DESSI

Decision Support on Security Investment

Grant Agreement no. 261178
Supporting activity acronym: DESSI

Activity full name:
Decision support on security investment

Deliverable 2.3 Dimensions in Security Investments

Due date of deliverable: 30th of September 2011

Actual submission date: 31st of October 2011

Start date of activity: January 2011

Duration: 30 months

Revision: Draft 1

Change Records

Version	Date	Change	Author
1	31.10.11		Johan Cas; Partners

Partners

The Danish Board of Technology,
Copenhagen, Denmark
Contact: Lars Klüver
lk@tekno.dk
www.tekno.dk

Peace Research Institute Oslo
Oslo, Norway
Contact: Peter Burgess
Peter@prio.no
www.prio.no

The Norwegian Board of Technology
Oslo, Norway
Contact: Tore Tennøe
tore.tennoe@teknologiradet.no
www.teknologiradet.no

Association for Sociological Research and Consulting
Munich, Germany
Contact: Reinhard Kreissl
reinhard.kreissl@irks.at
http://www.vsfb.de/

Institute of Technology Assessment,
Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Table of Contents page

Preface

Decision support on security investment

Through the last decade investments in safeguarding European citizens have increased substantially.

In the decision making processes leading to investments, the security dimension often overshadow other important societal aspects, such as individual rights, and other significant social, political and economic implications. This development has been described as a securitization of society, strongly affecting areas such as transport, public space, health care etc. Security investments are seemingly immediate responses to specific threats and hazards. The decision making processes tend to be technology driven and often show signs of incomplete considerations regarding societal implications.

A method for decision support

The EU commission has financed the DESSI project which will be developed by a consortium of partners from Denmark, Norway, Austria and Germany. The decision support system developed by DESSI will be launched in 2013.

DESSI will develop a method for decision support. The purpose is to provide a versatile assessment process, which takes into account the many and complex societal dimensions of a security investment. DESSI will make it possible for the user to compare different ways of counteracting different threats. The comparison will be made by looking into a set of dimensions, such as security gain/loss, impact on fundamental rights and ethical aspects, legal framework, social implications, acceptability, political significance and economy.

Participatory and transparent process

Security investments affect many different groups in society. Therefore, it is important that the investment is discussed in a participatory process, involving different groups. Using DESSI, different groups will be invited to assess the investment against different future scenarios, securing an open and transparent process.

The development of an internet-based tool will make the DESSI method available for potential users. The tool will be easy-to-use, and lead the user through the assessment method.

Chapter 1 Introduction

DESSI aims at assessing possible consequences and impacts of planned security investments or measures from a broad societal perspective. The objective is to support a systematic and holistic evaluation and comparison of security related Investments and their alternatives.

Any attempt to reflect societal complexity in a meaningful way must necessarily reduce this complexity and focus on a limited number of perspectives and aspects. DESSI assesses possible consequences and impacts of planned security investments by means of different dimensions. These dimensions concentrate on different aspects, representing specific classes of features of the security investments under consideration and specific impacts on other spheres of society, economy, law and policy which DESSI aims to take into consideration. These dimensions are organized according to the areas of social life, which are actually or potentially impacted and regarded as crucial in assessing the relative success of a security investment. Dimensions are parameters that decision-makers think or should think implicitly or explicitly. The systematic approach taken by DESSI that none of these dimensions is excluded in decision-making beforehand, that is before it is checked whether a certain security investment decision concerns these dimensions.

The DESSI assessment process distinguishes between the following dimensions:

- Security gain/loss
- Infringement upon Fundamental Rights and Ethics
- Legal Framework
- Social Implications
- Acceptability
- Political Significance
- Economic impacts

These dimensions are not designed as being completely independent from each other; if you change your perspective you can still see a certain feature, although it might have moved from the center of attention to the margin of the “lens coverage”. Many mutually interdependencies are obvious: for instance, infringements upon fundamental rights are probably reflected in the legal framework, social implications and increase political significance. The ranking of the dimensions does not imply a different importance or hierarchy of dimensions; there are, however, two dimension having an overruling character, Security gain/loss and Infringement upon Fundamental Rights. The first one is more related to practical and pragmatic reasons: if the planned security investment does not show or cannot plausibly prove a positive security gain/loss balance than all the other dimensions should become superfluous and the particular planned investment be cancelled. Infringement upon fundamental rights are the second exception: if an intended security measure is in conflict with fundamental rights and cannot prove that it is proportional and necessary in a democratic society a detailed analyses of the other dimensions also becomes superfluous. The rest of the dimensions are not ranked.

Whereas it is necessary to consider all dimensions in decision-making on security investments or measures, the dimensions need to be broken down from the high level of abstraction into more practical and operational units for the assessment and comparison of concrete cases. Therefore a preliminary set of criteria (or indicators) will be developed for each description of dimensions. These criteria will feed into further theoretical and practical

studies, involving experts, users and stakeholders in the field of security investments and measures.

This document is the second deliverable of WP2. It will serve as input for the second expert and end user workshop in WP2, D2.4, a workshop that will qualify the preliminary sets of criteria that has been suggested for the dimensions. In the final deliverable, D2.6, the dimensions and criteria will be further elaborated and prepared for operationalization in the DESSI web tool.

Chapter 2 Security gain/loss

Does the security measure or investment enhance objective or perceived (subjective) security?

Security is an opaque concept and notoriously difficult to measure. To grasp a gain or loss of security, the most general approach would be to assume a change of state, be it mental, cognitive, physical or discursive. Using this 'change of state' as a vantage point, we assume that security can be measured in terms of differences. This has an important implication: security is a relative concept. It is possible to identify a change from more secure to less secure or vice versa in a given context, yet, there is no absolute or objective scale for security. Having defined security as a relational, term we can distinguish different dimensions for the measurement of security gains or losses (hereafter referred to as SGL). The key question, when investigating the implications of a given security investment is: what kinds of effects will the investment have on the many facets of security. Any assessment of SGL is a projection of future developments and cannot reach a status beyond informed guessing. Having that said, we propose different aspects of security to be taken into account when assessing SGL.

We put forward three perspectives for the assessment of SGL: (a) subjective or perceived security; (b) objective security; and (c) security as a discursive frame. Each of these perspectives points to a specific research tradition, covering disciplines such as social psychology, social and political theory and sociology. To understand whether a given Security Investment entails SGL all of the abovementioned perspectives have to be considered. Depending on the type of security problem under investigation these perspectives will have different priorities.

(a) To assess SGL from the perspective of subjective or perceived security is a tricky business since subjective security, perceived as a mental state, is dependent on other factors, such as individual risk awareness, sensitivity, knowledge etc. If a person is exposed to the question whether she feels secure, she will activate a mental frame of reference to look at the world in terms of secure/insecure, which produces a paradox: asking the security question will create insecurity (or at least doubts about subjective security). In terms of assessing SGL from the perspective of subjective security, the key question is, whether a given security investment will have an effect on the mind-sets (or frame of reference) of individuals exposed to the security measure under investigation. This measurement also heavily depends on individual set-ups/levels of awareness/attitudes/mental states, such as being not attentive to or ignoring threats, hazards and risks, being in a settled state of ontological security and being aware of or even haunted by security risks, threats or hazards, or regarding abuse of state power or terrorist attacks as a dominant source of threats.

