DESSI

Decision Support on Security Investment

2.6 DESSI System of Criteria

Grant Agreement no. 261178

Supporting activity acronym: DESSI

Activity full name:

Decision Support on Security Investment

Editors: Johann Čas (OeAW-ITA), Mareile Kaufmann (PRIO)

Authors: Marie Paldam Folker (DBT); Mareile Kaufmann (PRIO); Alexander Neumann, Reinhard Kreissl (SWFB); Johann Čas, André Gazsó, Walter Peissl, Petra Wächter (OeAW-ITA)

Due date of deliverable: 1st of March 2012

Actual submission date:

Start date of activity: January 2011

Duration: 30 months

Revision: Final

Change Records

Version	Date	Change	Author
1	12.4.12		Johann Čas
1.1	12.4.12	Comments and track changes	Mareile Kaufmann
1.2	22.4.12	All draft contributions integrated	Johann Čas
	25.4.12	Comments and Track changes on whole draft	Mareile Kaufmann
1.3	7.5.12	Revised dimensions integrated	Johann Čas
	8.5.12	More revisions integrated, check on all comments and text, formatting	Mareile Kaufmann
1.4	20.5.12	Final revisions integrated	Johann Čas

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: Walter Peissl
wpeissl@oeaw.ac.at
www.oeaw.ac.at/ita

Table of Contents page

Preface

Decision support on security investment

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

In the decision-making processes on security investments the primary aim of security gain often overshadows 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 different societal domains such as transport, public space, health care etc. Security investments are seemingly immediate responses to specific threats and hazards. Related decision-making processes tend to be technology driven and often show signs of incomplete considerations on societal implications.

A method for decision support

In order to further research on decision-making on security investment, the European Commission has financed the DESSI project which is developed by a consortium of partners from Denmark, Norway, Austria and Germany. In close cooperation with stakeholders and scientific advisory, the consortium is designing a decision support system, which will be launched in 2013.

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 beyond security gain/loss, including 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 and stakeholders. Using DESSI, groups will be invited to assess the investment against a variety of criteria and future scenarios, providing for 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 A brief theoretical introduction

Reinhard Kreissl (SWFB) and Johann Čas, (OeAW-ITA)

DESSI is a tool designed to provide support for decisions on security investments. In doing this, it confronts its users with a number of questions that often lack any definite or objective answer, while, at the same time, forcing them to closely and objectively investigate the problems they want to solve.

As opposed to other tools for decision support, DESSI is not designed as a search procedure leading to a definite answer - a pre-existing right solution, hidden somewhere, waiting to be discovered - and is not primarily based on expert knowledge.

The objective of DESSI is to let an array of the most rational answers emerge out of a deliberative and participative process in which the involved actors share a robust and complex understanding of the locally relevant aspects of what is called a “security problem” in the DESSI process.

The key point here is that DESSI should be seen as a tool, applied to increase the variety of perspectives and aspects to be considered in a deliberative process, starting with an input – the “problem” or “investment” to counter a problem– which then has to be integrated into a set of alternative measures, among which the participants may choose what for them is the most satisficing solution. The concept of a satisficing solution goes to back to cybernetics and systems theory and denotes a situation where no single optimal solution for a given problem can be achieved. (Simon 1955).

One of the core elements of DESSI is the participatory approach. Providing the users with a set of dimensions to investigate their initial problem (be it a security problem or an envisaged investment to solve such a problem), the DESSI process is designed to open up entrenched definitions and pre-understandings of a given state of the world. Each of these dimensions is itemized using a number of operational criteria to closely scrutinize the security investment or security problem within a specific frame of reference (legal, political, social, etc.). In doing so, the topic under investigation unfolds is multidimensionality.

As opposed to the usual expert systems, where an asymmetrical situation prevails among (human or artificial) experts and their clients, DESSI takes a different approach. It starts from the assumption that clients, users and participants are knowledgeable in the domain under consideration. The external experts’ role is furthermore rather that of assistants helping to make implicit knowledge explicit and to structure this explicit knowledge in a usable format.

Developing DESSI along these lines is a strategic decision with far-reaching epistemological and also political implications. First of all, it takes the laypersons’ perspective on the issues under consideration serious. It is not only the experts but also non-expert stakeholders, field operatives, clients, customers and others who do

have their own elaborate theories about the world. Secondly DESSI acknowledges the existence of different, conflicting or overlapping views that should not be reduced to the status of pieces in a jigsaw puzzle, but as locally relevant comprehensive interpretations of a complex problem. Experts tend to work towards overarching syntheses, treating accounts from other involved actors as partial and selective representations, which are in need of the experts' capacities and competences for a full understanding. Laypersons may provide the input, but the experts compile these inputs according to their own logic. DESSI rejects this approach.

