costs and Risks. *Pacific Affairs* 77 (3), 517–542

Greacen, Chris and Palettu, Apsara (2007) Electricity secotr planning and hydropower in the Mekong Region. In Louis Lebel, John Dore, Rajesh Daniel and Yang San Koma (eds.). Democratizing Water Governance in the Mekong Region. Bangkok: Mekong Press.

Hajer, Maarten A. (1993) Discourse Coalitions and the Institutionalization of Practice: The Case of Acid Rain in Great Britain. In Fischer, Frank & John Forester (eds.) The Argumentative Turn in Policy Analysis and Planning. London: UCL Press Limite

Hajer, Marteen (1995) The Politics of Environmental Discourse. Ecological Modernization and the Policy Process. Oxford: Clarendon Press

Hajer, Maarten (2003) A Frame in the Fields: Policymaking and the Reinvention of Politics. In Hajer, Maarten & Hendrik Wagenaar (eds.) Deliberative Policy Analysis. Understanding Governance in the Network Society. Cambridge: Cambridge University Press

Hajer, Maarten & Hendrik Wagenaar (2003) Introduction. In Hajer, Maarten & & Hendrik Wagenaar (eds.) Deliberative Policy Analysis. Understanding Governance in the Network Society. Cambridge: Cambridge University Press.

Hughes, Larry (2009) The Four 'R' of Energy Security. *Energy Policy*. Vol. 37, Issue 6, pp. 2459-2461.

IEA, International Energy Agency (2006) World Energy Outlook OECD/IEA, Paris.

IRN (2006) Mekong Under Threat: New Strategy Promotes Dams and Diversions. International Rivers Network's factsheet, http://internationalrivers.org/files/MekongUnderThreatEnglish.pdf, haettu maaliskuussa 2008.

IUCN, TEI, IWMI & M-POWER (2006) Feedback to the World Bank and Asian Development Bank from Participants and Conveners of The Mekong Region Waters Dialogue on WB/ADB Joint Working Paper on Future Directions for Water Resources Management in the Mekong River Basin, Mekong Water Resources Assistance Strategy (MWRAS) www.sea-user.org/UserFiles/File/docs/ConvenorsMWRAS%20comments%2025%20Sep%202006u.pdf

Jackson, Tim (2009) Prosperity without Growth? The Transition to a Sustainable Growth. Sustainable Development Commission.

Keskinen, Marko, Matti Kummu, Mira Käkönen & Olli Varis (In press) Mekong at the crossroads – alternative paths of water development and impact assessment To appear in: Joakim Öjendal, Stina Hansson, & Sofie Hellberg (Eds.): Water, Politics and Development in a Transboundary Watershed – the Case of the Lower Mekong Basin. Berlin: Springer-Verlag.

Kuronen, Timo (2010) Thaimaassa vaaditaan myös oman ilmastopesän putsaamista. Teoksessa Outi Hakkarainen ja Mira Käkönen (toim.) Kenen ilmasto? Into-pamfletti. Helsinki: Like, 2010.

Käkönen, Mira and Philip Hirsch (2009) The Anti-Politics of Mekong Knowledge Production. In Francois Molle, Tira Foran and Mira Käkönen (Eds.): Contested Waterscapes in the Mekong Region - Hydropower, Livelihoods and Governance. London: Earthscan, pp. 333–365.

Lamberts, Dirk and Koponen, Jorma (2008): Flood pulse alterations and productivity of the Tonle Sap ecosystem: a model for impact assessment. *Ambio* 37(3), 178–184.

Li, Xianguo (2005) Diversification and Localisation of Energy Systems for Sustainable Development and Energy Security. *Energy Policy* 33, pp. 2237–2243.

McCully, Patrick (2001): Silenced Rivers: The Ecology and Politics of Large Dams: Enlarged and Updated Edition. London and New York: Zed Books.

Middleton, Carl & Lee, Gary (2007): Mekong Water Assistance Strategy: Justifying large water infrastructure with transboundary impacts. *Watershed* (12)1, 11-19.

Middleton, Carl, Jelson Garcia and Tira Foran (2009) Old and New Hydropower Players in the Mekong Region: Agendas and Strategies. In Francois Molle, Tira Foran & Mira Käkönen (eds.): Shaping Waterscapes in the Mekong Region: Hydropower, Livelihoods and Governance. London: Earthscan.

Ratner, Blake (2003) The politics of regional governance in the Mekong River Basin: Global change, *Peace and Security* 15(1), 59–76

Sarkkula, Juha, Marko Keskinen, Jorma Koponen, Matti Kummu, Jeff Richey and Olli Varis (2009): Hydropower in the Mekong Region: What are the Likely Impacts on Fisheries? In Francois Molle, Tira Foran & Mira Käkönen (eds.): Shaping Waterscapes in the Mekong Region: Hydropower, Livelihoods and Governance. London: Earthscan.

Scott, James C. (1998): Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed. New Haven, CT London: Yale University Press.

Simpson, Adam (2007) The Environment-Energy Security Nexus: Critical Analysis of an Energy "Love Triangle" in Southeast Asia. *Third World Quarterly*, 28(3), pp. 539-554.

Stone, Richard (2010) Along With Power, Questions Flow at Laos's New Dam. *Science* 328 (5977), pp. 414–415

Thomson, Elspeth (2006) ASEAN and Northeast Asian Energy Security: Cooperation or Competition? *East Asia*, Fall, (23)3, pp. 67–90.

UNESCAP, United Nations Economic and Social Commission for Asia and the Pacific (2008) Energy Security and Sustainable Development in Asia and the Pacific. United Nations, New York.

Watcharejyothin, Mayurachat & Ram M.Shrestha (2009) Regional Energy Resource Development Energy Security under CO2 Emission Constraint in the Greater Mekong Sub-Region (GMS). *Energy Policy* 37, pp. 4428–4441.

WCD, World Commission on Dams (2000): Dams and development: A new framework for decision making. The Report of the World Commission on Dams. London: Earthscan.

World Bank (1993) The World Bank's Role in the Electric Power Sector: Policies for Effective Institutional, Regulatory, and Financial Reform. Washington D.C: The World Bank Group.

World Bank (2002) The World Bank Group's Energy Program - Poverty Reduction, Sustainability and Selectivity. Energy and Mining Sector Board. Washington D.C: The World Bank Group

World Bank (2004) Renewable Energy Development. The Role of the World Bank Group. Washington D.C: The World Bank Group

World Bank & Asian Development Bank (2006) WB/ADB Joint Working Paper on Future Directions for Water Resources Management in the Mekong River Basin, Mekong Water Resources Assistance Strategy (MWRAS). www.adb.org/water/operations/partnerships/mwras-June2006.pdf

World Bank (2009) The World Bank Group's Energy Strategy Approach Paper. Sustainable Development Network. The World Bank Group

World Bank (2010) Winds of Change: East Asia's Sustainable Energy Future. World Bank East Asia and Pacific Region/East Asia Infrastructure Unit – EASIN. Washington DC.

Yergin, Daniel (2006) Ensuring Energy Security. *Foreign Affairs*. 85(2).

Yu, Xiaojiang (2003) Regional cooperation and energy development in the Greater Mekong Sub-region. *Energy Policy* 31, p. 1221–1234.

FOOD, ENERGY AND WATER (FEW) SECURITY ANALYSIS CUBE: FINLAND, BOLIVIA, BHUTAN AND BOTSWANA AS EXAMPLES

Tarja Ketola
University of Vaasa, Finland

ABSTRACT – *This paper builds a food, energy and water (FEW) security model with which different countries can assess their current state and future developmental needs of FEW security based on globally sustainable development. The FEW security analysis cube is built from its various building blocks, i.e., dimensions, taking their relationships and reflections into account. The resulting model is tested in four different kinds of countries: Finland, Bolivia, Bhutan and Botswana. Conclusions are drawn on the potential practicability of the model in analysing the food, energy and water security of nations, and further research plans on the other levels of needs of nations are discussed.*

Introduction

The past and present organizational form of the world is nations' society. Regional unions, such as the European Union (EU), the Latin American Economic System (SELA), the Asia-Pacific Economic Cooperation (APEC), the Asia Cooperation Dialogue (ACD and the African Union (AU) have remained politically weak organizations. The low-profile appointments to the EU's two top offices, presidency and foreign affairs, in 2009 exemplify the member states' wish to keep regional unions weak. Nations rule, and their power struggles create conflicts between them. The dark side of nation states inspired some of the lyrics for John Lennon's song *Imagine*: "Imagine there's no countries. It isn't hard to do. Nothing to kill or die for…" However, as long as nation states exist, their needs must be addressed constructively, in order to minimize the problems.

Maslow's (1943) individual hierarchy of needs can be applied to nations. They can be described briefly in the following way:

Level 1: *Physiological needs* of nations: water, food and energy.
Level 2: *Safety needs* of nations: sovereignty and peace.
Level 3: *Social needs* of nations: good relations and cooperation with others.
Level 4: *Esteem needs* of nations: respect by/of others.
Level 5: *Self-actualization needs* of nations: morality and creativity.
Level 6: *Self-transcendence needs* of nations: united consciousness.

It is often thought that these needs should be met in this order, but in reality that is not the case with individuals, organizations or societies. At societal level, each country tries to secure the fulfilment of the

different level needs in its own characteristic way. The distinctive way a nation adopts does not necessarily depend on its material development stage, but rather on the values of its people and leaders. For example, it could be claimed that Finland emphasizes the maximum fulfilment of physiological and safety needs, Botswana social needs, Bolivia esteem needs, and Bhutan self-actualization and self-transcendence needs. The argument will be discussed later in this and subsequent papers.

These different need emphases are one reason for choosing Finland, Bolivia, Bhutan and Botswana as case examples. In addition, these countries are from different continents, which gives chances for locality comparisons. On the other hand, all four countries have small populations, and, therefore, they should be able to meet their citizens' needs more easily than large population countries. I am a Finn and my expertise is currently limited to analyses of small countries – the needs and their fulfilment of large countries, like China and India, are on a much larger scale than those of small countries the analyses of which can be more focused.

Since examining all these different level needs leads to complex analyses that go beyond one paper, I shall write several papers and analyse and compare only few needs at a time. The final paper will integrate the findings and draw holistic conclusions.

My study starts from level 1 and investigates the basic national needs of food, energy and water (FEW). The most critical challenges facing nations in the next decades involve securing fresh water, food and alternative energy supplies. The basic needs of people are: water to drink, food to eat, and energy to boil water, cook food and keep warm. Meeting these needs is crucial for the survival of the citizens. There is no nation without citizens. Different political ideologies see the role of citizens in different ways: the currently prevailing capitalist ideology reduces citizens to producers and consumers, communism to producers and informers, and militarism to cannon fodder. Yet all nations and their leaders need people to govern. That is why countries strive for securing the sustainable supply of food, energy and water.

It might be argued that there are other, equally crucial, basic needs to be met, such as health services and forest conservation, but they are not really national needs. Health is an individual need, and although the general level of health of citizens is important to a nation, people will always hurt themselves, get ill and die – these are inevitable consequences of living and aging. Pandemics like influenzas are global, not national issues. The HIV/AIDS has hit some countries harder than others – in Swaziland the HIV infection rate is 26.1% and in Botswana 23.9% (Kaiser Family Foundation 2008) and in both countries AIDS kills about 2 per cent of adults every year (WHO, 2006a; WHO, 2006b), leaving children orphans and paralyzing the country's economic and socio-cultural development – but no country should be left alone to fight it; instead its prevention and treatment should be global concerns. Forest conservation is also a major global issue. Forests protect the biological heritage of this planet, i.e., the biodiversity comprising plants, animals and ecosystems. In addition, forests absorb carbon dioxide emissions travelling from all parts of the globe. These greenhouse gases do not know any national boundaries but fly freely in our atmosphere. Hence forest conservation is not just a national concern but also a local and global task.

Why then should food, energy and water be national issues? Shouldn't they, too, be solved both locally and globally at the same time? In a fair world this would be a reasonable expectation. Everyone should have enough nourishing food, clean water and energy at their disposal. Our current world is not fair, though. Nations fight over food, water and energy. They do not fight over who can save lives or forests more or most. What a researcher can do in this situation is to help leaders and citizens to under-

stand the interdependent nature of food, energy and water need fulfilment between nations. A country that solves its food, energy or water needs at the expense of others will have to pay for it sooner or later. Since climate change accelerates the speed of environmental changes leading to drastic socio-cultural and economic changes with exponentially growing numbers of climate refugees, that day will come sooner rather than later. It is understandable and acceptable that nations wish to survive and prosper and, therefore, secure their food, energy and water supplies – as long as this can be done without compromising the similar efforts of others.

The *purpose* of this paper is to build a food, energy and water (FEW) security model with which different countries can assess their current state and future developmental needs of FEW security based on globally sustainable development. In this endeavour, various dimensions, relationships and reflections must be taken into account.

Dimensions: Food, energy and water supply issues integrate the environmental, socio-cultural and economic dimensions of sustainability. These dimensions are the fundamental building blocks of a FEW security model.

Relationships: In some situations, food, energy and water needs can be met parallel. The solution of one need may even enhance the solution of another need. In other situations, conflicts arise from trying to meet food, energy and water needs simultaneously: a solution to one need may harm or even destroy the supplies of another need.

Reflections: The levels of needs are not independent of each other, but interact. Some solutions may help a nation to meet different level needs at the same time. When the different level needs clash, a nation will prioritize some needs over others or make compromises between them. That is why already in this level 1 needs' research other level needs must be discussed as intervening variables.

The rest of this paper will progress in the following way. First the food, energy and water (FEW) security analysis cube will be built from its various building blocks. The resulting draft model will then be tested in four different kinds of countries, Finland, Bolivia, Bhutan and Botswana. The data for the country cases will be derived from secondary sources: scientific journal articles, newspapers and web pages. Finally, conclusions will be drawn on the potential practicability of the model in analysing the food, energy and water security of nations, and further research plans will be discussed.

Food, Energy and Water (FEW) Security Analysis Cube

Food

In the 21st century world, food is a global market commodity and foreign food is eaten in all countries together with local food. There would be shortage of many foodstuffs if imports suddenly ceased. The level of food security would then be revealed: if the citizens still managed to continue a balanced diet and found substitutions with necessary nutrients to previously imported food, the level of national food security would be satisfactory. This is one reason why developed countries subsidize their agriculture. The governments of many developing countries either have no resources to support local agriculture or focus rather on other issues, such as rapid economic growth, which results in dwindling opportunities for non-export farming and vulnerability to food crises. Moreover, the environmentally malignant effects of cli-

mate change, desertification and floods and their combined impacts, tend to hit these countries harder than developed countries, decreasing their fertile soil area available for farming dramatically.