Generally, we suggest that if a person is feeling secure before a security investment is implemented and insecure after the investment, the SGL is negative, i.e. there is – from the perspective of subjective security – a loss of security. Whether this is in itself to be seen as a positive or negative effect depends on the context. If the security investment is designed to make individuals more alert (and thus increase subjective insecurity) a loss of subjective security can be seen as a positive overall net effect. The relation between perceived and objective security is complex and has to be considered very carefully in each case under investigation.

(b) Objective security is measured from the perspective of the detached outside expert observer. SGL can be calculated from this perspective on the basis of probabilities and quantifiable expected costs of future damages. This probabilistic concept of security, based on risk assessments, allows for very detailed and complex calculations, based on equations and assessments taking into account a wide range of parameters and factors. This approach, although sophisticated in detail and scope, nonetheless has its limitations, since the other less easily measurable perspectives (perceived/subjective security and security as discursive frame) have to be taken into account. While an assessment of SGL for a given security investment from the perspective of objective security may yield positive results it may produce negative effects from the perspective of subjective and discursive security. Looking at SGL from the perspective of objective security is important and can produce valuable information to assess a given security investment. Nonetheless the results have to be measured against the two other perspectives.

(c) Security seen from the perspective of a discursive frame cuts across the other two perspectives. Whereas subjective / perceived security focuses on the dynamics of psychological processes, and objective security on the dynamics and operation of complex techno-social systems, security as a discursive frame addresses processes that have been analysed under the heading of “securitization”. Securitization provides the most comprehensive perspective when looking at gains and losses of a given security investment. Securitization is at the collective or societal level of public discourse what increased perceived insecurity is at the level of the individual. Both dimensions can interact.

These three perspectives on SGL capture the relevant issues at different levels of abstraction. They have to be broken down in specific ways, depending on the type of security problem and kind of investment under scrutiny. In order to adapt this abstract framework we list a number of questions that can be of relevance for the assessment of SGL and different security investments for a given security problem.

When investigating SGL from the perspective of subjective or perceived security it is important to take into account a number of different roles or professional contexts. Experts and professional security workers will usually display reactions that are different from the laypersons’ perspective. For both groups SGL from the subjective security perspective has to be seen in a specific way: Whereas a layperson typically will experience a subjective security loss, when confronted with a new security measure, an expert or security worker may feel more secure and experience an increased perceived security in his daily work routine. This again may have a detrimental effect, since it can lead to a decline in alertness. In terms of perceived security we get something like this:

	Subjective security increased	**Subjective security decreased**
Layperson, client	SGL typically positive	SGL typically negative
Expert, security worker	SGL typically negative	SGL typically positive

Table 1

From the perspective of objective security a number of distinctions can be applied when assessing SGL. Gains and losses can be investigated in terms of costs (financial security), technological robustness (safety, technological resilience), system stability, vigilance etc.

Security investments can be measured and compared against each of these classical aspects.

Finally from the perspective of securitization the SGL will look different with the researcher conducting the assessment. Actors who support a securitized view of the field under investigation will see the world differently from those who hold a different view. So securitization or security as discursive frame probably should be treated as a kind of “meta” dimension or perspective used to critically assess the SGL scores developed from the other two perspectives (perceived and objective security).

Chapter 3 Infringement upon Fundamental Rights and Ethics

This DESSI dimension assesses whether security measures potentially infringe upon fundamental rights as recorded in the European Charter of Fundamental Rights and to what extent security measures follow a general set of ethical norms. This chapter illustrates what infringement upon fundamental rights and ethics could mean and suggests categories of rights and ethics which should be referred to when analyzing potential ramifications of security measures.

Whereas fundamental rights seem clearly formulated, the interpretation of those rights can divert. Additionally are certain security issues notoriously difficult to solve, so that boundaries between legality and infringement upon rights seem blurred (e.g. when counter-terrorism "weighs" heavier than rights to fair trial and defense), paving the way for 'states of exceptions'. A classic argument for those committing the infringement upon fundamental rights in the name of security refers to the applicability of laws, claiming a lack of sufficient jurisdiction. Alternatively may exceptional circumstances or emergencies even suspend legal regulation and security trumps human or fundamental rights. To avoid that exploitation of supposed legal cavities or the overruling of legal rights by emergencies, human security is a helpful concept to assess and plan the implementation of security measures (Paris 2001). Criticizing the state-centered conception of security, the UN Human Development Report appealed in 1994 to explore "new frontiers of human security in the daily lives of the people" (United Nations Development Programme 1994:3).

The Charter of Fundamental Rights of the European Union: Six Categories of Rights

The following paragraphs address the rights security measures could infringe upon. Special attention will be given to those articles which potentially have a high vulnerability. The charter subdivides the ensemble of rights into six general categories: dignity, freedoms, equality, solidarity, citizen's rights and justice (Official Journal of the European Communities, Document 2000/C 364/01).

In chapter I, the right to human dignity (Article 1), the right to life (Article 2), the prohibition of torture and inhuman degrading treatment or punishment (Article 4), as well as the right to the physical and mental integrity of a person (Article 3) are outstanding rights which have been infringed upon in the name of counterterrorism and migration control. For evaluating those kinds of security measures, which are assessed by the DESSI project, the prohibition of "inhuman degrading treatment" and the right to human dignity and physical and mental integrity could be taken as a 'minimum guideline' to comply with the general rights to human dignity.

Chapter II on freedoms traditionally takes a central position in the assessment of security measures in Europe. A whole body of literature is directed at surveillance practices and the respect for private and family life (Article 7), as well as the protection of personal data (Article 8). Whereas privacy has become suspect and has lately been recast as a "codebook for

danger"[1] (Burgess 2008b) in the context of security, the lawful processing of personal data has gained ascendancy, de-coupling personal data from the individual and its privacy (Sandvik et al., under review).

Whether the right to liberty and security (Article 6) can be consulted to defend more intrusive security practices depends on the conception of security it relates to. When using state-centered security as point of origin, article six can create tensions with other articles. In the context of counterterrorism, for example, the focus of 'securing the citizen' has indirectly been re-directed at the citizen, exploiting rights to privacy or data protection to find supposed perpetrators. Freedom of thought, conscience and religion (Article 10) and the freedom of expression and information (Article 11) are central articles when assessing classification of information or cases of censorship, which lately gained importance through technological innovation; freedom of assembly (Article 12) is of potential relevance for crowd control technologies. In the context of counterterrorism and migration control the right to property (Article 17) and asylum (Article 18), as well as the right to protection in the event of removal, expulsion and extradition (Article 19) are again very central guidelines when exercising security measures.