Thirdly, DESSI focuses on the social-cognitive procedures of constructing the locally relevant interpretations rather than on their substantial content. Since the substantial issues of security problems cannot be determined in advance we consider it important to focus on the process of emerging ideas of security problems.

This shift from a substantial to a procedural approach, focussing primarily on the process of negotiation and deliberation, solves a problem that affects all empirical inquiries, but becomes most obvious when issues of security are addressed. Security is notoriously difficult to define in an unambiguous way (Zedner 2009). First of all, the concept of security addresses future states of a system that cannot be known beforehand. Secondly, security can be approached from very different angles - as security perceived by an individual or security calculated on the basis of an external assessment of risks, damages and probabilities (Burgess, 2010). Depending on what is taken for granted in a given situation or context, security can have a whole array of different meanings. Thus, different strategies to approach security "problems" at the operative level seem appropriate.

As opposed to concrete objects and things (like stones, trees or animals), security is not something that is "out there" for inspection and inquiry to be measured and weighed. Yet, the notion of security is regularly invoked in debates over the state of affairs of individuals and/or different kinds of systems. Speakers have no problem to use the word security. Here, the same point has to be considered. DESSI does not distinguish between everyday und expert definitions (or usage) of the term security, but treats different usages of the term as what they are – different in a "horizontal" way. Nonetheless, most usages of the term create a common discursive effect: they securitize their object in different ways.

DESSI takes a participatory, procedural approach, inviting participants to take a reflexive look on how they securitize the world by applying different abstract interpretations, which are rooted in empirical evidence drawn from different sources. The role of experts in this process is to take up participants' accounts, relate to them and engage with individuals in a critical learning experience by scrutinizing the conceptual and empirical basis of the views held about the (to be securitized) state of the world under investigation. Beyond the experts' viewpoint, DESSI proceeds via a reflexive hermeneutics of preconceived ideas taken for granted by the participants. Each participant's viewpoints are exposed to the same scrutiny as the participants' view of the world, which then can create mutual learning processes.

Dimensions in the context of the DESSI process have to be seen as frames of reference or frames of relevance applied in successive order. Analysing a security investment, a variety of dimensions can highlight different aspects of the investment

under investigation. These different aspects focus in a straightforward manner on a single dimension such as economic costs, legal regulations, social impact, etc. Comparing ideas and suggestions for a security investment in this way not only increases the variety of options in the final decision processes, but also compensates for differences in expertise and authority among the participants.

One could consider DESSI a “discursive algorithm”, re-arranging and integrating a variety of perspectives on a given social object. DESSI is designed to disentangle entrenched understandings of the social world under investigation: What is the problem? What are the threats? What is at stake? Who is responsible? Who is accountable? What is technical, what is social, what is cultural? What can be changed, what has to remain as it is? All these questions are at stake when a security problem is under investigation (in construction or de-construction).

Beyond this cognitive focus, DESSI addresses problems of normative evaluation as well. While de-constructing seemingly simple security problems and measures into their constituent parts, the DESSI process unveils the complexity of the security problem/investment under investigation. The subsequent evaluative part brings this complexity back to a format of alternatives, which can be ranked and among which the participants of the DESSI process can choose. The overall DESSI process can be understood as a process of consecutive de-construction and re-construction, with the dimensions and criteria as conceptual tools to perform these tasks.

The different DESSI-dimensions dismantle established interpretations of a given problem by focussing on new perspectives. By strongly focusing on the process before closing in on a decision, DESSI avoids an early consensus and the application of knockout-criteria in early stages of the assessment.

One of the features that make the DESSI process stand out among other assessment tools and methodologies for decision support, is the lack of pre-given indicators for the evaluation of alternative options. Security investments are not measured against default values or quantifiable thresholds. Nonetheless DESSI will produce numerical values to compare different solutions. This makes DESSI a very flexible tool that can be tailored to the practical problems at hand. The criteria operationalizing each dimension allow for a deliberative approach to better understand the alternative options under scrutiny. Participants are invited to apply the criteria in an interpretive way rather than working their way through a checklist with yes/no options. DESSI also provides for the consideration of non-technical (e.g. social, organisational) solutions to security problems. The broad range of dimensions and criteria can prevent the debate from its reduction to technological fixes at an early stage. The dimensions and criteria used in the DESSI process were carefully chosen to avoid the early reduction of options to technological measures only.