In many developed countries there is overproduction of food, even of basic foodstuffs like corn, resulting in farm fields left lying fallow with the assistance of subsidies, and excess foodstuffs dumped onto the markets of developing countries, so that local farming there becomes unprofitable, farmers lose their livelihoods and cannot afford to buy food for their families. While the wealthy overeat the poor go hungry.

Despite this gross imbalance developed countries wish to protect their future food supply at the expense of developing countries. In politically, economically and ecologically unstable times most countries wish to pay special attention to securing national food supplies for the future. Populous and rich countries have started to buy and lease farmland from developing countries to secure their own food supplies: e.g. China 1.24 million hectares (ha) from Philippines, South Korea 1.3 million ha from Madagascar and 690,000 ha from Sudan, United Arab Emirates 324,000 ha from Pakistan, and Libya 100,000 ha from Mali (von Braun and Meinzen-Dick, 2009). The purchasers or leasers are either states or corporations.

The International Food Policy Research Institute estimates that during 2008-2009 about 20 million hectares of agricultural land were handed over to foreigners in developing countries (von Braun and Meinzen-Dick, 2009). The reasons are obvious. Political and economic circumstances change fast and may suddenly stop food imports or multiply the price of food. Additionally, in oil-wealthy Arab countries desertification has been progressing so fast that soon farming will be impossible on nearly all of their land area. Their farming has been dependent on irrigation, which becomes practically impossible to maintain because of prolonged periods of lack of rainfall, which reduce the water levels of waterways, and because of sea level rise, which turns vast areas infertile. Asian countries have such large numbers of inhabitants that even partial desertification and/or flooding may cause shortage of food. China also suffers from major irrigation problems on its vast fields it needs to feed its 1.345 million citizens, and from quickly growing cities that conquer farmland.

But the target countries of their conquests are also suffering from desertification and/or flooding, irrigation problems, urbanization, food price changes and potential import restrictions – and still they are selling or leasing their most fertile and least draught/flood vulnerable areas. So far there has been little open opposition to such deals; if local people voice their dismay, the government silences them because of the cash or promised infrastructure. If the living conditions deteriorate slowly, protests may spread, but rapidly increasing hunger will not lead to demonstrations because hunger makes people too weak to act. Hence the fact is that rich countries will be producing their food freely on the farms of poor countries at a low local cost and taking them to their home countries free of charge.

It is the rich or immensely populous countries that may fight food wars amongst themselves for the poor countries' farmlands in the future. All self-confident nations want to be self-sufficient and not dependent on other countries in food production. Securing national food production is an acceptable goal. However, instead of conquering and fighting over other nations' food supplies and destroying their fields with intensive, large-scale, chemically enhanced farming, they could develop their own domestic farming towards non-eroding, conserving forms, such as organic, small-scale, subsistence farming, which respects ecosystem biodiversity and cultural traditions, and employs many, many more of their inhabitants. Sustainable food production and food security start at home.

Energy

Oil wars have been fought for a century particularly in the Middle East and Central East Asia because oil-producing countries have had a powerful weapon to force their views through in global politics and economics. Non-oil-producing countries have been dependent on their crude oil supply. Now that climate change is motivating countries to develop renewable energy forms, the power of oil-producing countries in threatening to diminish. Renewable energy production, such as solar, wind, wave and biomass power, is typically a local activity, resulting in independent power supplies for communities and nations. Energy security is just as strong incentive for countries to invest in renewable energy as climate change. Even countries like China, the USA, India, Australia, Russia and South Africa, which have enormous coal reserves, take renewable energy opportunities seriously. They need all energy available to boost their economic growth. China has committed to reducing its carbon intensity – carbon dioxide emissions relative to gross domestic product (GDP) – by 40-45 per cent from 2005 level by 2020, which means that with the GDP soaring, the actual CO2 emissions will be rising. While increasing energy efficiency will take care of much of this relative reduction, renewables are needed to offset the malignant effects of coal. Renewable energy seems to be an endless source of technological, economic, social, cultural and environmental innovations in which research and development (R&D) is flourishing. Yet mere local renewables development does not seem to be enough for some countries.

Populous and rich countries have started to buy and lease farmland from developing countries to secure their biofuel supplies: e.g. China 2.8 million ha palm oil plantation from Democratic Republic of Congo and 2 million ha for jatropha from Zambia, and Sweden 100,000 ha for biofuel crops from Mozambique (von Braun and Meinzen-Dick, 2009). The pattern resembles the way in which the rich and populous nations have conquered countries with oil and gas resources. Their next conquests will be land and sea area owned by developing countries captured for solar, wind and wave energy production as soon as their storing and transporting problems have been solved. The gradual removal from unrenewable to renewable energy forms is reflected on the kind of raw materials these nations now want to grab. Although renewable energy is marketed as an ethical option, the actual renewable energy production is no more ethical than fossil energy production. The same unethical ways of behaviour are appearing, and eventually leading to energy wars.

Developed countries look after their socio-cultural energy security by building centralized energy systems in urban areas and decentralized energy systems in rural areas. Most developing countries cannot afford to build infrastructure for centralized energy systems in their urban areas and even if they could, e.g. through development cooperation or aid, most of their citizens could not afford to buy the service. Urban households, companies and other organizations in developing countries are, therefore, interested in similar small, decentralized energy systems to the ones introduced in their rural areas and based on cultural traditions.

Many nations are currently building a number of new nuclear power plants, and even those countries that decided after Chernobyl to gradually phase out nuclear power altogether are taking back their promise. Corporations in the developed world advocate nuclear energy as the solution to climate change, ignoring its major malignant impacts and hazards: the mining, transporting, utilizing and disposing of radioactive uranium and fuel made of it cause huge environmental, health, safety, security and economic

problems at every stage of the process and destroy indigenous cultures and traditions in both the uranium production and nuclear waste dumping sites. The only way nuclear energy is better than other unrenewable energy forms, such as oil and gas, is that during the actual energy production it does not cause carbon dioxide emissions, although during its building, mining and all transportation stages CO2 emissions are plentiful. From all these points of view, renewable energies – solar, wind and wave – are environmentally, socio-culturally and economically secure energy forms.

Water

Drinking water is the most important substance for humans to survive. In the developed areas drinking water is tap water, in developing areas pump water, both of which usually come from either groundwater wells or rainwater ponds, but decreasingly from lakes or rivers, which are mostly too polluted to have drinkable water. Only in remote areas, not connected to other waterways, you may find a spring with clean water – if airborne emissions have not polluted it. Cleaning contaminated water is possible but for large-scale continuous use both expensive and only partial. The quality and taste of treated water does not equal those of fresh water.

Climate change causes both lack of rain, leading to draught, and excessive rain, leading to floods. Lack of rain lowers groundwater levels, which means that drinking water becomes scarce. If it rains hard after a long period of draught, dry soil cannot absorb the excessive amounts of rainwater, resulting in no rise in groundwater levels but in floods, which spread hazardous substances dissolved into surface water from overflowing sewages and other industrial, agricultural and household sources. Gradually soil absorbs some of it. If groundwater becomes contaminated, or if rain falls as acid rain, people are in trouble. Poor people have to drink polluted water even from stagnant water ponds while wealthy people buy bottled water produced elsewhere, often abroad, and transported by road or sea to these lucrative markets. In some cities in India and African countries the poor buy water from tanker trucks circulating around the slums. Tanker water is much more expensive than tap water.

Since global warming – lack of rain and shrinking glaciers – lowers the water level of lakes and rivers in the problem areas, they cannot solve the fresh water problem even with the help of water purification plants. Seawater can be turned into drinking water only after major multi-stage treatments that are very expensive. So far even wealthy seaside Arab countries suffering from persistent drinking water shortages rather import water from abroad in tanker ships than desalinize massive amounts of seawater.

The global need for water will increase by 40 per cent over the next 20 years because of population growth of 50 million a year (Kropp, 2009). Yet water reserves are shrinking even at a higher rate due to unsustainable water use practices and climate change. Water may become a major cause for wars in the future. Water conflicts on household water and irrigation have been taking place in the Middle East and Northern Africa for thousands of years; the names of states change, but the rivers remain the same. Nowadays Israel, Palestine, Jordan, Syria and Lebanon fight over water rights and distribution of the Jordan. The Euphrates and Tigris river basin conflict involves Turkey, Syria and Iraq. Ten countries along the Nile each want to direct more water onto their fields and into their towns and cities.

Similar regional disputes will become more widespread as desertification progresses in Africa, Asia, Europe and America. Currently the worst hit areas include the Sahel (a belt running through Senegal, Mauretania, Mali, Burkina Faso, Niger, Northern Nigeria, Chad, Northern Central African Republic, Su-

dan, Ethiopia, Eritrea and Djibouti), North-Western India, Northern and Western China, Spain, North-Eastern Brazil, Mexico, Southern and Western states of the USA and Australia.

Some currently fresh water secure areas, such as the Nordic countries, will have increased precipitation due to climate change, which means that they may be able to sell water to the rising number of fresh water insecure countries – unless the climate change refugees migrating from northwards cause them a population explosion. In any case, few small northern countries cannot solve the problem: their water supplies are miniscule compared to the thirst of billions of southern people. Environmental security of water everywhere is threatened by pollution from municipal sewage, industrial wastewater and agricultural overflows.

Food vs. Water

Water is needed for irrigation of fields where food crops are grown. Climate change is changing rainfall patterns and quantities all over the world. Let us take Africa as an example. Conway (2009) postulates that Northern and Southern Africa are becoming much hotter and drier, with an impact that wheat production in the north and maize production in the south will be adversely affected. He also predicts that sea levels are rising in the Nile Delta and some parts of West Africa, conquering fields and cities.

In worst hit areas of the world complete lack of rain or constant heavy rains prevent farming altogether. In the benefitting areas reduced or increased precipitation improves farming opportunities. While most plants need water to grow, the bond between food and water is very strong for rice, the most widely eaten basic foodstuff in the world. Rice is usually planted in flooded fields; therefore, if water evaporates or becomes polluted, rice dies. Some plants like durra, on the other hand, are not dependent on water and can thus be cultivated in arid lands.

Meat production consumes more water than corn and vegetable cultivation because of both indirect water consumption to grow feed for cattle in sheds or to prepare fields for grazing livestock and direct water usage on farms and ranches. Agriculture and raising cattle pollute waterways when fertilizers, pesticides, herbicides and manure flow from fields to brooks, rivers, lakes and seas. Organic farming, subsistence farming and hunting are the least water-intensive food production methods.

Fresh food needs a fraction of water compared to water consumed by processed food. The continuous 24/7 processes of food manufacturing industry consume vast amounts of water. Both the food processing industry and large-scale farming use groundwater sources. In some areas groundwater is a scarce resource; furthermore, in many countries increasingly frequent and prolonged heat waves reduce the level of groundwater. The wells of cities, towns, municipalities, villages, small-scale farmers and families dry up from the combined effect of over-consumption and un-renewability of water resources.

If water is used for producing food for exports, local people may suffer a triple blow: they turn their fields into monoculture, which gradually destroys soil fertility; they have to sell their harvest at dumped export prices to greedy middlemen so that their own families go hungry; and concentrated monoculture farming by all farmers in the area as well as multinational food processing industry established next to the monocultures in low-salary, low health, safety and environmental (HSE) concern areas dry up the groundwater sources so that local people go thirsty. The capitalist solution to these problems is to sell imported foodstuffs and bottled water to the impoverished local inhabitants.

Multinationals also build beverages factories in many dry, population-rich market areas and monopolize all the groundwater, like Coca Cola in Rajasthan, India, resulting in local farmers losing their subsistence crops and local inhabitants losing their drinking water (Woods, 2006). The families start using water from streams polluted by wastewaters from factories.

Post-modern famine caused by mono-crops for exports and death from diarrhea and other diseases caused by polluted drinking and washing water take place publicly among a population of well-nourished and healthy people, not privately in isolated villages.

Energy vs. Food

Field residues, such as straws, have always been used for energy production at farms. Increasingly also food crops are burned as bioenergy or refined into biofuels. In many western developed countries there is overproduction of barley, wheat and maize, which makes it lucrative for farmers to sell their harvest to biofuel refineries. Yet many people and organizations feel that corn should be used for food, not for fuel. The greatest problem arises from developing countries copying the formula. If important food crops like cassava, maize and sweet corn are put into car tanks instead of human mouths, famine becomes a permanent state, instead of a periodical phenomenon, in a large number of developing countries. Local food production by small-scale farmers is essential for the survival of not only families but also communities. Apart from a social issue food for fuel concern is a cultural issue: traditional, ecologically sustainable farming skills will be forgotten, if they are not passed on to the next generation.

In addition to field biomasses, bioliquids are refined from plant oils, such as palm oil, soya oil, rapeseed oil and sunflower oil. Palm oil usage is heavily criticized by environmental and social non-governmental organizations because it causes severe ecological and socio-cultural problems. But as palm oil is used for many purposes also by cosmetics industry and chemicals industry, its biofuel use does not greatly contribute to loss of food. Many other plant oils used for biofuels – soya oil, rapeseed oil and sunflower oil – are more important foodstuffs, particularly since they are essential ingredients of healthy diets. It is recommended that these oils should replace animal fat in cooking and salads and on bread. That is why using these oils as raw materials for fuels is questionable. Many people think that food should not be used for fuel either in developed or developing countries. On the other hand, animal fat, which is unhealthy to humans, can be used for biofuels. There is a market niche for mass production of biofuels extracted from animal fat. Leftover fat from frying – whether of animal or plan origin – is already a common source of biofuel raw material.

Energy is needed to plough, sow, harvest, transport, and process food. In traditional societies human and animal energy is used for this purpose, but development has meant heavy investments in machinery that use unrenewable oil-based fuels all over the world. The ecological footprint of food production has multiplied because of this “development”. Agricultural machinery use accounts for most of the CO2 emissions and other pollution from farming. Renewable fuels have been experimented on a small scale at some farms for decades since the farmers have been able to produce their own biofuels. In early 1970s Brazil pioneered at national scale in refining sugarcane into ethanol for both cars and farm machinery, and the programme has been most successful. Since 1976 it has been mandatory to blend ethanol into gasoline in Brazil; in 2009 the minimum was 25 per cent of ethanol, but even 100 per cent is possible. This initiative has boosted innovations in Brazilian agricultural technology and biotechnology, which has benefitted also food production.