Equality is the connecting theme of chapter III, which classically gains ascendancy in the debates on policing (stop and search, surveillance) and profiling, standard security practices in the field of counterterrorism. Here, the right to non-discrimination (Article 21) and the right to cultural, religious and linguistic diversity (Article 22) are central articles which have been infringed upon. Article 34 on social security and assistance could play a role as a positive incentive when devising security measures and defining security very broadly. The remaining chapter IV on solidarity mainly addresses worker's rights and conditions as well as the duties of the state, such as health care and environmental, and is thus not very central to the assessment of security measures, unless they are directed at specific fields such as health security or environmental security.

Chapter V encompasses the citizen's rights. Article 41, the right to good administration, can be consulted to assess security measures as most of them are in fact administrative measures (i.e. administered by the police). The sub-section saying that the administration is obliged to "give reasons for its decisions" can influence the general discourse and communication of new security measures. When considered broadly, the sub-section saying that "every person has the right to have the Community make good any damage caused by its institutions or by its servants in the performance of their duties", can be consulted to assess police behavior when implementing a security measure. Similarly, does every citizen have the right to petition (e.g. the European parliament; Article 44)[2]. Article 45, the freedom of movement and of residence, is again a very central aspect for the assessment of body scanners, video surveillance etc., but also non-permanent security measures for demonstrations, just to name a few.

Finally, chapter VI addresses rights and duties concerning justice. The right to an effective remedy and to a fair trial (Article 47), the presumption of innocence and the right to defense (Article 48), the principles of legality and proportionality of criminal offenses[3] and penalties

[1] Those who don't reveal personal data are considered a potential threat.
[2] In the context of counterterrorism habeas corpus petitions are those legal actions, through which a prisoner can be released from unlawful detention.
[3] i.e. penalties have to follow the law and need to be proportional to the crime committed.

(article 49) as well as the right not to be tried or punished twice in criminal proceedings for the same criminal offense (Article 50) are highly influential and repeatedly debated in the context of counterterrorism, not only for cases of pre-trial detention, but also for more regular practices such as 'stop and search' or dragnet investigations based on profiles.

Concerning the relationship of security measures, fundamental rights and citizens, a general problem is that the average citizen is not necessarily aware of his or her rights and the scope they entail. Debates on heightened security levels and an increasing implementation of security measures are not necessarily critically assessed within the populace itself. The DESSI project should advise decision makers how fundamental rights can be safeguarded and make a critical assessment of security measures for the European citizens.

A central question is whether this DESSI dimension needs to distinguish between rights as a matter of life or death and 'soft' rights such as privacy. Scholarly and political discussions about the latter are a result of and criticized as a Euro-centristic agenda, putting European perspectives of security to the fore while trivializing human security crises in the global south. Yet, as the DESSI project concentrates on security measures within the European realm it will have to include 'soft' rights as a crucial principles for European citizens, knowing that fundamental rights are much broader and more substantial than that. In support of Oakes' proportionality test, the DESSI project should assist decision-makers to examine thoroughly whether security measures are suitable, necessary and proportional to their aims.

Fundamental Rights – a question of Ethics?

Fundamental rights, ethical norms and values can be understood as a continuum, where, on the one end, rights are manifest, having the character of relatively universal legal rules, and on the other values are highly dynamic and subject to negotiation varying with different societal groups down to the individual level. Ethics take the position in the middle.

Fundamental rights could be considered a codification of ethics, morale or shared values. Yet, Ethics and fundamental rights are not the same. Unlike relatively consistent and manifest rights, ethical norms are more intricate and contextual. They are co-determined (Burgess 2008a: 2), shared, but not always explicitly mentioned or manifest and might vary according to specific groups (nations, societies etc.). Ethical considerations might change as security measures gain ascendancy in specific discourses or contexts. This means that our understanding of ethics is also passing through a process of transformation, potentially bringing new ethical considerations to the surface or carving out novel shared values. Due to their 'situated' nature, it is almost impossible to limit the scope of ethical norms or 'standardize' them for this DESSI dimension. A general attempt of grouping such ethical considerations and values can be found below.

Ethics can be implicit or 'tacit' referring to the level of behavioral guidelines, attitudes or even 'opinions', but are often made explicit in codes of conduct or codes of ethics, which refer to different levels of groups, such as the professional, corporate, or employee level. Ethics are also formulated, for example by defense forces as 'military ethics', but also in philosophies, oaths, commandments or creeds.

Ethical norms and values do not only vary by societal group or 'author' and in terms of manifestation or universality. A main difference between rights and ethical norms is furthermore that rights give citizens or humans the *right to* something. A right can be violated, which generally has legal consequences, whereas *ethics* are mostly formulated as *norms to follow*, an infringement upon which is a lot harder to assess. Hence, they are often formulated as guidelines. A DESSI assessment would thus analyze or describe *to what extent* a security measure follows ethical norms or incorporates certain values[4].

By scanning different codes, creeds or commandments, one can find that they reflect to a large extent 'themes' from fundamental rights, which brings us back to the question whether rights are a materialized form of ethics or whether ethics follow rights. Even if such ethical norms are legally less binding, they are of significant societal value or importance.

The following general themes, which are extracted from ethical codes, are often formulated as a positive states or characteristics, ethical behavior or reasoning seeks to strive for, fulfill[5] or respect:

- Accountability, Lawfulness and Justifiability
- Capacity and Strength (coping with Vulnerability)
- Commitment, Dedication and Care
- Cooperation (countering exploitation)
- Identity, Diversity & Value pluralism
- Impartiality and Equality (race, religion, culture, opinion, politics, gender, age)
- Innovativeness
- Life and Dignity
- Privacy
- Professionalism (Clear Thinking, Clear Statement, Accuracy)
- Profitability, Efficiency and Effectiveness (Constructiveness)
- Proportionality and Fairness
- Responsiveness
- Social Cohesion
- Transparency
- Trust and Confidence
- Truthfulness

Such ethical norms or themes don't only help to assess the ramifications of security measures on an abstract level, such norms are, according to a study by Ioannides, also consulted by security professionals being confronted with ethical considerations while doing their work. As these values influence their decision-making security professionals act as moral agents (Ioannides and Tondini, 2010), a finding DESSI should take into account when assessing security measures together with professionals.

[4] This puts DESSI interestingly into a position between the two classical schools of deontological ethics (rules to follow) and consequentialist ethics (a 'cost-benefit analysis' assessing which solution is 'good' for a greater number of people).

[5] This list is not exhaustive. For this list, the following kinds of documents were screened: Military Ethics, Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief, Code of the U.S. Fighting Force, Declaration of Geneva, Hippocratic Oath, Journalist's Creed, Rule of St. Benedict, Uniform Code of Military Justice, Patimokkha etc.