Combining a strong participatory approach with a deliberative strategy while including a wide array of dimensions, the DESSI procedure is designed to provide for rational decisions on security investments, reaching beyond established expert systems for risk assessment.

The DESSI methodology forces an informed societal discourse to take place on the pros and cons, cost-benefit, trade-offs and wider societal connotation of alternative

security investments. It advances the state-of-the-art of security investment decision-making in several important conceptual and methodological areas. In the past the dominating approach to investments in security has been a pragmatic approach, in which the political necessity of taking action is being balanced with trade-offs in civil rights, privacy and economic costs in a highly politicized process.

The DESSI approach overcomes these limitations by adding new elements and learning from related assessment methodologies in a comprehensive, participatory and inter-disciplinary procedure.

The first important element of improving the state-of-the-art of security investment decision-making concerns the explicit integration of the political nature of security investment in a decision support system. This will be done by integrating a specific dimension on "political significance" in the method and by making use of broad participation, including decision-makers, in the assessment procedures.

The second key item consists of adding the qualities of participatory approaches to the investment assessment. Europe has built up a profound experience of citizen and stakeholder consultation on science and technology issues during the last 20 years, mainly through technology assessment activities in the member states.[1] Participation contributes to the societal clarification of complex issues by favouring the cognitive dimension (by the diversity of knowledge that is brought into the process) and the normative dimension (by the insight into and the negotiation of standpoints that participation brings about). The pragmatic dimension can also be improved by the political/democratic relevance and knowledge about implementation of results of the participants. Participation also increases the democratic credibility of analysis by supplying a multi-perspective peer to the analysis. Furthermore, the chance of making socially robust solutions increases considerably when the societal disagreements have been heard and listened to in the formation of the outcomes.

The integration of foresight methods, specifically of scenario techniques, is a third enhancing element of the DESSI approach. Especially in uncertain environments it is decisive to increase the robustness of decisions against context shifts. This may be done by testing how decisions would perform under stress from a set of virtual futures – scenarios. Security investments by definition exist in an uncertain environment – in fact, they are installed as a reaction to uncertainty. DESSI will combine scenario techniques with systematic identification and assessment of investment alternatives.

A fourth element involves learning from risk assessment in an extended way. State-of-the-art was probably reached by the end of last century when it was generally recognised that risk assessment, besides being a statistically based expert discipline, would need to involve risk communication and risk dialogue in order to take risk perceptions into account when designing risk policies. DESSI adds this reflexive element to the standard risk assessment approach: By scrutinising the security

[1] Some of the available and well tested methods are the Consensus Conference; Planning Cell; Future Lab; Deliberative Polling; Citizen Summit; Voting Conference; Interview Meetings; Scenario Workshop; Citizen Jury, World Café; Open Space, etc.

investments themselves, they can be viewed not only as solutions to a security problem, but also potential sources of new societal conflicts, connected to the involved trade-offs. The DESSI methodology will imply that the impacts of the measures are fully assessed.

As a further innovative element, DESSI introduces contrasting levels of problem perception in the societal discourse and an evaluation of security enhancing practices. The need for problem orientation arises from the different views on the concept of threats and security. Related to anti-terror initiatives, 'threats' are generally connected to the possible loss of human lives and physical and economic values. Opposing this connotation, threats are often seen in the threats to civil rights, privacy or in missing proportionality, efficiency and specificity of security measures. From a military/police point of view, 'security' means a state of affairs, in which persons or values are not harmed. From a human rights perspective 'security' also has a connotation of protection against intrusion from the State.

The multi-dimensional assessments approach of DESSI links different professional developments to each other and furthers an interdisciplinary research process. The dimensions and criteria depicted in the following chapter reflect DESSI's interdisciplinary approach.

Simon, H.A. (1955), A Behavioral Model of Rational Choice. Quarterly Journal of Economics Vol. 69, 99-118.