Use of sugarcane for biofuel is not opposed much from the no-food-for-fuel point of view because added sugar does not belong to a healthy diet. However, in many countries healthy food plants would be the only economically viable option for large-scale biofuel production. Instead of such food-for-fuel programmes it is possible to develop the production of biogas fuels from field residues, sludge, dung and human excrement as well as electricity from the sun, wind and wave energy. Farming and food production can become simultaneously ecologically, socio-culturally and economically sustainable anywhere in the world through wise, locally specific renewable energy solutions.

Water vs. Energy

One of the oldest forms of renewable energy is hydropower, which has been used for thousands of years in the form of waterwheels and watermills. On a very small scale hydropower does not contribute to climate change. Micro-scale hydropower is an ecologically and socio-culturally sustainable energy production method when it takes advantage of a stream's natural movements to create power and respects local traditions.

Large-scale dams, built to manipulate natural water levels and flow to produce electricity, have major ecological and socio-cultural harmful impacts. Villages and towns have to be removed, which upsets people's lives and livelihoods, destroys communities and leads to the disappearance of cultures and traditions. Damming land areas create artificial lakes. Groundwater sources and cornfields are lost under water. Land sunk into the bottom of the lake emits its heavy metals and other poisonous substances into the water and pollutes the lake so that emerging fish and other marine life either dies or suffers from serious diseases. Storms and other extreme weather conditions, which are becoming more frequent as a result of climate change, as well as earthquakes, can break dams, drowning whole cities for which they have produced electricity. Stagnant water makes plant material decay fast particularly in tropical areas, resulting in major methane and carbon dioxide emissions, thereby contributing to climate change. Water wars may break out when dams have malignant effects on the waterways and lands of neighbouring countries, by diverting water away from their rivers or flooding their fields and population centres.

Power-generating methods that use the natural phenomena occurring in water without disrupting it are usually much more sustainable. These include tidal power, tidal stream power, wave power, osmotic power, marine current power and ocean thermal energy conversion.

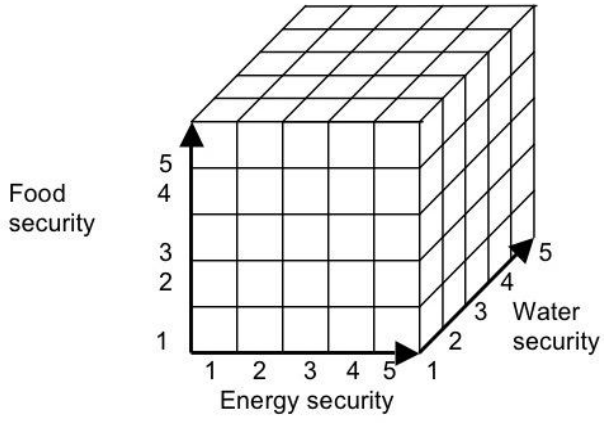
Energy is needed among other things to boil water, which makes even somewhat polluted water acceptable for drinking or at least for other household use like washing. Any energy form is suitable for electricity production, but if we think of living conditions of the poor who account for half of mankind, of the renewable energy forms water power is an indirect way of boiling water like wind power while solar and biomass energy are direct methods. Solar power is the least disruptive and energy-consuming way of boiling water. Many unrenewable power production methods, such as nuclear power plants as well as oil refining and coal production, need large amounts of water in their processes. Their wastewaters are hazardous waste that should be cleaned before discharging, or rather not be discharged at all. Those oil refineries and coal power stations that have adopted the best available technologies (BAT) have closed-loop wastewater treatment processes, which decrease the need to dump wastewater into waterways. Nuclear power plants use huge amounts of water for cooling, and, instead of being used as an energy source the heated water usually ends up in cooling ponds, rivers, lakes, or seas, causing at least ecosystem

changes. Mining the raw material, uranium, for nuclear power plants, may also need masses of water, which leads to radioactive wastewater, the treatment of which is expensive and dumping tempting in countries were environmental laws are not enforced effectively. This may result in the radioactive pollution of groundwater.

Food vs. Energy vs. Water

Food, energy and water issues are interrelated in many ways, and sometimes create a tangle, such as in the case of alga. Exploitation of algae integrates the fulfilment of food, energy and water needs, but causes further ecological, social and economic problems. Naturally growing large algae, i.e. seaweeds are important foodstuffs particularly in Asia, the British Isles, western coast of the USA and New Zealand. In addition, algae can be harvested and used as organic fertilizers on fields. Algae can also be used to capture chemical fertilizers that are flowing from fields to waterways. Moreover, sewage and other wastewater can be treated with algae instead of chemicals or direct discharges into waterways. Plans to refine algae into biofuel are also coming true. Although sewage from cities and wastewaters from industry and agriculture have made the sea and lake conditions favourable for alga growth, which has caused marine life to die for lack of oxygen, biofuel production will require active alga farming. This may cause further lake and sea deaths. Marine biodiversity will be destroyed. Health of local people may suffer. Fishing, tourism and recreation will end. While collecting algae for biofuel extraction cleans up waterways and revives marine life, thus giving the triple benefit for food, energy and water security goals, cultivating algae for biofuel extraction may lead to benefitting energy security goals but impeding water and food security goals. Similar complex interrelations can be detected in most food, energy and water security issues.

Figure 1 illustrates the way in which nations can assess their food, energy and water security on scales 1-5 for each of the three variables.



Change of strategies by the personal disconnection of decision maker

Figure 1. Food, energy and water (FEW) security analysis cube.

The ideal FEW situation is at the top right hand corner of the figure where food, energy and water security are all at levels 5 and the worst situation is in the bottom left hand corner where they are all at level 1. The basic FEW security level criterion is self-sufficiency:

level 5: very high:	≥ 100 % self-sufficiency
level 4: high:	75-99 % self-sufficiency
level 3: moderate:	50-74 % self-sufficiency
level 2: low:	25-49 % self-sufficiency
level 1: very low:	< 25 % self-sufficiency

Self-sufficiency needs to be supplemented by great strengths and potentials for and great problems and threats against food/energy/water (FEW) security. For great strengths and potentials, one level, or even two levels in exceptional situations, can be added. For great problems and threats, one level, or even two levels in exceptional situations, can be subtracted. The measurements for each level need to be tested through cases. The food, energy and water situation of four small countries – my home country Finland and three developing countries of my interest – Bolivia, Bhutan and Botswana – from different continents will be analysed through the FEW security analysis cube.

Testing the FAW Security Cube in Four Countries

Let us first look at the very basic data on the four case countries (table 1).

Table 1. Some basic information about Finland, Bolivia, Bhutan and Botswana (NationMaster, 2010abcdefghi)

	FINLAND	BOLIVIA	BHUTAN	BOTSWANA
POPULATION	5.36 million	9.78 million	0,69 million	1,99 million
TOTAL AREA **-Water** **-Agricultural land**	338,424 km2 10 % 7.44 %	1,098,581 km2 1.29 % 34.2 %	38,394 km2 < 1 % 12.6 %	581,730 km2 2.6 % 45.84 %
ARABLE CROPLAND PER CAPITA	0.42 ha	0.25 ha	0.07 ha	0.23 ha
FOOD PRODUCTION INDEX	103.6 %	110.3 %	94.5 %	104.3 %
GDP PER CAPITA	$ 33,556 (PPP)	$ 4,455 (PPP)	$ 5,212 (PPP)	$ 13,992 (PPP)
ELECTRICITY PRODUCTION / CAPITA	14,702.794 kWh	621.549 kWh	1,922.376 kWh	556.919 kWh
ELECTRICITY CONSUMPTION / CAPITA	16,850.372 kWh	558.385 kWh	227.163 kWh	1,464.260 kWh

Bolivia is the largest of the four countries both in area and population. Botswana is second in area but Finland in population. In Finland surface water covers a much higher percentage of the land area than in the other three countries. Bolivia's and Botswana's actual water surface coverage is just over 40% of Finland's, Bhutan's only just over 1%.

In agricultural land percentage of the whole area Finland ranks even lower than Bhutan while Botswana and Bolivia have great areas dedicated to agriculture. However, it is the quality of agricultural land that counts: Finland has nearly twice as much arable cropland per capita as Bolivia and Botswana, and six times more than Bhutan. The high food production index of all other case countries than Bhutan means that, at least in theory, these countries are self-sufficient in food production, which would suggest that their food security level would be very high – yet there are problems and threats that may reduce food security. Gross domestic product (GDP) per capita gives some idea how well a country could afford to mitigate or solve its food, energy and water problems and threats and take advantage of its strengths and potentials. Finland is a high-income, country Botswana a middle-income country and Bhutan and Bolivia low-income countries.

Energy security covers both electricity and fuels, but reliable, comparable statistics are available only about electricity. The production and consumption of electricity per capita is the highest in Finland, which is 87% self-sufficient and needs to import 12.5% of its electricity. Bhutan produces the second largest amount of electricity but consumers least of all these countries, leading it to a tremendous 845% self-sufficiency in theory. Bolivia produces slightly more electricity than it consumes, making it 111% self-sufficient in theory. Botswana is only 38% self-sufficient in electricity production.

The numbers may be misleading because there are many strengths and potentials as well as problems and threats that they do not take into account. The following, more detailed descriptions of food, energy and water (FEW) security and their interrelations of the four countries will pay special attention to these intervening factors.

Finland

Food: F4: Finland is self-sufficient in food production with enough, good arable land for farming, green pastures for grazing and well-developed food production industry. Finland produces a good variety of food, securing a nutritious, balanced diet. The country could feed its current population without imports. It could replace imports with domestic substitutes. Finland is dependent on fertilizers but organic food production is increasing. Climate change refugees could add mouths to feed, but since Finland is the furthest country up north in its longitude, the refugees from Africa will populate first Southern Europe, wander then to Central Europe, and of the Northern European countries probably try Denmark and Sweden, which are accessible by road, before taking a ferry to Finland.

Energy: E2->3: Currently Finland imports 70% of the energy it needs. Most of it, 45%, comes from Russia as unsustainable, unrenewable oil, gas and coal. Of the domestic energy production nuclear accounts for 25%, wood 20%, hydropower 5% and peat 5%. In electricity production Finland is 87.5% self-sufficient. There are 200 hydropower plants in Finland; the largest is 170 MW, others much smaller, all totalling nearly 3,000 MW. It is not really possible to build more hydropower in Finland without damaging the environment. According to the government's energy plan (Finnish Government, 2010) Finland aims to reduce carbon dioxide emissions by 20% from the1990 level and become almost self-sufficient by 2020 by adding nuclear power and renewable energy production. The nuclear energy share should thus gradually increase even to 62% with the fifth nuclear power plant currently under construction and two or three more nuclear power plants being planned. The building of nuclear power plants 1-5 has been given to French and German companies, which have subcontracted work mostly to other foreign

companies with foreign workers. The share of renewables is planned to reach 38% of total energy production by adding wood, biofuel, wind and geothermal energy (Finnish Government, 2010).

Water: W5: Finland is totally self-sufficient in water supply: it has very good rainfall, groundwater all over its land area as well as 190,000 lakes and 209 rivers. The country borders to seas in the south and west, but seawater is not needed for households or agricultural irrigation. Algae overgrowth caused by eutrophia is an increasing problem in the surface waters of seas, lakes and rivers.

Positive FEW interrelations: Algae collection for biofuels from lakes, rivers and seas could clean waters; algae could also be used for food, but that is not traditional in Finland. Climate change with a more temperate climate and increased precipitation may improve food and water security, unless heat waves make soil too hard to absorb the rainwater, turn into floods and lead to soil erosion.

Negative FEW interrelations: A nuclear power plant disaster would lead to food, energy and water crises because of radiation and great dependence on nuclear. Big increase in wood-based energy may reduce forests, lead to soil erosion, and result in food and water crises. Biofuel production may mean sacrificing others' forests for fuel (destroying rainforests for palm oil plantations) or own food for fuel (growing e.g. rape seed oil for biofuels rather than food oil).

Bolivia

Food: F2: In Bolivia food production is based on subsistence agriculture. The country produces a good variety of food because of various climates, but not sufficiently. Only 2% of land area is in arable farming. Bolivia suffers from extremely low productivity, poor distribution of the population in relation to productive land and lack of transportation facilities. Additionally, as poverty in remote areas amounts to 83%, most of the citizens have difficult geographical and financial access to food (WFP, 2010a). Constant natural disasters, such as floods, mudslides, landslides and droughts, cause crop loss (FAO/WFP, 2008; WFP, 2010b). Malnutrition is common in rural areas (WFP, 2010a). Bolivia exports soya bean on the Andean Community market. The country develops food production through irrigated agriculture, which has malignant impacts on the environment. More environmentally benign ways of achieving food security and diversification of crops would be crop rotation and planting of nitrogen fixing legumes, which improve soil without irrigation or fertilizers.

Energy: E3: In theory Bolivia has full self-sufficiency in energy supply. In gas production Bolivia ranks 29th) and in oil production 46th in the world (Wikipedia 2010ab). It exports oil and, particularly, gas to Brazil, which brings revenues for Bolivia's development. Bolivia is a land-locked country and needs Brazil's pipelines to export its hydrocarbons. Brazil plans to increase its own hydrocarbon production so that it would not need any imports by 2011. Other export opportunities are dwarfed by the neighbouring countries' doubts of the ability of Bolivia's national energy company, YPFB, to maintain continuous energy supply and by Argentina's and Chile's own hydrocarbon development plans (Romero & Schipani 2010). In electricity production Bolivia is 111% self-sufficient due to hydropower plants. However, many because of huge distances in varied terrains and poverty Bolivians have difficult geographical and financial access to energy, which means that the nation cannot supply energy to all its citizens. Gas and oil production was re-nationalized in 2006 by Bolivia's first indigenous president, Evo Morales, and on Labour Day, 1 May 2010, he nationalized also four hydroelectric companies (Ore & Garcia, 2010). The long-term aim of nationalization is to provide all Bolivians with electricity. The re-nationalization of gas

and oil in 2006 did not much ease the fulfilment of energy needs of ordinary Bolivians although some of the revenues have been invested in the socio-economic development of the lives of indigenous peoples.

Water: W2: The eastern tropical and subtropical areas of Bolivia and lake Titicaca basin are self-sufficient in water supply, but western semiarid and arid areas are not. One third of the city dwellers have no access to water. In 2000 water supply was privatized in arid Cochabamba and La Paz, which led to triple prices and violent protests, resulting in re-nationalization (Hailu et al., 2010). Access and maintenance problems continue. Water quality is constantly decreasing because of the dumping of untreated effluents from industries, cities and irrigated agriculture into water sources. The Water Ministry of the current government has a water reform plan, which focuses on community decision-making, integration of traditional methods and new technology, water rights registration, water quality, and irrigation infrastructure. Irrigation accounts for 94% of all water withdrawals. Melting of glaciers will make Bolivia more dependent on rainfall.