The DESSI project follows the dual approach of assessing infringements upon fundamental rights on the one hand and to which extent a measure follows more general categories of ethical norms on the other.

References

Burgess, J. P. (2008a): Human Values and Security Technologies, *PRIO Policy Brief* 7/2008.

Burgess, J.P. (2008b): Security after Privacy: The Transformation of Personal Data in the Age of Terror. *Policy Brief 5/2008.* Peace Research Institute Oslo, PRIO

Ioannides, Isabelle and Matteo Tondini (2010): Ethical Security in Europe? Empirical Findings on Value Shifts and Dilemmas across European Internal-External Security Policies. Policy Recommendation Report. INEX Work Package 3. Available at: http://www.inexproject.eu/index.php?option=com_docman&task=cat_view&gid=54&&Itemid=72 (16.08.2010)

Official Journal of the European Communities (2010): Charter of Fundamental Rights of the European Union. Document 2000/C 364/01. Adopted: 18.12.2000.

Owen, Taylor (2010): Human Security: A Contested Contempt. In *The Routledge Handbook of New Security Studies*, edited by J. Peter Burgess. New York: Routledge.

Paris, Roland (2001). Human Security: Paradigm Shift or Hot Air? International Security 26 (2): 87-102

Sandvik, Kristin B., Kaufmann, Mareile and Kjesti Lohne (under review): Terror Threat as Legal Adaption. A Socio-Legal Examination of Norwegian Regulatory Practices on Privacy and Data Protection.

United Nations Development Programme (1994): Human Development Report 1994. New York/Oxford: Oxford University Press.

Chapter 4 Legal Framework

The problems to be considered under the heading of “legal framework” are manifold. Most of the other dimensions in the DESSI dimension list can be assessed from a legal point of view or display some aspect relevant for the “legal framework”. Complexity is further increased by the fact that any security investment (SI) can involve either a change in existing organisational procedures, the implementation of a new technology (hardware or software) or any combination of different elements (organisational process, data-processing, hardwired technology). It is not possible to follow the ramifications of all legal problems arising with any given SI. In many cases it also could be difficult to determine which (national) legal order is applicable, when effects beyond national borders have to be taken into account. So on the one hand legal aspects appear to be of crucial importance. On the other hand there is a growing body of literature questioning the feasibility of classical legal regulation in the domain of new technologies and security technology is one form of this new type. The interaction and mutual effects between law and technology are complex and the question whether law can regulate technology-at-use is highly controversial.

At this stage the legal framework will concentrate on a series of “sensitizing” questions requiring close scrutiny for any given SI. Legal aspects have to be considered at the EU-level, the national level, at the level of non-state regulations and finally the interference of different legal or regulatory regimes has to be considered as well. To design this dimension of legal framework, two different approaches can be taken: one approach emulates a corporate lawyer’s perspective by focusing on legal obstacles to be considered when designing and implementing a given SI. The main goal of the corporate lawyer is to circumvent litigation against the corporation implementing the SI. The other perspective would focus on legal issues in a more comprehensive way, by scrutinizing a given SI in the context of a specific reading of the law, emphasizing the “rights” aspect of law rather than the litigation aspect.

The legal framework is structured according to the following challenges:

(1) **Data protection / privacy:** This is the most obvious dimension in the context of contemporary SI. Since most of security technology involves the gathering, storing and processing of person related data in one way or the other legal questions of data protection and privacy arise.

(2) **Accountability:** Law is the central institutional means in modern societies to handle the problem of accountability. Using law’s tool kit actors can determine who is responsible for what. In the field of SI system malfunction or misuse are common problems and from a legal point of view one has to determine with whom the legal responsibility resides.

(3)**Range of use:** SI involving technological systems often can be put to different uses (the problem of function creep). Within a legal context the question arises whether and how the range of use is determined and how any extension not covered by existing regulations can be prevented. This problem again feeds back into the abovementioned dimensions “accountability” and “data protection / privacy”.

(4) **Social sorting:** Since SI often involves a categorization of individuals and their selective processing within a given environment, granting or refusing access or service the issue of social sorting has to be addressed within a legal framework as well. Does the SI legitimately

and legally produce social sorting, are the individuals involved informed about their status, are the data used for the sorting procedure stored and recurrently used, probably also in other contexts?

(5) **Hazards to operatives:** Technological systems often use radiation or emit other potentially hazardous substances. Hence the potential hazards to operatives who are exposed to radiation etc. have to be considered within a legal framework, e.g. in determining the limits of exposure.

(6) **Hazards to clients:** The same holds for clients and / or the general public who is exposed to security technology. Hazards and limits of exposure have to be legally defined. In (5) and (6) there is an interface to the problem of “accountability”

(7)**Environmental effects:** Does the SI have any effects on the environment and are environmental regulations involved in the specific solution for the security problem at hand?

(8) **New legal provisions required**: If e.g. the police powers to stop and search are increased, or a new technology (e.g. UAV) is introduced, new regulations may have to be adopted.

	Data protection privacy	Accountability	Range of use	Social sorting	Hazards to operatives	Hazards to clients	Environmental effects
EU regulations	Do European guidelines have to be considered	Who is the provider/ producer of the system? Does the SI have effects beyond national borders? Where is the court of jurisdiction?	Does the SI produce only local and /or (trans)national effects?	Does social sorting take place and is there a legal basis for it?	Do EU-regulations for work-place safety apply?	Does EU regulation define standards for health and safety?	
National legal order	Will the SI involve the collection and storage of data? What are the measures against misuse?	What are the regulations for damage compensation in case of malfunction?	Can the range of application of the SI locally/nationally be limited in a reliable way?	Do national legal codes allow for social sorting of individuals? (e.g. patriot act)	Do national standards for work-place safety apply?		
Non-state regulations	Are there any standards for certification (ISO, etc) to be considered?	What are the professional requirements (training) to operate the system? Is certified/qualified personnel required to operate the System?	Can private actors within their regulatory framework extend the range of use by using redefinitions of central terms?	Can non-state regulations be applied to differentiate between different categories? (e.g. credit information)	Can employment contracts be used to exclude responsibility for risks and hazards?		
Interference	Do secondary effects with other legal regimes emerge?	Problems of piercing the corporate veil for secondary damages	Constraining range of action can be a problem under conflicting regulatory regimes	Problems may arise between conflicting standards at EU- and national levels	Conflicts among all levels of regulation are commonplace here		

Table 2

Chapter 5 Social Implications

Does the security investment affect social cohesion or social life in any positive or negative manner?

The purpose of security investments is to raise security or to minimise risk. Both may be achieved by influencing the behaviour of groups or individuals. In order to be able to influence the behaviour it is often necessary to observe actual or to anticipate future behaviour of people. In order to do so, it is supposed to be necessary to gain insight into people's thoughts and beliefs. Such security measures, however, often induce unintended repercussions on people's behaviour and thinking. The DESSI procedure will look into intended impacts and unintended side effects of the use of security investments in the social dimension.