Positive FEW interrelations: Substance farming has minor impact on water quantity and quality and it could be developed organic. There are solar, wind, wave and biomass energy potentials for food and water production.

Negative FEW interrelations: Irrigated agriculture has led to soil erosion and loss of production capacity of 41% of land area. Agricultural runoff is one of the main contributors to water pollution. Slash-and-burn farming reduces forests, leads to soil erosion and exhaustion of its nutrients, resulting in food and water crises. Amazon basin (66% of Bolivia) is prone to floods, causing crop loss. Constant natural disasters caused by El Niño and La Niña, accelerated by climate change, lead to food, energy and water crises. Major oil and gas production pollute soil and water and increase CO_2 emissions.

Bhutan

Food: F2: Food production in Bhutan is based on subsistence farming and animal husbandry. One third of the Bhutanese suffer from food insecurity (WFP, 2010c). The country imports 34% of its cereal needs, e.g. 60% of the staple rice from India. In January 2010 the first ever rice mill started operating in Bhutan (Bhutan Today, 2010). Southern subtropical plains and temperate central highlands could become self-sufficient in food production, northern polar-type Himalaya cannot. Natural disasters in rainy seasons cut off access to non-local food supplies and destroy local supplies. The government attempts to reverse the declining trend in cereal yield per hectare and per capita food production by education, zoning the country's territory and delineating protected areas for agricultural production. Yet, instead of maximizing gross domestic product (GDP), Bhutan aims to maximize Gross National Happiness (GNH), an indicator of the quality of life, which takes account of equitable and sustainable socio-economic development, conservation of the natural environment, preservation and promotion of traditional culture, development of good governance, and the satisfaction and spiritual growth derived from them (Ketola, 2010).

Energy: E4: Bhutan is a land-locked country with rugged terrains, which make energy production and supply to the citizens difficult. However, the country's rapid altitudinal variations and swift flowing rivers make it perfect for hydropower (Tshering & Tamang, 2004). Bhutan is 845% self-sufficient in electricity due to the gigantic Tala Hydroelectricity dam project; all its electricity is exported to India. This brings good revenues to the country. There are more than 20 other hydro dams that supply electricity to the Bhutanese. Further hydropower potential amounts to 30,000 MW. Yet 50% of Bhutanese (60%

of rural areas) have no access to electricity and use biomass, i.e. traditional methods: wood and animal dung. The Bhutanese government aims to expand domestic electricity network so that by 2020 the entire country would have access to electricity and the domestic tariff would be kept low enough for citizens to be able to afford to buy electricity (Tshering & Tamang, 2004). Hydropower should enhance Bhutan's sustainable development in two ways: (a) it provides clean, renewable, safe, reliable, sufficient and affordable electricity for domestic consumption and industrial use, and (b) it brings the much needed capital to finance social projects and achieve economic self reliance (Tshering & Tamang, 2004). The environmental and social problems caused by water diversion and damming – e.g. population displacement, intrusion into protected areas, loss of primary forests, dewatering impacts, soil erosion and fish migration (Tshering & Tamang, 2004) – need to be addressed better than before. Gross National Happiness (GNH) index protects forests of central highlands from overuse for energy. Bhutan imports all the fuel it needs. There is great solar energy potential in Bhutan.

Water: W3: The so far abundant water supply of the main rivers flowing through highlands, where most Bhutanese live, depend on Himalayan glaciers. Bhutan's rural water supply scheme (RWSS) from 1974 should provide 89% coverage of drinking water, but only about 36% work without problems due drying water sources, traditional water rights, damaged pipes and structures, lack of regular maintenance, inadequate community maintenance and lack of trained water caretakers and tools (Lamsang & Wangdi, 2009). Moreover, differences in rainfall patterns and increasing fluctuation between lean season and monsoon season water flows cause localized and seasonal water shortages.

Positive FEW interrelations: Vast river areas allow food, energy and water co-production. Small population helps to increase food, energy and water security at low cost.

Negative FEW interrelations: Melting of Himalayan glaciers will make Bhutan more dependent on rainfall. Hydropower dams sink fields and cause water and soil pollution. Floods and landslides resulting from hydropower and increasingly heavy monsoons lead to soil erosion and loss of arable farmland. Increasingly drier lean seasons have the same effect.

Botswana

Food: F3->2: Botswana's climate is arid and semiarid with low rainfall (Botswana, 2008). Kalahari Desert covers nearly 70% of the country. Increasing droughts cause water shortages and further desertification, shrinking arable land further. Less than 5% of agricultural irrigation can come from rainfall (Darkoh, 2003), making agriculture unprofitable. Hence 50% of Batswana households raise cattle and livestock, needing grazing lands, which accelerates desertification (Darkoh, 2003). Domestic production can supply only 10 % of the cereal needs, and nearly all the annual cereal requirement is imported (Botswana, 2008). About 25% of population is undernourished. Although this is less than in Sub-Saharan Africa in general, improvement of food security is one of the main objectives of the Botswana government (Botswana, 2008).

Energy: E2: Botswana is 38% self-sufficient in electricity, which comes from two coal power stations, and imports the rest. Electricity is available mostly only in urban areas, and the government supports rural electrification (Botswana, 2008). Botswana must import all the fuel it needs. The country has tiny oil reserves, which are not yet exploited. Botswana's vast national parks and game reserves are protected from forest cutting e.g. for energy. The country has major solar and wind energy potential, which the

government programmes support (Botswana, 2008) and which could make Botswana self-sufficient in electricity production.

Water: W1: Botswana's water shortage is very serious and continues to get worse because of accelerating droughts and desertification. The Okavango, Limpopo, Zambezi and Orange Rivers are shared by and get their waters from neighbouring countries, and are shrinking mainly due to droughts but also because of dams. This may cause water conflicts between the nations. Botswana does not produce hydropower but suffers from effects of hydro-production of the neighbouring countries. The dams on rivers in Botswana have been constructed for livestock watering and urban water supply (Botswana, 2008). Lack of seasonal rainfall in Botswana results in 75% of humans and animals dependent on groundwater. Surface water is very scarce.

Positive FEW interrelations: Botswana's Department of Forestry and Range Resources reintroduces indigenous vegetation, which aims to mitigate land degradation, thereby helping food production and water conservation (Mogotsi et al., 2006). The HIV/AIDS has left the younger generation without knowledge and practises usually passed on from the older generation. The United Nations Development Programme (UNDP) works with Batswana communities, re-introducing indigenous knowledge and traditional land management systems (Afrol News, 2004).

Negative FEW interrelations: Climate change accelerates droughts and desertification leading to food and water crises. Drilling deep boreholes for groundwater leads to soil erosion and consequently to even less arable land (Darkoh, 2003). The Okavango Delta is drying up because of overgrazing (Botswana, 2008).

Discussion: FEW security of the four nations

The findings of these brief food, energy and water (FEW) security analyses of the four case countries, Finland, Bolivia, Bhutan and Botswana, are illustrated by the FEW cube in figure 2.

According to these concise analyses taking account of self-sufficiency as well as great strengths and potentials and great problems and threats, the food, energy and water (FEW) security findings are as follows. *Finland's* (FEW) security is F4–E2->3–W5, meaning that food security is high, energy security is rising from low to moderate and water security is very high. *Bolivia's* FEW security is F2–E3–W2, meaning that food security is low, energy security is moderate and water security is low. *Bhutan's* FEW security is F2–E4–W3, meaning that food security is low, energy security is high and water security is moderate. *Botswana's* FEW security is F3->2–E2–W1, meaning that food security is decreasing from moderate to low, energy security is low and water security is very low.

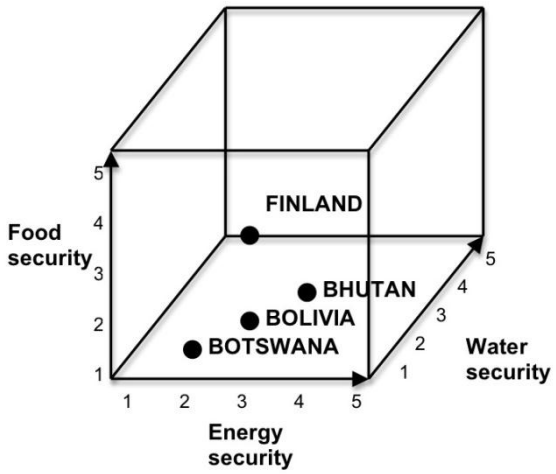


Figure 2. Four countries in the food, energy and water (FEW) security analysis cube.

In *food security* Bolivia, Bhutan and Botswana are weak and need considerable improvements. In *energy security* Botswana is weak but the others manage quite well. In *water security* Botswana is on the brink of disaster, and Bolivia is weak, needing major improvements. All in all, the most serious FEW problems lie in Botswana because of the downward spiral that anthropogenic climate change and its consequences are causing in the interrelations between food, energy and water.

The United Nations World Food Programme (WFP) operates in the most *food* insecure countries, including two of the case countries, Bolivia and Bhutan. Although Botswana has the worst prospects for food self-sufficiency, it is a middle-income country that can afford to buy all it needs to secure the food supply of its 1.99 million citizens. However, the United Nations Development Programme (UNDP) helps Botswana in its severe *water* security problems, which are closely connected to food security problems.

Bolivia, Bhutan and Botswana are land-locked countries, which impedes their ability to be independent in their *energy* sales and purchases. This problem should encourage them to distribute their existing energy domestically among their citizens and develop local renewable energy forms, such as solar, wind and biomass production, which they do to some extent, but also crave for revenues from exports. Seafaring Finland still imports most of its energy in oil tankers and coal ships, but plans to increase some renewable energy production in addition to building more nuclear plants. The governments of all four nations seem to ignore the most environmentally, socio-culturally and economically sustainable energy resource: organic waste. Human excrement, animal dung and organic waste streams from industry are infinite energy sources. Making bioenergy out of organic waste would additionally solve the over-fertilization of waterways causing sea, lake and river deaths.

Wealthy Finland wastes some of its abundant food, energy and water resources; hence it could be called Binland. The other B-countries, Bolivia, Bhutan and Botswana, could not really afford to waste any of their resources.

Conclusions

This research paper developed a food, energy and water (FEW) security model, so that nations could evaluate their current state and future developmental needs of FEW security based on globally sustaina-

ble development. The FEW model integrates quantitative data on self-sufficiency into qualitative information about the great strengths and potentials and great problems and threats in each issue, and takes account of the interrelations between the food, energy and water issues.

The four case studies show that analyses through the FEW model help to see the whole picture without getting lost in the details. The model needs further refining in taking simultaneously the environmental, socio-cultural and economic dimensions of sustainability into account, but seems to be practicable as a simple tool to filter masses of quantitative and qualitative information into guiding food, energy and water security levels.

This research paper studied only the first level of Maslow's hierarchy of needs: physiological needs. Meeting the basic food, energy and water needs of citizens is naturally crucial for all nations, but wellbeing covers more than that. The subsequent papers will analyze the fulfilment of the other five Maslow's needs groups – safety, social, esteem, self-actualization and self-transcendence needs – in Finland, Bolivia, Bhutan and Botswana, and make comparisons between the needs groups of the case countries.

References

Afrol News (2004) Botswana villages fighting desertification. *Afrol News*, 3 June 2004. http://www.afrol.com/articles/13090 retrieved 30 April 2010.

Bhutan Today (2010) First ever rice mill to aid food security in Bhutan. *Bhutan Today*, January 8, 2010. http://www.bhutantoday.bt/?p=2160 retrieved 30 April 2010.

Botswana (2008) National Investment Brief – Botswana. *High-Level Conference on: Water for Agriculture and Energy in Africa: The Challenges of Climate Change*. Sirte, Libyan Arab Jamahiriya, 15–17 December 2008.

Braun, Joachim von – Meinzen-Dick, Ruth (2009) "Land grabbing" by foreign investors in developing countries: risks and opportunities. IFPRI Policy Brief 13, April 2009, International Food Policy Research Institute, Washington, DC.

Conway, Gordon (2009) The science of climate change in Africa: impacts and adaptation. *Grantham Institute for Climate Change, Discussion paper* No 1, October 2009, Imperial College, London.

Darkoh, Michael B.K (2003) The Nature, Causes and Consequences of Desertification in the Drylands of Africa. In Darkoh, Michael B.K. – Rwomire, Apollo (2003) (eds.) *Human Impact on Environment and Sustainable Development in Africa,* 199-236. Ashgate, Aldershot.

FAO/WFP (2008) *Special Report FAO/WFP Food Security Assessment Mission - Bolivia, May 2008.* http://www.fao.org/docrep/010/ai467e/ai467e00.htm retrieved 30 April 2010.

Finnish Government (2010) *Government decides on policies for nuclear power and promotion of renewable energy production.* Ministry of Employment and the Economy, 21.4.2010. http://www.valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=293158 retrieved 30 April 2010.

Hailu, Degol – Osorio, Rafael – Tsukada, Raquel (2009) *Privatization and Renationalization: What went Wrong in Bolivia's Water Sector?* International Policy Centre for Inclusive Growth (IPC-IG). http://www.inesad.edu.bo/bcde2009/A3%20Hailu%20Osorio%20Tsukada.pdf retrieved 30 April 2010.

Kaiser Family Foundation (2008) *The HIV/AIDS Epidemic in South Africa*, October 2008. The Henry J. Kaiser Family Foundation, Menlo Park, CA. http://www.kff.org/hivaids/upload/7365-065.pdf retrieved 28 November 2009.

Ketola, Tarja (2010) Responsible leadership: building blocks of individual, organizational and societal behaviour. *Corporate Social Responsibility and Environmental Management*, Vol. 17(3): 173–184.

Kropp, Robert (2009) Global water resources threatened by climate change and population growth. *Sustainability Investment News*, March 5, 2009.

Lamsang, Tenzin – Wangdi, Nima (2009) Water shortage problem hits (PM's) home. *Kuensel Online – Bhutan's daily news site*, 11 April 2009. http://www.kuenselonline.com/modules.php?name=News&file=article&sid=12262 retrieved 30 April 2010.

Maslow, Abraham (1943) *Psychology of Science*, Gateway Publishers, Chicago.

Mogotsi, Kebadire K. – Kanego, Arabang – Sebele, Neelo – Kgaswane, Medy – Gabaitse, H. (2006) New opportunities for combating desertification in Botswana: Women in action for sustainable land and natural resources management. http://www.iydd.org/documents/NOTCDIB.pdf retrieved 30 April 2010.

NationMaster (2010a) *People Statistics: Population (most recent) by country*. http://www.nationmaster.com/graph/peo_pop-people-population retrieved 30 April 2010.

NationMaster (2010b) *Geography Statistics: Area: Total (most recent) by country*. http://www.nationmaster.com/graph/geo_are_tot-geography-area-total retrieved 30 April 2010.

NationMaster (2010c) *Geography Statistics: Area: Water (most recent) by country*. http://www.nationmaster.com/graph/geo_are_wat-geography-area-water retrieved 30 April 2010.

NationMaster (2010d) *Agriculture Statistics: Agricultural land: % of land area (most recent) by country*. http://www.nationmaster.com/graph/agr_agr_lan_of_lan_are-agriculture-agricultural-land-of-area retrieved 30 April 2010.

NationMaster (2010e) *Agriculture Statistics: Arable and permanent cropland (per capita) (most recent) by country*. http://www.nationmaster.com/graph/agr_ara_and_per_cro_percap-arable-permanent-cropland-per-capita retrieved 30 April 2010.

NationMaster (2010f) *Agriculture Statistics: Food production index (most recent) by country*. http://www.nationmaster.com/graph/agr_foo_pro_ind-agriculture-food-production-index retrieved 30 April 2010.

NationMaster (2010g) *Economy Statistics: GDP (most recent) by country*. http://www.nationmaster.com/graph/eco_gdp-economy-gdp retrieved 30 April 2010.

NationMaster (2010h) Energy *Statistics: Electricity: Production (per capita) (most recent) by country*. http://www.nationmaster.com/graph/ene_ele_pro_percap-energy-electricity-production-per-capita retrieved 30 April 2010.

NationMaster (2010i) Energy *Statistics: Electricity: Consumption (per capita) (most recent) by country*. http://www.nationmaster.com/graph/ene_ele_con_percap-energy-electricity-consumption-per-capita retrieved 30 April 2010.

Ore, Diego – Garcia, Eduardo (2010) *Bolivia nationalizes four power companies*. http://www.reuters.com/article/idUSTRE64013020100501 retrieved 1 May 2010.

Romero, Simon – Schipani, Andrés (2010) Neighbors Challenge Energy Aims in Bolivia. *New York Times*, January 9 2010. http://www.nytimes.com/2010/01/10/world/americas/10bolivia.html retrieved 30 April 2010.

Tshering, Sonam – Tamang, Bharat (2004) Hydropower – Key to sustainable, socio-economic development of Bhutan. *United Nations Symposium on Hydropower and Sustainable Development*, Beijing, China, 27–29 October 2004.

WFP (2010a) *World Food Program: Countries: Bolivia*. http://www.wfp.org/countries/bolivia retrieved 30 April 2010.

WFP (2010b) *Operations: Recovery of Food-Insecure Households Affected by Consecutive Natural Disasters*. http://www.wfp.org/content/recovery-food-insecure-households-affected-consecutive-natural-disasters retrieved 30 April 2010.

WFP (2010c) *World Food Program: Countries: Bhutan*. http://www.wfp.org/countries/bhutan retrieved 30 April 2010.

Wikipedia (2010a) *List of countries by natural gas proven reserves*. http://en.wikipedia.org/wiki/List_of_countries_by_natural_gas_proven_reserves retrieved 30 April 2010.

Wikipedia (2010b) *List of countries by proven oil reserves*. http://en.wikipedia.org/wiki/List_of_countries_by_proven_oil_reserves retrieved 30 April 2010.

WHO (2006a) *Mortality Country Fact Sheet 2006. Swaziland*, World Health Organization, Geneva. http://www.who.int/whosis/mort/profiles/mort_afro_swz_swaziland.pdf retrieved 28 November 2009.

WHO (2006b) *Country Health System Fact Sheet 2006. Botswana*. World Health Organization, Geneva. http://www.afro.who.int/home/countries/fact_sheets/botswana.pdf retrieved 28 November 2009.

Woods, Brian (2006) *A World Without Water*, Documentary. True Vision Productions.

THE INTANGIBLE THREATS OF CLIMATE CHANGE TO HUMANKIND ON THIS EARTH AND BEYOND

Bertrand G. Guillaume1[a]

[a] ICD-CREIDD, UMR CNRS 6279, Université de technologie de Troyes, France

ABSTRACT *– Climate change is an emblematic example of how humankind is now influencing the workings and dynamics of the planetary machinery.*

While the study of such an 'anthropogenic drift' of Earth System is grounded in natural sciences, social sciences have highlighted critical issues regarding its human dimensions, including the broad implications for security. Yet I am not sure that the 'intangible threats' to human security are not underexplored when it comes to the dénouements of this drama.

I shall first sketch the features of climate change as a security issue, and underline that without radical coordinated counteraction it will challenge many of our adaptive capacities. Climate change is likely to exacerbate conflict between and within countries over natural resources, migration, and the distribution of wealth. This could result in disorders and violence, jeopardizing human security to a new degree.

Yet there is no reason that the threats of climate change should amount to first-order (tangible) effects on the bio-physical world or the socio-economical system. Contrariwise, I shall argue that it will involve second-order (intangible) dimensions related to our human condition and our relationship to the world. I shall suggest that the threats of climate change to human security will also be of the latter form, threatening more specifically logic, axiology, metaphysics, and politics.

Introduction and Background

Climate change is an emblematic example of how humankind is now influencing the workings and dynamics of the planetary machinery (Turner et al., 1990 ; Crutzen, 2002).

While the study of such an 'anthropogenic drift' of Earth System is grounded in natural sciences, social sciences have highlighted critical issues regarding its human dimensions (Stern et al., 1992), including the broad implications for human security, and drawing attention to the factors underlying vulnerability to climate change (Matthew et al., 2009).

Yet I am not sure that the 'intangible threats' to human security are not underexplored when it comes to the dénouements of this drama.

Climate change as a security issue

Let me first sketch the features of climate change as a security issue.

There are numerous connections between climate change and security, including national security, human security and military roles (Barnett, 2003).

Following the German Advisory Council on Global Change (WBGU, 2007):

> *"Firstly, climate change could exacerbate existing environmental crises such as drought, water scarcity and soil degradation, intensify land-use conflicts and trigger further environmentally induced migration. Rising global temperatures will jeopardize the bases of many people's livelihoods, especially in the developing regions, increase vulnerability to poverty and social deprivation, and thus put human security at risk.(…)"*
>
> *"Secondly, new conflict constellations are likely to occur. Sea-level rise and storm and flood disasters could in future threaten cities and industrial regions along the coasts of China, India and the USA. (…)".*
>
> *"Thirdly, unabated climate change could cause large-scale changes in the Earth System such as the dieback of the Amazon rainforest or the loss of the Asian monsoon, which could have incalculable consequences for the societies concerned."*

Overall, if climate-induced interstate wars are hardly likely to occur, climate change could jeopardize human security to a new degree, triggering new conflicts between and within countries over natural resources, migration, and the distribution of wealth and intensifying existing issues such as state failure, social disorders, and rising violence.

With this in prospect, mitigation strategies and adaptation ways can be viewed as security policies to avoid security threats to nation-states, communities and individuals.

Second-order (intangibles) dimensions

Without radical coordinated counteraction climate change will challenge many of our adaptive capacities within the decades to come (Parry et al., 2007).

Yet there is no reason that the threats of climate change should amount to first-order (tangible) effects on the bio-physical world or the socio-economical system (Rockström et al., 2009).

Contrariwise, I shall argue that it will involve second-order (intangible) dimensions related to our human condition, values and relationship to the world.

I suggest that the threats of climate change to human security will also be of the latter form, threatening more specifically logic, politics, axiology and even metaphysics.

A first intangible threat of climate change is the one to the broad philosophical category known as logic that is a theory of knowledge, including reason, language, and reasoning.

Climate change illustrates the intuition that the ultimate impacts of some contemporary risks are literally "untold", for there is a crucial gap between their reality and the ways we have to quantify them or express them as "speakable" (e.g. numbers).

To put it (excessively) shortly in two striking questions:

- How could we express the threat of a large and irreversible recasting of human geography?

- How could we quantify the danger to get back in 2100 to the global climate of the Pliocene?

A second intangible threat of climate change is the one to the broad philosophical category known as axiology that is a theory of value, including aesthetics and ethics.

The issue of the impacts of climate change on world heritage properties, both natural and cultural, is of great interest (UNESCO, 2007) but let me focus on ethics, which is maybe more obvious.

On the front line is of course environmental justice, in both space and time, updating the old concepts of social justice, non-discriminating principle and moral virtue.

But there is also much more, that is the brand new responsibility we hold toward the deep future (Jonas, 1984).

History shows at least two instances of global environmental near-misses induced by human activity. Anthropogenic climate alteration is now on the list.

A third intangible threat of climate change is the one to the broad philosophical category known as metaphysics that is an exploration of the ultimate nature of the world and ourselves, including ontology and theology.

This threat is an extension of the former, for it may be that under a "rare Earth" hypothesis complex life be uncommon in the universe while simple, microbial animal or plant life could be widespread (Ward & Brownlee, 2000).

If very few planets could indeed offer the long-term stability necessary to the emergence of complex life, it would give a "karma vertigo" (Brand, 1999) to our civilisation.

This hyperbolic responsibility would, in turn, challenge the very sense of human action on Earth and beyond, something like a theodicy in the era of global environmental change.

Maybe the future does not need us (Joy, 2000). But maybe it does, and our destiny has a "cosmic signification" (Rees, 2003)

A fourth intangible threat of climate change is the one to the broad philosophical category known as politics that is the structure and the function of society, including in the liberal Western tradition freedom and democracy.

The stumbling block is here that systematic environmental externalities have become incompatible with the foundations of our society inherited from Hobbes, where everyone is in capacity to choose the ends of his actions and to maximise his interests.

It follows that the resolution of the ecological crisis could be "a tale of two possible threats to democracy" (Guillaume, 2009).

At the extreme, drastic wartime-style rationing could materialise a first authoritarian scenario, involving an arbitrary delineation between (assumed legitimate) needs and (assumed illegitimate) desires, with a monstrous planetary dictatorship in charge of controlling citizens to preserve the weakening nature.

A second "eco-fundamentalist" scenario which could de facto rule out democracy and politics in fighting climate change exhibits unilateral geo-engineering initiatives or massive technological fixes under radical technocracy.

Conclusion

The unprecedented (both quantitatively and qualitatively) scale of our relationship to nature calls for a deep renewing of our ways of thought and action.

We are now confronted with a global threat likely to recast the bio-physical abode of men, but also and more generally their cultural history and encompassing oecumene.

The "intangible threats" of global environmental change are such threats to human civilisation, on this Earth and beyond.

References

Barnett, Jon (2003). Security and climate change. *Global Environmental Change*, 13, 7-17.

Brand, S. (1999). *The clock of the long now: Time and responsibility*, New York, Basic Books.

Crutzen, Paul J. (2002). *Geology of mankind*. Nature, 415(3), 23.

Guillaume, Bertrand G. (2009). *Avoiding a 4+°C world: A challenge for democracy*, 4 degrees and beyond, University of Oxford.

Joy, Bill. (2000). Why the future does not need us. *Wired Magazine*. 8.04.

Jonas, Hans. (1984). *The imperative of responsibility: In search of ethics for the technological age*, University of Chicago Press, Chicago.

Parry, M.L.; Canziani, O.F., Palutikof, P.J. van der Linden, P.J. and Hanson, C.E. (2007). *Contribution of working group II to the Fourth assessment report of the Intergovernmental panel on climate change*, Cambridge University Press, Cambridge.

Matthew, Richard A., Barnett, Jon, McDonald Bryan and O'Brien Karen L. (2009). *Global environmental change and human security*, MIT Press, Cambridge.

Rees, Martin. (2003). *Our final hour: A scientist's warning: how terror, error, and environmental disaster threaten humankind's future in this century – On Earth and beyond*, Basic Books, New York.

Rockström, Johan; Steffen, Will; Noone, Kevin; Persson, Åsa; Chapin, Sturat; Lambin, Eric F.; Lenton, Timothy M.; Scheffer, Marten; Folke, Carl; Schellnhuber, Hans Joachim; Nykvist, Björn; de Wit, Cynthia A.; Hughes, Terry; van der Leeuw, Sander; Rodhe, Henning; Sörlin, Sverker; Snyder, Peter K.; Costanza, Robert; Svedin Uno; Falkenmark, Malin; Karlberg, Louise; Corell, Robert W.; Fabry, Victoria J.; Hansen, James;Walker, Brian; Liverman, Diana;Richardson, Katherine;Curtzen, Paul and Foley, Jonathan A. (2009). A safe operating space for humanity, *Nature*, 461(7263), 472-475.

Stern, P. C., O. R. Young, and D. Druckman. (1992). *Global environmental change: understanding the human dimensions*, National Academy Press, Washington, D.C.

Turner, B.L.; Clarck, William C.J.F.; Kates, Robert W.; Richards, J.F.; Mathews, Jessica T.; Meyer, William B. (1990). *The Earth as transformed by human action: global and regional changes in the biosphere over past 300 years*, Cambridge University Press, Cambridge.

UNESCO (2007). *Case studies on climate change and world heritage*, Paris, UNESCO World Heritage Centre.

Ward Peter D. and Brownlee Donald. (2000). *Rare Earth: Why Complex Life is Uncommon in the Universe*, Springer, New York.

WBGU, German Advisory Council on Global Change. (2007). *Climate change as a security risk*, London, Earthscan.

THE FUTURES OF CLIMATE CHANGE IN JOURNALISM

Ville Kumpu[a] & Sofi Kurki[b]
[a]University of Tampere, Department of Journalism and Mass Communication
[b]University of Turku, Finland Futures Research Centre

ABSTRACT *- Towards the end of the first decade of 21st century, climate change rose steadily on the news agenda, and during the fall 2009 Copenhagen climate summit made headlines in media all around the world. This study takes as a starting point the climate change journalism produced right before, during and after the summit in one Finnish and one US newspaper (Helsingin Sanomat and the New York Times). The study assesses the way journalism represents the future in the context of the climate summit: what kinds of images of the future are presented in the coverage, which aspects of the future implications are highlighted and what kinds of actors are allowed to comment on the future. The primary result of the study is that the summit was not used as a platform for discussion about the preferable and avoidable futures. Instead, the coverage concentrated mostly on the negotiation process leaving aside questions about the substance matter, climate change, in itself.*

Introduction and Background

An image of the future is an imaginary mental construct that individuals hold about the future (cf. Rubin 2000). Studying images of the future is an important topic of study within the futures research field as an effort to understand and explain human behavior. The importance of the images of the future is based on a notion that the beliefs individuals hold about the future in some way guides their actions in the present. The study of images of the future includes also the process of image making (Bell 1998). Despite the recent changes in media industry, professional journalism is still the core of nationally constructed communication spaces. This is true especially when concerning large scale issues with vast political relevance. Besides having political relevance climate change is definitely an issue that bears images, predictions and scenarios about the future within itself. It could be argued that as an issue it tunes any discussion towards the future and thus creates favorable conditions for journalism to discuss the future as well. In this study we have no intention to elaborate *how* the images of the future are communicated or created. The details of interactions between journalism, its audiences and other institutions in creating images of the future in a personal or societal level should be a subject of another study. In this study, we are primarily interested in making a sort of an inventory: what kind of images about the future were there to be found in journalism?