The social dimension is a very complex field with lots of different parameters to check. In order to analyse impacts in this complex field, "social implications" need to be operationalized. As a starting point serve the European Commission's Impact Assessment guidelines[7]. They list a number of types of potential social impacts, which need to be considered in our description of social implications:

- Employment and labour markets
- Standards and rights related to job quality
- Social inclusion and protection of particular groups
- Gender equality, equality treatment and opportunities, non-discrimination
- Individuals, private and family life, personnel data
- Governance, participation, good administration, access to justice, media and ethics
- Public health and safety
- Crime, Terrorism and security
- Access to and effects on social protection, health and educational systems
- Culture
- Social impacts in third countries

These categories cover a broad range of potential social impacts. However, they need to be fine-tuned and shaped according to the issue at stake. As can easily be seen from first glance security investments can have impacts on almost all dimensions of these social impacts. Some of them may be refined by some subcategories. These subcategories can be found by empirical approaches analysing recent developments in society. It is phenomena like standardisation or routinisation of procedures or overall objectives like rationalisation, outsourcing and delegation of functions (e.g. the outsourcing of services to consumers, known under the term prosumption) that may well be used to describe in more detail the developments subsumed under the social

[7] EC, 2009, Impact Assessment Guidelines, 15 January 2009, SEC(2009) 92, p 36

impacts “Employment and labour markets” and “Standards and rights related to job quality”. “Social inclusion and protection of particular groups” has direct links to social cohesion and solidarity. Another important value in modern liberal societies is autonomy and self-determination, which can be subsumed under the heading “Individuals, private and family life, personnel data”. Two phenomena that are closely interlinked with social inclusion and social cohesion are trust and confidence. These could as well be used to refine the analysis of impacts in the domains of “Culture” and “Governance, participation, good administration, access to justice, media and ethics". Further work will be needed to elaborate concrete criteria for the categories of impacts above.

Besides these elements of social impact we suggest to analyse “social implications” as side effects of security investments and related measures on various societal levels: first on the level of daily actions and interactions of individuals (micro-societal level), secondly the effects on organisations, companies or cities, districts etc. (meso-societal level) and thirdly larger social units like branches or even the society as a whole (macro-societal level).

Micro-societal (individuals)

The first level deals mostly with the sphere of social life and daily actions of individuals being affected by the measure. These persons may be customers of a company, which wants to install CCTV cameras, passengers of public transport systems, who have to pass through a biometric access control in order to proceed their journey or citizen of a state introducing electronic fingerprints on passports. But citizen, customers, clients or passengers should not be considered the only elements of analysis. Rather members of the institutions, companies, organisations that (want to) implement a security investment are affected by that measure as well. This is why security workers themselves should be taken into to account too. The first and most obvious question therefore should be: Will the security investment change daily routines and if yes, who will be affected by the measure in a positive or negative way? Talking about the micro-societal aspects we have to draw attention to “objects” and “subjects” of the measure. Individuals affected are those “scanned” as well as those “scanning”. The latter – field operatives running the system – are important because even an investment in the most recent security technology will only be efficient if the persons who run the system understand, accept and can handle it.

Meso-societal (organisations/communities)

The second level of analysis deals with repercussions of security investments on the implementing organisation or affected groups of individuals. If for example a public transport service decides on a security investment involving biometric access controls the meso-societal level should consider changes within the organisation. Does this investment involve a special training of the existing field operatives or can security checks be done without the use of staff members? If so what does this mean for the whole organisation? The meso-societal level shall basically reflect upon the effects of the investment for the company/organisation and will have a strong focus on the internal acceptance of the measure. At the same time a security measure taken, may also affect a specific “group of passengers”, which may be organized in a NGO. This NGO will therefore react to this measure via press or political action. Generally speaking the meso-level analysis impacts on organisational routines, structures and potential power-shifts.

Macro-societal (the larger society/institutions/cities etc.)

The third level analysis tries to find out how institutions or branches might be affected by the investment and if so, what possible consequences for the society would evolve. A change in certain institutions or sectors may result in a change of societal values. For example, if one wants to raise awareness for unattended luggage on airports because this can be a security problem in the special context of an airport, one might end up with a media hype that influences individual feelings and in the end paranoia has become a normal social mental state when visiting an airport. This shortened example shall give an impression, that security investments, particularly if they come along with a change of the legal framework, are not only affecting the people being involved on a level of interaction (micro- and meso-societal), but can have broader impacts on society. Examples for effects on the macro-societal level may be developments like “Dangerisation” described by Lianos and Douglas (2000) or “Social Sorting” (Lyon 2003).

As can easily be seen there is also a time dependency in these levels of analysis. Whereas the impacts on micro-level affect individuals mostly directly and immediately, the effects on macro-level often occur to be indirect and take quite some time to show impact. Although we won’t be able to consider the impact of an security investment on society in the short version of a DESSI process, we however want to draw attention of end users and stakeholders who are using the “DESSI machine” towards wider societal impacts and to encourage them to proof their investment on possible side effects on society.

Table 3 below shows the relationship between the different sub-dimensions and the level of analysis. The matrix may be filled with questions like in the model below; the questions can be regarded as operationalization of the sub-dimension or criteria.

Subdimension	**micro-societal (level of interaction)**	**meso-societal (organisational level)**	**macro-societal (societal level)**
Employment and labour markets		Does the security investment have specific negative consequences for particular professions, groups of workers, or self-employed persons? Does it affect particular age groups?	Does the security investment facilitate new job creation? Does it lead directly to job losses? Does it affect the demand for labour? Does it have an impact on the functioning of the labour-market?
Standardisation/routinisation	Does the security investment impact on job quality? Will it affect workers' health, safety or dignity? Does the option directly or indirectly affect workers' existing rights and obligations? Does the security investment directly or indirectly affect workers' existing rights and obligations, in particular as regards information and consultation within their undertaking and protection against dismissal?	Does the security investment affect the access of workers or job-seekers to vocational or continuous training? Does it affect the protection of young people at work?	Does it bring about a minimum employment standards across the EU? Does the security investment facilitate or restrict restructuring, adaptation to change and the use of technological innovations in the workplace?
Rationalisation			
Delegation/prosumption			
Standards and rights related to job quality			
Standardisation/routinisation			
Rationalisation			
Delegation/prosumption		Does the security investment shift responsibilities away from the organisation towards customers?	
Social inclusion and protection of particular groups		Does it affect equal access to services and goods? Does it affect access to placement services or to services of general economic interest? Does the option affect specific groups of individuals, firms, localities, the most vulnerable, the most at risk of poverty, more	Does the security investment affect access to the labour market or transitions into/out of the labour market? Does it lead directly or indirectly to greater in/equality? Does the option make the public better informed about a particular issue?

Subdimension	micro-societal (level of interaction)	meso-societal (organisational level)	macro-societal (societal level)
		than others? Does the option significantly affect third country nationals, children, women, disabled people, churches, religious and non-confessional organisations, or ethnic, linguistic and religious minorities, asylum seekers?	
Social cohesion			
Solidarity			
Gender equality, equality treatment and opportunities, non-discrimination		Does the security investment entail any different treatment of groups or individuals directly on grounds of e.g. racial, ethnic or social origin, religion or belief, disability, age or sexual orientation? Could it lead to indirect discrimination? Does the security investment have a different impact on women and men? Does the security investment promote equality between women and men?	Does the security investment affect equal treatment and equal opportunities for all?
Individuals, private and family life, personnel data			
Autonomy/Self-determination			
Governance, participation, good administration, access to justice, media and ethics			
Trust and confidence			
Public health and safety	Does the security investment affect the health and safety of individuals/populations, including lefe expectancy, mortality and morbidity, through impacts on the socio-economic environment (working environment, income, education, occupation, nutrition)? Does the security investment affect lifestyle-related determinants of health such as diet, physical activity or use of tobacco, alcohol or drugs?	Are there specific effects on particular risk groups (determined by age, gender, disability, social group, mobility, region etc.)?	Does the security investment increase or decrease the likelihood of health risks due to substances harmful to the natural environment?
Crime, Terrorism and security			
Access to and effects on		Does the security investment have an impact	Does it affect the organization and

Subdimension	**micro-societal (level of interaction)**	**meso-societal (organisational level)**	**macro-societal (societal level)**
social protection, health and educational systems		on the services in terms of their quality and access to them? More precisely does it create unequal access to health and long-term care services for example through the creation of barriers to access (financial, geographical, organizational, administrative) which may impact strongly on more vulnerable groups?	financing of social services (of general interest)? Does the security investment affect the financing/organization/access to social, health and education systems (including vocational training)? Does the security investment affect the cross-border provision of services, referrals across borders and co-operation in border regions?
Culture			
Trust and confidence			
Social impacts in third countries			

Table 3

Some of the categories do have strong links to other DESSI dimensions like the legal framework, infringements to fundamental rights and ethical issues or the economic dimension. These links and sometimes overlapping issues will be dealt with accordingly during the DESSI procedure.

Chapter 6 Acceptability

The **risk acceptability** has to be distinguished from the act of **risk acceptance** which is an informed and in many cases legitimated) decision to take a particular risk.

The best general definition of risk acceptability is given by the **ISO/IEC guide 51**[8] which is used in subsequent standards[9]. It says:

„Tolerable (acceptable) risk is determined by the search for an optimal balance between the ideal of absolute safety and the demands to be met by a product, process or service, and factors such as benefit to the user, suitability for purpose, cost effectiveness, and conventions of the society concerned. It follows that there is a need to review continually the tolerable level, in particular when developments, both in technology and in knowledge, can lead to economically feasible improvements to attain the minimum risk compatible with the use of a product, process or service."

In a slightly different approach the UK Health and Safety Executive (HSE) defines the acceptability of risk as „the willingness to live with a risk so as to secure certain benefits and in the confidence that it is being properly controlled".[10]

The **risk acceptability** is the degree of human and material loss that is perceived by the community or relevant authorities as tolerable in actions to minimize risk (amount of the highest acceptable residual risk). A different concept denotes acceptability as the willingness of a certain group to live with a risk, in order to secure certain benefits. Acceptability of risk depends on scientific data, social, economic, and political factors, and on the perceived benefits arising from a substance, technology or process that creates the risk(s) in question. These definitions of acceptability give room to integrate various forms of acceptability in one common concept and to add qualitative aspects to technical methods.

---

[8] ISO/IEC 51:1999 Safety aspects – Guidelines for their inclusion in standards (Revision of ISO/IEC Guide 51:1990). Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=32893 (01.06.2011)

ISO/IEC Guide 73:2002 Risk management – Vocabulary – Guidelines for use in standards. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=34998 (01.06.2011)

[9] ISO/IEC Guide 73:2002 Risk management – Vocabulary – Guidelines for use in standards. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=34998 (01.06.2011)

[10] Health & Safety Executive, The tolerability of risk from nuclear power stations, HMSO, ISBN 0-11-886368-1,1992

The acceptability of risk can be significantly influenced by different means of **risk treatment**, such as

- risk avoidance: not to start or continue with an activity that gives rise to a certain risk
- substitution or alternative solutions: removing the original risk source
- changing the likelihood (usually decreasing the probability of occurance)
- changing the type and/or severity of the consequences
- distribution: sharing the risk (possible loss or gain) with other persons or groups
- risk proneness: increasing the risk to obtain additional benefits

Risk acceptability depends on certain factors which are highly connected to **risk perception** (individual and societal risk evaluation), such as:

- voluntariness: an activity has been started or an application has been chosen on a voluntary basis
- controllability: the activity or technology in question is regarded as in principle under control and possible losses can be compensated by the affected groups by themselves.
- recognisability of (individual) benefits
- fair distribution of benefits
- not endangering specific societal groups such as risk groups, i.e. persons who are vulnerable to a higher degree or do not have enough capacities to cope with certain risks
- the fact whether risk related activities and/or technologies are perceived as "natural" and socially and/or politically "appropriate"
- risk framing, i.e. the way certain risks are communicated to the public
- habituation
- life situation and life prospect
- trust: depends on the amount of perceived reliability of organisations and their representatives which are responsible for risk treatment (risk management)
- infringement of certain moral standards prevailing in a certain society
- other factors?

Additionally, risk acceptability is influenced to a certain degree by the fact (1) by whom the decision to take a certain risk is eventually taken, (2) who the recipients of a certain possible damage are, and (3) on which factual or assessment basis the decision is grounded.

- risk acceptance and risk acceptability are congruent
    - the decision is taken by the same people but without prior risk assessment. In this case decision takers and recipients of both possible benefits and losses are identical (identical uninformed decision)
    - decision takers and risk recipients are identical and the decision is taken on an informed basis (i.e. some assessment method has been employed either by the decision takers or by external experts).
- the decision is taken by a different group than the risk recipients either uninformed or after employment of a proper risk assessment method

Chapter 7 Political Significance

This DESSI dimension seeks to unpack the political content of security decision making. The dimension is intended to investigate the political consequences of implementing a proposed security investment. What are the consequences for groups of citizens and political institutions in terms of public debate, democratic deliberation and participation, everyday life, political decision-making and media coverage? The DESSI dimension also draws attention to the fact that the way the security agenda is framed as a matter for experts and authorities risk undermining the public perception of the possibility of participating and making choices, i.e. influencing policy.

The previous decades have seen a proliferation of actual and perceived security threats arising from global networks of terrorists, climate change, everyday racism and xenophobia, drug trafficking, migration, weapons of mass destruction, regional conflicts and economic recession. The constitution of these social and political densities of insecurity (Bigo and Tsoukala 2008) has repercussions at corporate, local, regional, national, EU and global levels of security decision making. The DESSI dimension is intended to capture the complexities of interlinked security issues; how we are affected as collectives; and the scope of agency we are allowed.