Material and Methods

As the focus of our inventory we have selected the climate change journalism in two newspapers during the 2009 United Nations Climate Change Conference (referred from here on as the Copenhagen Summit). *Helsingin Sanomat* and *New York Times* were selected as objects of the study in order to compare journalism that is situated somewhat similarly (though New York Times is insurmountable in terms of resources, in institutional terms it is situated quite similarly as *Helsingin Sanomat*) in settings that differ greatly in terms of climate politics. The newspaper material includes all stories (including news, columns, comments, editorials, letters to the editors etc) mentioning either the Copenhagen summit or climate change published before, during and after the Copenhagen summit itself10. Altogether 242 stories were collected, 167 from *Helsingin Sanomat* and 75 from *New York Times*. Of all the stories 42 % was news, 15 % letters to the editors and 12 % columns or comments by journalists.

As a method, a combination of quantitative and qualitative content analysis was used. The basic journalistic dimensions of all stories (size, section, front page connection and genre) were noted, all voices (people quoted directly or indirectly) appearing in the texts were coded in one of 28 classes in five principal groups (national political systems, transnational political system, civil society, business and scientist & experts) by the institution or group they were considered representing and finally the future orientation of the stories was investigated by estimating whether the story made some kind of a reference to future, and then whether this reference was made explicitly mentioning some future year. All the future years mentioned in the stories were noted.

The qualitative analysis was conducted to find out what was the content of the references to the future. The aim was to identify articulated images of the future from the material. References that were directly linked to the negotiated climate deal were excluded from the analysis. Such were for instance commitments to reduce emissions by x % by some future date. Also excluded were articles that did present a state of the future (such as a difference in temperature in comparison to the present or a specific level of carbon dioxide in the air in the future) but did not elaborate upon the concrete effects of such states.

Results

As mentioned, the future orientation of the stories was at first studied in a relatively simple manner: by investigating whether the story made any textually explicit references to future. More than half of the stories made some kind of a reference (vague as it may be) to future (52 % of the stories in *Helsingin Sanomat*, 65 % of stories *in New York Times*). The act of mentioning a specific year in a news text can be considered as anchoring the discussion into a more specific future context. Of the 87 stories in *Helsingin Sanomat* with any kind of a future orientation, 48 explicitly mentioned some future year. That is 55 % of the stories with some kind of a reference to future and 29 % of all stories. In New York Times 34 stories mentioned some future year that being 71 % of stories with a future reference and 45 % of all stories.

[10] The Copenhagen summit took place 7.–18.12.2009, stories for this study were collected between 1.–22.12.2009. Material was collected using electronic archives of *Helsingin Sanomat* (www.hs.fi/arkisto) and in the case of New York Times, Factiva (www.factiva.com).

Three years clearly dominate the discussions: 2012, 2020, 2050 (table 1). These are the years that were most debated in the negotiation tables as well: 2012 marks the end of the Kyoto protocol and 2020 and 2050 were the years most often used as points of reference when discussing proposed actions. Looking at the mentioned years genre-wise few interesting observations can be made. In general, reporting genres (news, reportage) make more references to future than opinionated stories (columns, comments, editorials, letters to the editor). Opinionated stories focus more on the immediate near future of 2010 and less to 2012 and 2020. On the other hand 2050 is more prominent in opinionated stories.

We may elaborate our answer on what kinds of futures were there to be found in journalism in quantitative terms by looking at what how the future orientation interacts with voices that get to speak. The question, simply put, would be *who gets to speak about the future in the climate change coverage?*

Table 1. *Years mentioned in the Copenhagen coverage of New York Times and Helsingin Sanomat*

	Reporting		Opinionated		All stories	
2010	7	6 %	5	13 %	12	7 %
2011	2	2 %	1	3 %	3	2 %
2012	26	21 %	3	8 %	29	18 %
2013	2	2 %	0	0 %	2	1 %
2015	4	3 %	3	8 %	7	4 %
2016	2	2 %	2	5 %	4	2 %
2020	45	37 %	11	28 %	56	35 %
2025	3	2 %	1	3 %	4	2 %
2030	12	10 %	2	5 %	14	9 %
2050	16	13 %	9	23 %	25	16 %
2055	1	1 %	0	0 %	1	1 %
2100	2	2 %	1	3 %	3	2 %
2109	0	0 %	1	3 %	1	1 %
Total	122	100 %	39	100 %	161	100 %

There are clearly two actor groups that dominate the Copenhagen coverage (table 2, far right column). The summit is mainly covered through political actors from different countries (national political system) but civil society (e.g. NGOs, demonstrators, men-on-the-street) is very prominent as well. Scientists and experts are quoted as well but not as frequently as the two groups mentioned above. The role of business actors in the stories is minimal. The quite small role of transnational political actors (UN, EU etc) is noteworthy. In these respects there are no notable differences in the voice groups between the two papers.

Table 2. Voice groups within different future orientations

	No future orientation		Future orientation		Specific year(s) Mentioned		All stories	
National political system	29	18 %	158	48 %	111	53 %	187	38 %
Transnational political system	8	5 %	33	10 %	21	10 %	41	8 %
Civil society	63	39 %	65	20 %	35	17 %	128	26 %
Business	6	4 %	19	6 %	12	6 %	25	5 %
Science, experts	37	23 %	47	14 %	26	12 %	85	17 %
Other	19	12 %	10	3 %	6	3 %	29	6 %
Total	162	100 %	332	100 %	211	100 %	495	100 %

There is an interesting shift between the two major actor groups when comparing stories with no future orientation with stories having any kind of a future orientation or mentioning explicit years. It seems that the more explicit the future orientation of a story is, the more it is politicians who get to speak. Civil society voices on the other hand are most prominent when there is no future orientation at all and least visible when specific years are mentioned in the stories. It is also interesting to note that scientists and experts are most prominent when there is no future orientation at all. This seems to hint that there are significant differences in different orientations and their respective actor-relations. Civil society is indeed a major part of the coverage of the summit but journalism seems to designate civil society actors to a different time-zone than the actual political decision-makers. Partly this is of course due to the nature of a summit as a political event but there is no reason to underestimate the possibilities of journalism to deviate from this summit-logic.

We can get a sense on how or why different time zones seem to be forming inside journalism by looking at the way different time orientations vary by genre (table 3). Reporting genres are clearly dominating the most future oriented coverage, especially the stories mentioning explicit years. Reportage and feature are as genres clearly not designated for dealing with the future in journalistic imagination.

Table 3. The future orientation of different journalistic genres

	No future orientation		Future orientation		Explicit year(s) mentioned	
News	43	41 %	58	43 %	42	51 %
Reportage, feature	11	10 %	8	6 %	4	5 %
Interview	2	2 %	4	3 %	2	2 %
Other reporting	9	8 %	12	9 %	11	13 %
Total reporting	65	61 %	82	60 %	59	72 %
Editorial	4	4 %	6	4 %	3	4 %
Column or comment by journalist	14	13 %	16	12 %	9	11 %
Column or comment by non-journalist	1	1 %	6	4 %	4	5 %
Letters	13	12 %	23	17 %	6	7 %
Other opinionated	7	7 %	3	2 %	1	1 %
Total opinionated	39	37 %	54	40 %	23	28 %
Unclear	2	2 %	0	0 %	0	0 %
Total	106		136		82	

It seems that the explicit future talk in the context of the Copenhagen coverage was strongly driven by the logics of power politics. Journalism echoes the importance of those specific future years considered important in the negotiation tables. Going beyond the plain numbers one may argue that this dimension was broadly characteristic for the Copenhagen coverage. The *negotiation process* was on the centre stage of the coverage and the issue, climate change, as such was pushed aside. The same logic seems to be at play when looking at who gets to speak in the stories as well. Explicit years are mostly discussed by those *inside* the negotiations. Civil society voices are most prominent when the future is not discussed at all. Partly this of course reflects the nature of the summit as a political event but on the other hand it does reveal that journalism is eager to follow such logic.

The qualitative analysis concentrated on the nature of the presented future references. The references to the future ("future states[11]" from here on) were categorized by their essential contents under four categories: 1) preferable states of the future, 2) probable states of the future[12], 3) avoidable states of the future[13], and 4) references to a possible black swan[14]. In addition, we collected proposed actions towards a preferred state of the future and criticism of the mainstream political solutions to combat climate change. This was included as, even though the stories did not present a straightforward description of the future, the underlying motivator for them was either reaching a preferred future or avoiding a dystopic one. As noted earlier, such references to the future that were made directly in the context of the summit were excluded from the analysis. These would include the majority of the futures references in the material, leaving for qualitative analysis only 30 (out of a total of 168 stories with a reference to the

[11] A state of the future is a fragment of an image of the future, describing future from a specific angle.
[12] There was considerable overlap with the probable and avoidable categories. In these cases categorization was made according to the tone that seemed dominating in the context of the whole story.
[13] The division into preferable, probable, and avoidable futures is a common framework within futures research
[14] A black swan is a term for an occurrence of a high impact, low expectancy event (Taleb 2007).

future) articles from *Helsingin Sanomat* and 18 (out of a total of 75 future related stories) from the *New York Times*.

In the Finnish newspaper *Helsingin Sanomat*, the category with the most stories was 2) states of the future that were presented as probable. These included mostly articles that could be also categorized as avoidable. However, the way the probable states of the future were presented was different from the purely avoidable stories. The probable futures often relied on calculations projecting the present trends into the future, used analogies from the past or by the selected wording implicated that the future depicted was seen as likely to unfold. The category divided into sub-categories of 2a) economic descriptions of the future, 2b) natural hazards and 2c) threats to indigenous cultures / life in especially vulnerable areas.

The subcategory of 2a) that described future on economic terms was the most prominent. Of all of the categories, it included some of the most detailed descriptions of the future. Under the category fell worries ranging from the financial burden brought about by the potential binding climate deal…

> *The aid to the developing countries will in itself cost the Finnish people 66–225 million euros by the year 2020. There are also other costs, as listed by the Government Institute for Economic Research: compared to a business as usual emission track the demand for consumption will decrease, investments to renewable energy are costly, the gross domestic product will lower as will the employment rate.*
> (A48, HS 9.12.2009, editorial)

…to the consequences of extending the cap & trade system to include air traffic in the year 2012:

> *The cap & trade system in air traffic is feared to lead to unnecessary intermediate landings. The industry fears that if the system remains enforced only within the European Union, it can bring about a chain of intermediate landing airports in the countries bordering the Union.* […] *According to the designed system, for example a flight operated by a Japanese air carrier JAL flying directly from Helsinki to Tokyo will need to have carbon permits for every flown ton kilometer. If it were to make stops in St. Petersburg, it would only be required permits for the flight from Helsinki to St. Petersburg, but not the leg of flight from St. Petersburg to Tokyo.*
> (A19, HS 5.12.2009, news story)

The subcategory 2a) had often a relatively short time span (up to 20 years into the future). Compared to the detailed calculations in the subcategory 2a), in the two other sub-categories (2b, 2c) references to natural catastrophes and threats to vulnerable cultures and areas were much less elaborated and more sketchy, often contending to list a number of calamities in a general and at times even routinely manner. Timescales were often ill-defined. Typically no specific years were mentioned.

> *For instance the basis of the Inuit hunting culture is in danger of collapsing as the arctic ice melts.* […] *The Salomon Islands are drowning to the sea. The melting rate of glaciers and arc-*

tic ice is accelerating. The developing countries dependent on agriculture are already suffering from heat, drought and severe rains. Coastal floods have increased in Finland.
(A52, HS 9.12. 2009, comment by a journalist)

Warming of the Earth will in the future bring unprecedented pressure to every nation. The worst consequences will be suffered by the poor, the young, women, as well as habitants of coastal and dry areas, and small farmers
(A49, HS 9.12.2009, column by non-journalist)

Unlike the multifaceted avoidable future, there was little variance in the preferred future state (category 1). In all the stories the good future was described as a low carbon society attained by new, green technology (in one case nuclear power).

…What if the climate change was a false alarm, but we would make drastic cuts to the carbon dioxide emissions? We would be speeding up the transition to a greener energy and traffic that we needed to do in any case. We might be paying a bit more for the energy investments in the next decades but in return we would get cleaner and more self-sufficient electricity and heating and also our breathing air would be cleansed. We could stop worrying about the rise of the oil prices.
(A6, HS 2.12.2009, letter)

Resolutions or proposed actions towards a preferred state of the future as well as criticism of the mainstream political solutions to combat climate change were targeted at various different directions, from proposing geo-engineering, to embracing reforestation plans as a boost for the creative economy, to suggesting a global one child policy.

Pentti Linkola was right on in his writing (HS letter to the editor 6.12.) demanding a one child policy to stop population growth. It is evident that three billion new people pursuing western living standards do not help stop climate change nor does it promote sustainable development.
(A63, HS 10.12.2009, letter)

Avoidable futures were formulated as threats, repeating the un-specific but gloomy style used in subcategories 2b and 2c.