In the aftermath of the September 11 attacks, the necessity of trading personal freedom in order to obtain improved national security through greater government surveillance has been widely accepted. That security measures intended to protect a liberal democracy can end up eroding core values of liberal democracy is often described as the problem of striking the right balance or trade-off between security and civil liberties and democratic principles (Čas 2009, Huysmanns 2004, Posner and Vermeule 2007, Schneier 2003, Waldron 2003). Indeed, security is often described as the 'trump of trumps' outweighing civil and political rights. Especially within the field of counter terrorism, the logic of inevitability and necessity eliminates the existence of choice concerning security problem definition and choice concerning adequate security measures and relevant security actors. The 'downside of securitization' is its depoliticizing effect (Ole Wæver, personal communication).[11]

Thus, entailed in the DESSI dimension on political significance is also a view to the depoliticizing effects of prevailing security logics and a commitment to query to what extent it is acceptable to question a security agenda from a non-expert view.

[11] According to Buzan et al. (1998 p. 24) securitization is when "the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure." Securitization studies therefore aim to understand: "…who securitizes on what issues (threats), for whom (referent object), why, with what results, and not least, under what conditions" (Wæver 1995).

DESSI seeks to expand the interstice between the traditional dichotomy of threat and response by targeting the interrelated security concerns characteristic of contemporary societies and by reinstating that security decisions involve choices - choices of *if* something needs to be done, what is to be done, how much and how it is to be done.

Previously, most theorists within security studies have warned against a security framing for various societal affairs. Refraining from attributing positive or negative connotations to securitization, the securitization process can be seen as a social and political construction related to speech acts. Also, according to Ole Wæver (personal communication) security inter-issue competition has created a conceptual inflation of the security concept. Paradoxically, it is exactly this 'security inflation' that seriously challenges the logic of necessity and therein lies a room for maneuver or a potentiality for insisting on an inclusive public discussion on security issues, on the 'right' way of responding as a society and for developing a language for tackling political responses to the handling of complex and networked threats. Political decision-makers are confronted with a host of incompatible security problems and the interrelatedness of security agendas transgresses traditional fields of expertise. Currently, policy makers and the media try to translate between security fields but we need to develop a language for carrying out these vital translations between security fields and for discussing and devising socially robust decisions on security investments. This is a translation task that requires interlinks between different forms of expertise – scientific, technical and citizen.

References

Bigo, D. and Tsoukala, A. (2008). Terror*, insecurity and liberty: illiberal practices of liberal regimes after 9/11*. London; New York, Routledge.

Buzan, B., Wæver, O. & de Wilde, J. (1998). *Security: A New Framework for Analysis*, Boulder CO, Lynne Rienner.

Čas, Johann (2009). PRISE Conference Proceedings:"Towards privacy enhancing security technologies – the next steps", Vienna, April 28th and 29th 2008, available at http://www.prise.oeaw.ac.at/docs/PRISE_D7.3_Concluding_Conference_Proceedings.pdf

Huysmanns, J. (2004). Minding Exceptions: The politics of Insecurity and Liberal Democracy, Contemporary Political Theory 3.

Posner, E. A. and Vermeule, A. (2007). *Terror in the Balance: Security, Liberty and the Courts*. New York, Oxford University Press.

Schneier, B. (2003). Beyond Fear: Thinking sensibly about Security in an Uncertain World. New York, Copernicus Books.

Waldron, J. (2003). Security and Liberty: The Image of Balance, *Journal of Political Philosophy* 11.

Wæver, O. (personal communication), telephone interview with Ole Wæver, September 13, 2011

Wæver, O. (1995). Securitization and Desecuritization, in: Ronnie D. Lipschutz, (ed.), *On*

Security, Columbia University Press 1995, pp. 46-86.

Chapter 8 Economy

1. Overview: European Security Market

To obtain data about the exact size of the market or employment is not easy (Martí Sempere, 2011a) because the data provided by governments operate within broad categories including additional goods and services and private firms operate within many markets and countries. These information about security revenues and expenditures is not always disclosed and many provided data are based on interviews whose reliability is unknown (Künzel et al., 2009). Hence, the numbers obtained can rather serve as rough estimations of economic activity than exact measures. Regarding labour opportunities in the security market, Eurostat assesses the number of employees with about 1.1 million (Martí Sempere, 2011a), whereby the employees can be mainly found in private security services.

On the demand side in the security market, governmental institutions are the main of security services and products serving as the principal security provider to society. Governments usually demand high-end products and services to demonstrate their effectiveness in affording security. The acquisition in the public sector is not centralized because according to the function of the demanding institution different goods and services are purchased (Martí Sempere, 2011b). Governmental expenditures grew with an annual rate of nearly 7% in the EU-27 in the period 2001-2007 (Martí Sempere, 2011a); in Austria, governmental expenditure rose from 779.1 million € in 2001 to 945.1 Mio € in 2007; Germany: 9,520.0 (2001)-12,100.0 mio € (2007); EU-27: 44,702.7 mio € (2001) - 66,518.7 mio € (2007), which corresponds to 0.5% of GDP of EU-27 in 2007 (Martí Sempere, 2011a).

Private companies lay the focus on the protection of their business including employees, clients and their company. Especially private organisations with a large numbers of costumers such as shopping malls are considered as large investors in security measures. Individuals invest in security equipment mainly to protect their homes.

Estimates of physical security market about the distribution between different kinds of application show the following: video surveillance 23%, access control 14%, intrusion detection 22.8% and fire detection 43.5% (Martí Sempere, 2011a).

In standard economic theory, the decision to implement a certain security measure depends on if the benefits outweigh the costs. The fundamental problem that occurs is the fact that decision-makers often regard the investments in security technologies and services mainly as cost factors and oversee the impacts of long term effects. The underlying reason is that direct investment costs can be easily identified whereas the economic return can be calculated only in case of avoided damage, which is in general difficult to prove. In the case of human damage the damage can hardly be monetarily quantified at all. It is almost impossible to assess what are the optimal levels of the protective measures nor is it usually possible to prioritize them. Benefits and costs depend on many variables, whose real value and influence is unknown and traditional cost-benefit analysis is rendered nearly impossible (Jackson et al., 2007). Therefore, especially the DESSI tool helps to develop a more holistic sight than the monetary one.

2. Microeconomic effects and implications

The operational and dynamic aspects of an economic analysis require a deeper assessment than usual accounting based approaches (e.g., return on investment type calculations, cost-benefit analysis). The assessment should go beyond conventional management decisions on investments leading to security gains. A rather comprehensive economic view ensures an economic assessment embedded in societal frameworks and should focus on an assessment of the consequences of the security investment on economic actors and institutions.