[…] *Pachauri warned that hundreds of millions of people would end up as climate refugees if the emissions would not be curbed*
(A40, HS 8.12.2009, news story)

If the Copenhagen *summit were to fail, the next top-level environmental meetings would have to concentrate on the costs inflicted by the failure, measured in loss of human lives.*

(A49, HS 9.12.2009, column by non-journalist)

The *Helsingin Sanomat* material included also one reference to category 4, a possible black swan (a scenario where something rather unexpected but high in its impacts would occur):

> *Only recently Richard Betts, a climate modeler at the British meteorological institute, with his group, anticipated that the Earth could heat up to four degrees already in 50 years.*
> (A25, HS 6.12.2009, letter)

In the *New York Times* the group with the most stories was resolutions or proposed actions towards a preferred state of the future. The group was dominated by different proposals as to how the market could be used to tackle the problem of climate change and the economic downturn

> *Still, I am an Earth Race guy. I believe that averting catastrophic climate change is a huge scale issue. The only engine big enough to impact Mother Nature is Father Greed: the Market. Only a market, shaped by regulations and incentives to stimulate massive innovation in clean, emission-free power sources can make a dent in global warming. And no market can do that better than America's. Therefore, the goal of Earth Racers is to focus on getting the U.S. Senate to pass an energy bill, with a long-term price on carbon that will really stimulate America to become the world leader in clean-tech. If we lead by example, more people will follow us by emulation than by compulsion of some U.N. treaty.*
> (B58, NYT 20.12.2009, column by a journalist)

Also the few preferable images of the future (category 1) included putting the market forces to use in combating climate change and other environmental problems

> Hence *Coca-Cola's survival compels it to be deeply concerned with problems of water scarcity, energy, climate change and agriculture. One company goal is to make its plants water-neutral, returning to the environment water in quantities equal to the amount used in beverages and their production. Another goal is to work on the conservation of seven of the world's river basins, including the Rio Grande, Yangtze, Mekong and Danube -- all of them sites of major environmental concerns besides supplying water for Coca-Cola.*
> (B3, NYT 6.12.2009, column by non-journalist)

The *New York Times* material did not contain direct black swans (category 4) but it did use the concept in one story:

> *Soon after Suskind's book came out, the legal scholar Cass Sunstein, who then was at the University of Chicago, pointed out that Mr. Cheney seemed to be endorsing the same "precautionary principle" that also animated environmentalists. Sunstein wrote in his blog: "According to the Precautionary Principle, it is appropriate to respond aggressively to low-probability, high-impact events -- such as climate change. Indeed, another vice president -- Al*

Gore -- can be understood to be arguing for a precautionary principle for climate change (though he believes that the chance of disaster is well over 1 percent).
(B17, NYT 9.12., column by non-journalist)

The avoidable futures followed usually the same lines that were detected also in the *Helsingin Sanomat*, slightly unspecific but very unattractive options in the future that were not specified by any years or dates:

Politics, ideology and economic interests interlace the debate, and the stakes on both sides are high. If scientific predictions about global warming's effects are correct, inaction will lead at best to rising social, economic and environmental disruption, at worst to a calamity far more severe. If the forecasts are wrong, nations could divert hundreds of billions of dollars to curb greenhouse gas emissions at a time when they are struggling to recover from a global recession.
(B65, NYT 7.12.2009, news story)

At the same time, he made clear that the United States was prepared to join other industrialized countries both in cutting their own greenhouse gas emissions and in giving aid to the poorest and most vulnerable countries to deal with rising seas, drought and other phenomena that are expected to worsen as the planet warms.
(B21, NYT 10.12.2009, news story)

The probable futures array was two-fold: there were the probable/avoidable stories…

If the water problems are not solved, El Alto, a poor sister city of La Paz, could perhaps be the first large urban casualty of climate change. A World Bank report concluded last year that climate change would eliminate many glaciers in the Andes within 20 years, threatening the existence of nearly 100 million people.
(B39, NYT 14.12.2009, reportage)

…But unlike in the *Helsingin Sanomat*, NY Times found also probable and preferable futures available:

In human affairs politics will always trump science. Nothing significant will be done until conditions become much worse. Yet a nonbinding agreement on emissions may prove surprisingly productive. If climate temperatures continue to rise, nations will see for themselves that more must be done, and may compete with one another to reduce emissions, going beyond what would have been mutually acceptable in 2009. The know nothings will evaporate. Genuine cooperation will grow from grim necessity.
(B48, NYT 22.12.2009, letter)

Discussion and Conclusions

From the perspective of this study, it seems that climate change summit is not the optimal context for journalism to discuss the preferable and avoidable futures. Instead of climate change as an issue, the summit in itself, as a political event and the negotiations as a process were at the focal point of journalism. This might a reflection of the state of the climate change debate. It seems that in both papers, the premises of climate change are commonly accepted at least in the way that it is not considered necessary to repeat the basic facts about the issue itself in great detail. Considering the future it then follows that while both of the newspapers give a rather nuanced account of the different interests of and conflicts between the key negotiators, the future consequences of the deal are left to sketches that at times had a feel to them that they were used as mere rhetorical devices to emphasise the twists and turns of the negotiations. The question left to further study then is, whether the context of the summit is the crucial factor or if the nature of journalistic process is the main reason behind the result. There seems indeed to be a strong argument that a kind of a journalistic meta-language of summit journalism directed the coverage. In this sense, the issue at stake is not a decisive factor. Same kinds of stories would be produces in all somewhat similar events, be it the Olympics, or the European song contest.

However, the kind of summit we have investigated brings together an enormous amount of actors who would be able to provide journalists with knowledge, views, arguments and visions of those consequences in the future. Based on our material, journalism did not make much out of these potential impacts. In the case of Copenhagen this was underlined by the fact that both papers had several correspondents present. By using so little of this potential amounts to making a conscious decision to ignore the future aspect of the topic. In this sense *getting the deal now* was the driving factor in narrating the coverage and not, for example *what will happen if* or *how should we cope*.

Despite the generally bland orientation towards the future, there were still several references to the future among the stories. Looked at quantitatively it seems that the people that were trusted to provide their impression of the direction of the future came mostly from the political power elites. The future years most frequently referred to were the important dates on the agreement, 2012 and 2020. Also in the qualitative investigation, most images of the future reflected rather conventional wisdom about the consequences of climate change. Failure in finding agreement on cutting emissions would result in all sorts of natural catastrophies, however the sufferers of these were depicted to be mostly in the developing world. Also, the specific nature of the natural hazards as well as the potential time when they were to be expected was not defined. Little reference to the consequences for the lives of the assumed readership was made except for in economic terms as income transfers to the developing countries.

It is notable that the most detailed and also most common were the articles describing the economic burdens brought about either by the forged deal or the possible effects of climate change. The most often cited solution to reach temperature goals was by technology (*Helsingin Sanomat*) and by the cap & trade mechanism (*New York Times*). Both the quantitative and the qualitative analysis point to the direction that journalism was quite willing to adopt the (quite one-sided) image of the future provided by the political elites, emphasizing the market mechanism and technological solutions. Neither of the papers, for example, delved very deep on the fundamental causes of the rising co2 –levels, for instance the economy based on the paradigm of continuous growth was not commented upon, despite numerous demonstrators at the summit were addressing it as a major problem. The straightforward interpretation of the re-

sults would be that the summit as a frame was somehow prohibitive to stories presenting different alternatives for the future. When the main story was about an inter-governmental solution to climate change, it proved too difficult to mix with competing approaches.

References

Bell, Wendell (1998) Making people responsible: The Possible, the Probable, and the Preferable. *American Behavioral Scientist* 42(3), 323-39.

Rubin, Anita (2000) Growing up in Social Transition: In Search for a Late-modern Identity. Annales Universitatis Turkuensis. Ser. B. Tom. 234. Humaniora. University of Turku, Turku. 204 p.

8. SECURITY AND DEVELOPMENT

FORGOTTEN INFRASTRUCTURE – IN THE QUEST FOR DEVELOPMENT, SUSTAINABILITY AND SECURITY

Dr. Jarmo J. Hukka[a], Dr. Tapio S. Katko[b], Dr. Pekka E. Pietilä[b], Dr. Osmo T. Seppälä[c] & Dr. Eija M. Vinnari[d]

[a]Ramboll Finland Oy, International Operations

[b]Tampere University of Technology, Department of Chemistry and Bioengineering

[c]Finnish Water and Waste Water Works Association

[d]University of Turku, Turku School of Economics, Department of Accounting and Finance

ABSTRACT – *Critical Infrastructure Protection or CIP is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. Traditionally, mainly natural disaster or terrorism threats are discussed. Yet, CIP must be widened to cover also so-called normal circumstances, where especially visionary thinking and strategic decision-making concerning the funding of rehabilitation, replacement, and operations and maintenance has become vital, in particular due to the longevity of most infrastructure assets.*

Introduction and Background

Critical Infrastructure Protection or CIP is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. In May 1998, President Bill Clinton issued Presidential directive on CIP. This recognized certain parts of the national infrastructure as critical to the national and economic security of the United States and the well-being of its citizenry, and required steps to be taken to protect it.

Yet, traditionally we have been thinking mainly natural disaster or terrorism threats, but the CIP concept should be widened to cover also the so-called normal circumstances, where especially strategic decision-making concerning the funding of rehabilitation, replacement, and operations and maintenance of infrastructure has become vital.

Contemporary, well-located and -functioning infrastructure is the backbone both of the sustained economic development and viable economic activities of any nation. Sometimes the word “economic infrastructure” is used, when energy, roads, railways, ports, airports, water resources management, water supply and sanitation, waste management and information and communication technology (ICT) are discussed.

On the other hand, in order to safeguard the healthy living conditions and to protect the environment, properly built and operated water supply and sanitation (WSS), and waste management infrastructure must be in place. In developing economies presently at any given time a half of the beds in the

hospital and health centers are occupied by the patients suffering from diseases caused by unsafe drinking water and unhygienic living conditions. Every year the poor people are losing about 5 billion working days because of inadequate WSS infrastructure and services. In addition, countries with the greatest economic infrastructure needs are often the least attractive to investors.

The healthy living conditions and the economic development supported by the adequate and functioning infrastructure are essential form the point of view of individual, community, national, regional and global security.

Africa has low access to basic water supply and sanitation services, i.e. 36% (341 million people) have no access to water supply and 62% (583 million people) have no access to sanitation. Africa is not on track to meet water services related Millennium Development Goals (MDGs), and it's badly off-track in meeting sanitation services related MDGs (Jallow 2009). Figure 1 and 2 show the worldwide use of improved sanitation and drinking-water sources in 2008 (World Health Organization and UNICEF 2010).

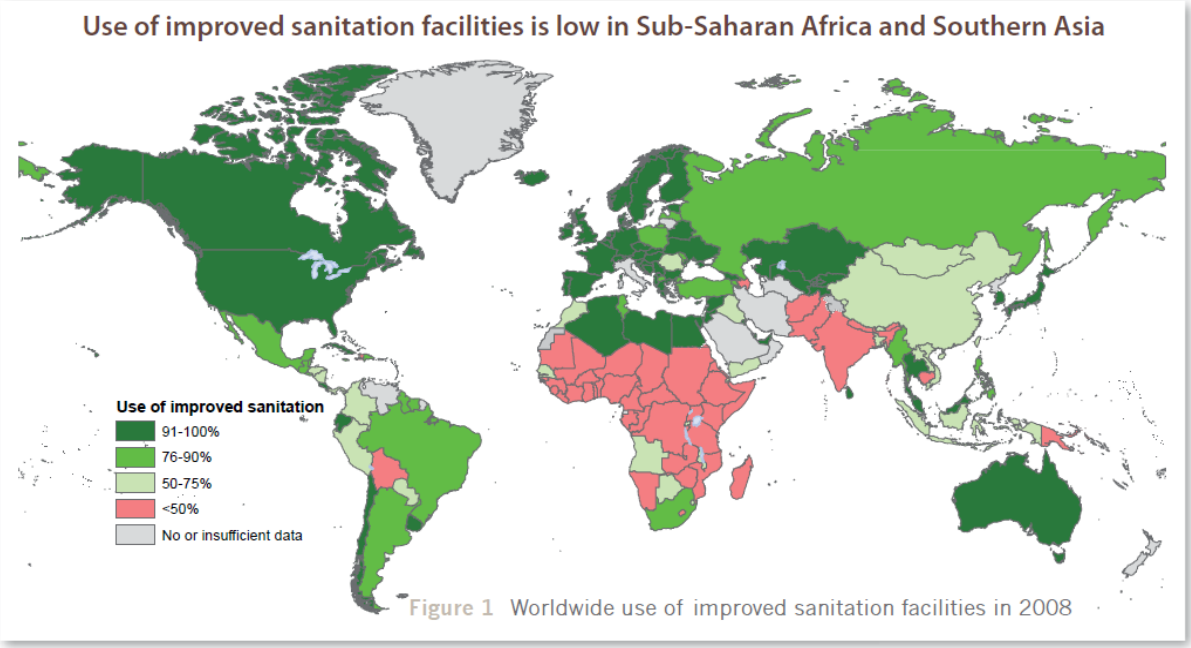


Figure 1. Worldwide use of improved sanitation facilities in 2008.

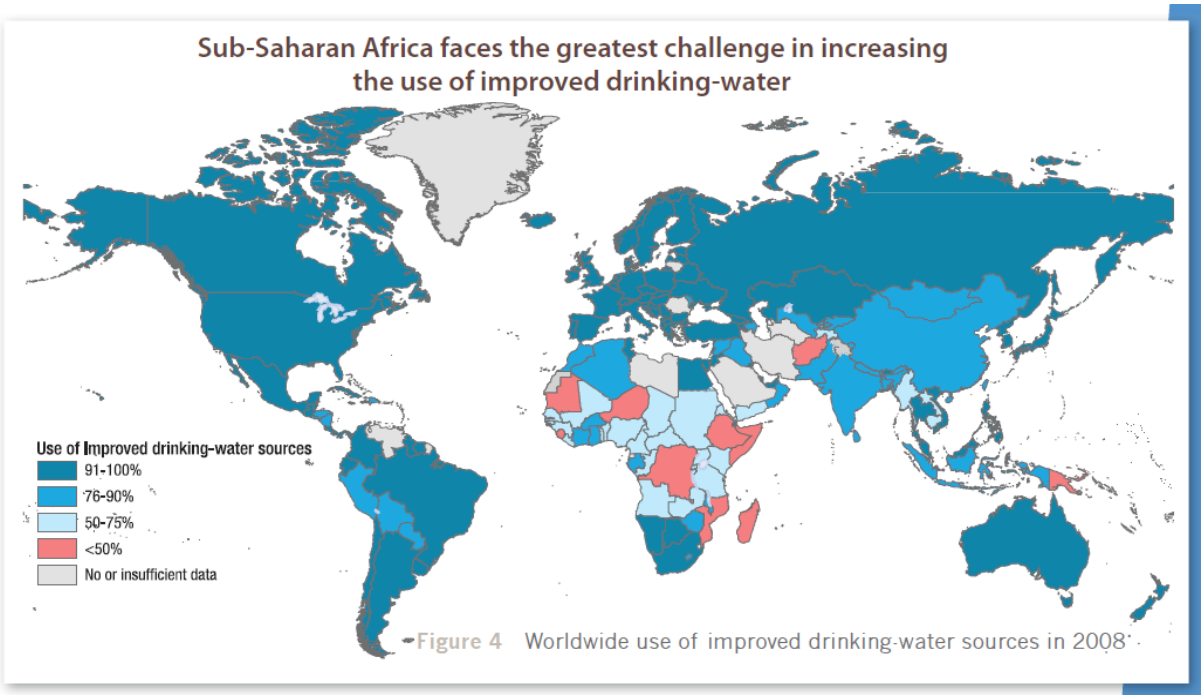


Figure 2. Worldwide use of improved drinking-water sources in 2008

A recent study (Foster and Briceño-Garmendia 2009) in 24 African countries shows that the poor state of infrastructure in Sub Saharan Africa (SSA) decreases national economic growth by two percentage points every year and reduces business productivity by as much as 40 percent. The study reveals that SSA has the weakest infrastructure in the world, but ironically Africans in some countries pay twice as much for basic services as people elsewhere.