Any investment in security technology or service or emergency relief is a decision to directly take an expenditure on a specific investment. The question how much does the investment cost can be seen as an important starting point prior to any other considerations. As security investments can be quite different in their size, magnitude, and its claimed human resources it should also be questioned why it is important to invest in a certain quantity. The literature about investments of security industry recognises a proclivity towards over-investing in protective measures at the expense of pro-active measures.

After defining the amount of money for a certain investment it has to be considered who takes over cost and who profits from the investment. It should be differentiated between private or public investment and who the beneficiaries in each case are. Intention of public institutions is acting as security providers for their citizens whereby it is also one of the fundamentals of society that the state receives revenues through taxes to provide services for citizens. The intention of a private firm is different: overall aim is gaining profits. If this goal can be achieved better by enhanced security the envisaged security investment will take place. The direct beneficiaries of this security gain therefore are the employees and the clients. One step further, it should be also taken into account who is the firm that receives the investment assignment and questioned if this firm complies certain criteria that have to be fulfilled (as usual). In this context also, transnational impacts are of importance. Especially in security equipment market, main products are at least partly produced outside Europe such as video surveillance equipment is usually manufactured in Taiwan, Korea, or China. The investors should consider production conditions for humans and also the environmental impact in the production process and in the long distances of transport. Investments outside EU provoke cross-border investment flows and result in relocation of economic activities

Indirect costs are defined as costs that cannot be assigned exactly to a certain investment and cannot be identified specifically to a certain measure. Indirect costs are not caused by a specific activity. An example would be the costs for the salary of employees who are in charge of decision making in security investments but also have other duties, meaning that they receive the salary independently if the investment take place or not. Moreover side costs should also be considered, e.g. employees need a special training for improving their skills in relation to the security investment. The desired investment should also be evaluated according to their non-monetary costs meaning any costs or any activity that are affected by the activity like gains or losses of reputation or trust or time consuming security procedures which cannot be expressed in monetary terms although the consequences may have economic impacts. Security investments may also affect economic behavior and produce behavioral changes.

To achieve a certain security gain, there is always a range of alternatives that can be accomplished. Opportunity costs are defined as costs for the value that would be created by the given up (second best) alternative that cannot be realized because of

the making the investment under consideration (sacrificed benefit). The consideration of opportunity costs makes it possible to conduct a comparison between different alternatives and their monetary value. For example, if someone decides to invest in video cameras she/he has to give up the possibility in investing in human security staff. That means one cannot profit from the advantages of this security staff such as flexibility in spatial surveillance. This flexibility could also be measured in monetary terms which would make it possible to define exact opportunity costs. Or if people have to wait in line at security checkpoints at the airport, they could have spent their time working. These income losses are called opportunity costs.

Especially in security investments decision, it is indispensable to consider externalities. Externalities are any unintended positive or negative effects caused by the security investment that affect non-involved third parties. Any security investment that has a high environmental impact due to extensive resource use causes negative externalities on the environment, although it is not the intention to pollute the environment. Or waiting a long time in the airport due to longsome security checks causes negative externalities to the cafeterias because people don't have the time any more to take a coffee. A positive external effect would be, for example, because of increased security measures in a public building neighbors also feel more secure.

Security investments may cause short or long term economic dynamics in the respective organisation: e.g., lock-in effects prevent organisations switching from one system to another because it would cause high costs (important mainly in IT-security). Another important field is the regard of inter-dependencies to other security investments that may be accompanied with unexpected costs and to existing organizational processes and practices.

A certain type of cost that is sometimes overlooked are costs of potential misuse; security investments run the risk that someone misuses security devices, e.g. someone uses data that are stored for security reasons and sells it.

3. Macroeconomic effects and implications

Macroeconomic effects of security investments address the economic impacts on larger economic scales. It considers the interconnectedness and interdependency of different areas of economic activities and its actors and institutions. Although microeconomic considerations affect more likely security investment decisions, macroeconomic effects should be considered in case of large, mainly governmental security expenses. In all other cases, the impact of a single investment decision has a minor impact on the macro-level. The following points are examples what the relevant macro-economic variables in the security market are.

Demand side (private): The intention of private companies to invest in security measures is to avoid economic losses and to ensure business continuity. In principle, protection takes place on three different levels: the enterprise itself, the employees and the costumers. Special cases are privately operated infrastructures with a high societal dependency such as electricity grids, oil and gas pipelines and other energy grids, transportation area (especially air area), food chains, and health sector.

Demand side (public) and governmental crowd out: Governmental and public institutions are seen as principle security provider to society through legislative and executive power on the one hand and on the other through large demand for security

goods and services. How is the investment financed? Which budget has to be increased and therefore which budget has to be decreased? Especially in the case of low- and middle-income countries security and defense spending may not only increase budget deficits but also create economically and socially significant opportunity costs, by these investments jeopardizing economic development. Is the investment large enough that it could possibly have these consequences? On a more general level, a fundamental question may be how much governments spent on security investments and how are the expenses justified?

Effects on other sectors or regions: Not only in the respective organisation, also effects on closely related industries and markets (defense industries, building monitoring and management industry, industrial automation and control industry, scientific instrumentation industry, ICT industry) should be in the focus of interest to assess its possible effects. Changes in demand for tourism industries, security regulations at transport hubs that increase transaction costs of trade are examples of additional potential impacts on markets. The investment may also have a specific impact on certain regions or nations which are disproportionately affected.

Share of investment in security industry: Depending on the monetary amount of the investment, on a regional or even national level it may indicate a remarkable investment decision which is reflected in respective regional or national data on economic investment.

Employment market and employment conditions: As research on the employment market in the security branch in Europe has shown that the majority of employees work in security services. Deeper analysis should reflect which type of employees will benefit from the investment: Does the security investment require high or low skilled worker (or more precise the profession needed), does the investment demand mainly female or male workers, does the investment employ people in production sector or service sector (abroad or home country), how much workers will the measure employ, how are the working conditions in regard of time (full time jobs or part time; working by day or by night; time contracts; payment conditions) and other related questions.

References

Brück, T. and Engerer, H: (2009): Ökonomie der Sicherheit. Vierteljahreshefte zur Wirtschaftsforschung 78 (4), 5-10

Brück, T., Karaisl, M., and Schneider, F. (2008): A Survey of the Economics of Security. Economics of Security Working Paper 1, Berlin: Economics of Security

Jackson, B.A., Dixon, L., and Greenfield V. A. (2007): Economically Targeted Terrorism. A Review of the Literature and Framework for Considering Defensive Approaches. Rand – Center for Terrorism Risk Management Policy, Santa Monica, USA

Künzel, M., Loroff, C., Seidel, U., Hoppe, U., Botthof, A. and Stoppelkamp, B. (2009): Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen. Final report. VDI, Berlin

Martí Sempere, C. (2011a): A survey of the European security market. Economics of Security Working Paper 43, Berlin: Economics of Security

Martí Sempere, C. (2011b): The European Security Industry. A Research Agenda. Defence and Peace Economics 22 (2), 245-264