The report estimates that USD93 billion are needed every year over the next decade, more than twice what was previously figured out. The new estimate amounts to about 15 percent of the SSA's gross domestic product (GDP), comparable to what China invested in infrastructure over the last decade. The study found out that existing spending on African infrastructure is much higher than previously known, USD45 billion a year. Surprisingly, most of this is locally financed by the citizens in SSA. The study also found that there is also considerable wastage to address; a number of efficiency improvements could potentially expand the available resources by a further USD17 billion.

Yet, even if major efficiencies are gained there is still a funding gap of USD31 billion every year, much of it for power and water infrastructure in fragile states. The funding gap is daunting for the region's low-income countries (who would need to spend an additional 9 percent of their GDP) and particularly for the region's fragile states (who would need to spend an additional 25 percent of their GDP).

In Africa, there is also low utilization of water resources, i.e. about 4% available water is used, about 6% of cultivated area is irrigated, and less than 6% of hydropower potential developed. Furthermore, there is only about 200 m3/capita storage compared to about 6 000m3/capita for USA (Jallow 2009). With more than 60 transboundary rivers in Africa, developing large-scale infrastructure to manage water use and avoid conflicts is a huge challenge. Over the last 40 years, only 4 million hectares of new irrigation have been developed, compared to 25 and 32 million hectares for China and India respectively (Foster and Briceño-Garmendia 2009).

Since the river basins in many regions in Africa are shared by two or more countries, the use and further development of water resources requires that adequate agreements based on the principles of international water law (Helsinki Rules 1966) as well as management practices on transboundary waters are in place. This is a necessity also to ensure peace and security among the riparian countries. If these mechanisms are not there, the potential investors might consider the situation too risky. This would mean that the investments are not made or they become more costly.

Generally speaking, in the developed economies the infrastructure is still adequate to support the business activities and the well-being of the societies. Yet, for example in the United States and in Finland we are not investing enough in rehabilitation and replacement of the aging infrastructure. This indicates clearly, that not only in Africa, but also globally, decision-makers are not aware of the importance of the investments in infrastructure or they close their eyes in front of these absolute necessary investments. Furthermore, this indicates that the decision-makers in the developed world might not consider the increasing the support for the infrastructure investments in the developing economies, when they do not even see the need in their own better-off countries

In US, according to Grigg (2006, 243), the approximately 0.6 million kilometers of US water distribution systems will continue to age and at today's renewal rate will certainly deteriorate in condition. Piped water systems are confronted by more risks, including intrinsic decay and failure, natural disasters, accidents, malevolent threats from insiders or outsiders, and collateral damage when other infrastructure systems go down.

A study (Hukka and Katko 2007) shows that the funding gap in water and sanitation is EUR 1 000 million, whereas the total value of the WSS and waste management infrastructure is estimated to be EUR 8 000 million. The conclusion is that we need to increase the investment level from the current annual level of about EUR 250 million up to EUR 500 million for the next 15-20 years. Even this increase would mean that we would be only able to maintain the current status of our WSS infrastructure.

In Finland, over 30% of water supply pipes and 37% of sewer pipes are already over 30 years old. The current rehabilitation and replacement level is inadequate. The level should be increased from the current annual level of EUR 120 million to about EUR 360 million (ROTI 2010).

One of the reasons for the current low level of the rehabilitation and replacement in the biggest Finnish water undertakings is that their owners, the municipalities, are withdrawing rather large amount of money from the undertakings as the rate of return. This "hidden tax" is used for financing other municipal operations. Table 1 shows the rate of return calculations for the different utilities (Vinnari 2006a, 163).

Table 1. *The average rates of return of the owner municipalities of 15 large water services undertakings in Finland 1997-2003, calculated from the data provided by the utilities in their annual financial reports.*

Water undertaking	Population served in 1999	Compensation for owner's basic capital, %[1)]	Total owner's rate of return, % of turnover[2)]
Helsinki Water	549 840	9.0	45.5
Espoo Water	203 490	10.0	38.8
Tampere Water	186 210	11.9	29.3
Vantaa Water	165 850	8.2[3)]	28.7[3)]
Turku Water Utility	165 220	7.8	27.8
Oulu Water	117 314	18.0	23.7
Kuopio Water	82 216	5.5	17.5
Jyväskylä Water	77 530	13.2	27.1
Pori Water Utility	73 934	4.5	18.7
Vaasa Water	56 247	5.8	15.3
Lappeenranta Water Utility	53 724	6.0[4)]	14.9[4)]
Kotka Water	52 900	5.2[5)]	21.0[5)]
Joensuu Water	50 815	12.0	31.5
Porvoo Water	38 930	0.0	0.0
Rauma Water	37 300	2.0[6)]	8.0[6)]
AVERAGE	127 400	7.9	23.2

1) Return on basic capital divided by basic capital
2) Sum of return on basic capital, loan installments, loan interest payments, and other regular payments to the municipality, divided by turnover
3) Independent accounting only from 2002 onwards
4) Independent accounting only from 2003 onwards
5) Data available for years 1999-2003
6) Data available for years 1998-2003.

On the other hand, Seppälä, Rodiqi, Nyanchaga & Hukka (2004) argue that most water utilities have traditionally not been very futures oriented, and in practice not very interested in the ethical aspects of socially important decisions regarding water services provision and production. Utilities also do not actually manage their knowledge and information processes well, although these are the most central elements for their long-term performance and success.

Water utilities and other water services organizations and their supervisory and management bodies are on average not well aware of the theoretical basis and concepts of visionary and knowledge management, and do not commonly utilize established VM and KM methodologies and tools in their operations.

Discussion and Conclusions

In SSA, but also to some extent in developed economies, there is capability and capacity to diagnose the existing situation, but we argue that what is missing by large is the lack of understanding among various stakeholders how to benefit from futures research. We highly recommend that the futures research approaches, methodologies and practices should be used to help the decision-makers on the way towards identifying sustainable development paths and security based inevitably on the critical infrastructure protection.

Thus, an integrated framework consisting of visionary and knowledge management is needed to conceptualize and improve water utility operations. Through visionary management the long-term development of utilities can be ensured, and through knowledge management the utility's human capital can be sustained – including critical knowledge and tacit knowledge.

In the SSA context, the financing situation is somewhat more complex than in developed economies, since in addition to huge funding gap in greenfield investments, there is a large and rapidly increasing need for closing the funding gap for rehabilitation and replacement of existing infrastructure as well as the need for closing the efficiency gap. In practice, this means that in order to ensure sustained critical infrastructure in SSA the needs are relatively speaking greater than in developed economies. Particularly with the prevailing global financial crisis, investing in African infrastructure is critical for Africa's future.

In Finland, as well as in many other countries including the nations in the SSA, the properly arranged WSS asset management structures, policies, regulations, systems and practices would create the enabling environment for better strategic decision-making concerning both the investments and efficiency improvements.

Therefore the regulatory approaches adopted in some countries should be examined thoroughly and applied into WSS service production (Table 2, Vinnari & Hukka, 2009, 21).

Table 2. Comparison of international asset management policies.

Country	Fixed asset ownership	Policy driver	Main organizations involved	Asset management planning
England and Wales	Private	Water Industry Act 1991	National regulator	Required by regulator. Currently five-year plans, anticipated future requirement 25 years.
Australia	Public	Accounting Standard 27, CoAG principles	State regulators; professional associations	Required by some of the regulators. Length varies according to state.
New Zealand	Public	Local Government Act 1989; 2002	Local governments, professional associations	Statutory minimum requirement 10 years; in practice up to 40 years.
United States	Mostly public	GASB 34	EPA, professional associations	Not specified.

The above recommended regulatory approaches and a practical asset management system defined in Table 3 (Vinnari 2006b, 34) should also be considered to be used, in addition to the WSS infrastructure management, in other water infrastructure, e.g. hydropower, irrigation systems management. This systemic and systematic approach would give a practical tool for better asset management and performance improvements.

Table 3. Components of Seattle Public Utilities (SPU) Asset Management System.

Component	Implementation Activity
Define service levels	Annual customer surveys, stakeholder interviews
Learn about risks	Tracking and tagging of most critical assets by probability of failure/consequence analysis; lower risks by rehabilitation, operations and maintenance
Focus on life cycle costs	Assess life-cycle costs and benefits of each planned project/investment
Use triple bottom line	Prioritize projects/investments based on societal, economic and environmental impacts
Optimize data and data systems	Inventory of technical characteristics, age, location, maintenance history, condition and current value of each asset component
Create strategic asset management plans	Description of current condition of asset components, and operations, maintenance and rehabilitation strategies; risk management plans for operational and economic risks
Clarify roles and responsibilities	Define work team and individual responsibilities, responsibility areas and decision-making authorities
Make large investment decisions via asset management committee	Meet once a week, analyses and finances large investments (> eur 200,000), ensures that decisions are based on life-cycle cost and trible bottom line principles, approves project plans, decides customer service and environmental standards

References

Foster, V. – Briceño-Garmendia, C. (eds.) (2009) *Africa's Infrastructure: A Time for Transformation*. The Agence Française de Développement and the World Bank. 355 p. http://www.infrastructureafrica.org

Hukka, J.J. – Katko, T.S. (2007) (Original in Finnish) Vesihuollon haavoittuvuus. *Vulnerability of water services and critical infrastructure protection*. The Foundation for Municipal Development. Available at: www.kaks.fi or http://www.polemiikki.fi/files/1133-25459_TutkJulk58.pdf. 148 p.

Jallow, S. 2009. *African Development Bank Water Sector Activities*. Presentation at Finland Water Forum. 19 October 2009. Helsinki, Finland.

Grigg, N.S. 2006. *Ready or not? Disaster preparedness and emergency response in the water industry*. Journal AWWA. Vol 98, no 3. pp. 242-255.

Seppälä, O.T, Rodiqi, I., Nyanchaga, E.N. – Hukka, J.J. (2004) *Visionary Leadership and Knowledge Management in Water Service*. pp. 279-300 in: Seppälä, O.T. 2004. Visionary management in water services: Reform and development of institutional frameworks. Tampere University of Technology. Publications 457. 300 p.

Vinnari, E. (2006a) *The economic regulation of publicly owned water utilities: The case of Finland.* Utilities Policy 14 (2006). Elsevier Ltd. pp. 158-165. <www.sciencedirect.com>

Vinnari, E. (2006b) (Original in Finnish) Vesihuoltolaitosten käyttöomaisuuden hallinta – oppia Yhdysvalloista. *Asset management in water utilities – Lessons learned from US*. Finnish Journal for Professionals in the Water Sector. Vol. 47, No 6. pp. 33-36

Vinnari, E.M. – Hukka, J.J. 2009. *An international comparison of the institutional governance of water utility asset management and its implications for Finland*. IWA Publishing. Water Policy Uncorrected Proof (2009) pp. 1–18.

World Health Organization – UNICEF (2010) *Progress on Sanitation and Drinking-water: 2010 Update.* 56 p.

http://www.who.int/water_sanitation_health/publications/9789241563956/en/index.html

ROTI (2009) Rakennetun omaisuuden tila. *State of the Built Environment – Finland*

http://www.roti.fi/fin/yhdyskuntatekniikka

RECENT FFRC eBOOKS

4/2011	Heinonen, Sirkka - Keskinen, Auli & Ruotsalainen, Juho. RIIHI – radikaalit innovaatiot ilmastonmuutoksen hillitsemiseksi. RIIHI-tulevaisuusklinikan tulokset.
3/2011	Rubin, Anita & Siivonen, Katriina: Kärjet tekevät aina reikiä seiniin, muuten ilma ummehtuu. Osallisuuden luova voima.
2/2011	Heinonen, Sirkka & Ruotsalainen, Juho: Kestävä monipaikkaisuus. Sitran Tulevaisuusklinikan 10.12.2010 tulokset.
1/2011	Turunen, Jenny –Snäkin, Juha-Pekka – Panula-Ontto, Juha –Lindfors, Heikki –Kaisti, Hanna –Luukkanen, Jyrki – Magistretti, Stefano & Mang, Chinda. Livelihood resilience and food security in Cambodia – Results from a Household Survey.
8/2010	Lauttamäki, Ville & Heinonen, Sirkka: Vähäisten päästöjen Suomi 2050. Raportti ilmasto- ja energiapoliittisen tulevaisuusselonteon skenaario-työstä.
7/2010	Varho, Vilja & Joki, Laura: Suomen liikennesektorin tulevaisuus. Ensimmäisen Delfoi-kierroksen perusteluja.
6/2010	Siivonen, Katriina: Taiteen särmällä nuorille hyvinvointia. Sitoumuksia ja toiminta-ajatuksia nuorten tueksi.
5/2010	Heinonen, Sirkka: Kurkistuksia kaupunkiasumisen tulevaisuuksiin. Tulevaisuusklinikan 14.6.2010 tulokset.
4/2010	Nurmi, Timo – Vähätalo, Mikko – Saarimaa, Riikka & Heinonen, Sirkka: Ubitrendit 2020: Tulevaisuuden ubiteknologiat. Kehityskulkuja, sovelluksia, trendejä sekä heikkoja signaaleja.
3/2010	Ahvenainen, Marko – Heinonen, Sirkka & Hietanen, Olli: Suunnittelu- ja konsulttialan kehitys, toimintaedellytysten arviointi ja kilpailukyvyn parantaminen -hankkeen loppuraportti. Liiteosa.
2/2010	Hietanen, Olli: Onnellinen Varsinais-Suomi – eli visio ekologisesti, taloudellisesti, sosiaalisesti ja kulttuurisesti kestävästä Varsinais-Suomesta.

FFRC eBOOK 5/2011

Burkhard Auffermann & Juha Kaskinen (editors)

SECURITY IN FUTURES – SECURITY IN CHANGE

Proceedings of the Conference “Security in Futures – Security in Change”,
3-4 June 2010, Turku, Finland

ISBN 978-952-249-063-6
ISSN 1797-132

Turun yliopisto
University of Turku

TULEVAISUUDEN TUTKIMUSKESKUS