Zedner L., (2000): The Pursuit of Security, in *Crime Risk and Security,* eds. Hope T. and Sparks R. Routledge, London

Chapter 2 Dimensions and Criteria

The following subchapters represent the criteria selected for being used in the DESSI assessment process. They represent the DESSI evaluation and comparison dimensions Security gain or loss, Fundamental Rights and Ethics, Legal Framework, Social Implications, Acceptability, Political Significance and Economy. For any of these dimensions large sets of various criteria could be used. The limitation to sets of about six criteria for each dimension reflects practical needs to limit the criteria to manageable numbers. The concrete selection and prioritisation is taking into account the information and feedback from stakeholders and users during the expert interviews and the DESSI workshop “Making better security decisions – How do we get there?” November 8, 2012 in Copenhagen.

Each subchapter starts with a brief introduction, followed by the criteria and supporting information to be used in the DESSI web tool; they are represented in the same tabular form as in the web tool.

2.1 Security gain or loss

Alexander Neumann, Reinhard Kreissl (SWFB)

Security can be defined as the absence of threats or as a low probability of damage (see Wolfers 1952). Some scholars distinguish between objective and subjective security. Objective security refers to a low probability of damage, while subjective security refers to the feeling of security, or the absence of fear.

The DESSI process puts forward three perspectives for the assessment of security gain or loss (SGL): (1) subjective or perceived security; (2) objective security; and (3) 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 (See Zedner 2000). 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.

(1) 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 (see Gabriel & Grewe 2003). 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 frames of reference) of individuals exposed to the security measure under investigation. This measurement also heavily depends on individual set-ups/levels of awareness, attitudes and 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.

Generally, DESSI assumes that if a person feels secure before and insecure after a security investment is implemented, 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 effect. The relation between perceived and objective security is complex and has to be considered very carefully in each case under investigation.

(2) Objective security is measured from the perspective of the detached 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: other, less easily measurable perspectives (perceived/subjective security and security as discursive frame), also have to be taken into account. While an assessment of SGL for a given security investment may yield positive results from the perspective of objective security, it may produce negative effects from the perspective of subjective 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 other perspectives.

(3) 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” (see Lyon 2007). 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 operationalized 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 criteria 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. 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 employee working with security issues 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.

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, technological robustness (safety, technological resilience), system stability, vigilance etc. Security investments can be measured and compared against each of these aspects.

Finally, from the perspective of securitization, the SGL vary with respect to who is conducting the DESSI assessment. Actors who support a securitized view of the field under investigation will see the world differently from those who hold a different view (see Waever 1995). 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).

Security gain or loss	
Description:	Security investments are undertaken to cope with threats and hazards, in order to minimize risk or to increase security. Security gain is the main purpose of the investment. It does no matter whether the threat assessment, which has led to this investment, is based on an evidence-based threat, or on a perceived threat. Security investments can be taken in order to react on a specific event which has happened in the past or in order to prevent a specific disruption. Often, however, we only see an assumed security gain: be it short-term only, be it just a displacement of the underlying problem or be it hard to assess in advance. Whether the consequences of a specific security investment can be classified as security gain or loss, depends on different individual perceptions. Paradoxically, security measures may decrease subjective security and thus increase demand for new security investments. The DESSI process will distinguish between these two concepts of objective and subjective (perceived) security. Basically objective security can be understood as a measurable increase or decrease of facts that are related to security (e.g. decrease of reported incidents to the police after the investment was taken). On the opposite, subjective or perceived security is defined as a mental state, which is dependent on other factors, such as individual risk awareness, sensitivity, knowledge etc. An example for an increase of objective security could be that the investment will lead to a decrease of reported incidents. But on the other hand, when the investment is focusing on rare events like

	terrorist attacks, even such an evidence-based concept as objective security will be hard to measure. The fact that an investment will provide a security gain on the objective level, whether this gain is measurable or not, does not necessarily mean that the subjective security is increased as well. Reasons why an individual feels secure or insecure are manifold. The DESSI process can hardly provide evidence-based data to analyse the effects that a proposed investment could possibly have on the subjective perception of security. But DESSI operationalizes this distinction between objective and subjective security in the form of questions (so called criteria) to create a better understanding of the purpose and benefits of the foreseen investments. The DESSI procedure will not prove whether an increase or decrease of objective or perceived security is caused by the actual investment. In most cases further investigations on the measurability of the expected impacts, which are caused by the investment, will have to be considered.
The discussion on the dimension	Security is an obscure 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. 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. DESSI will, however, propose three different aspects of security to be taken into account when assessing SGL. (1) subjective or perceived security (2) objective security (3) security as a discursive frame A more detailed explanation of these three concepts will be provided in the overall discussion of the dimension.
Criterion 1:	Increase of objective security

Title	
Criterion 1: Description (Mouse-over)	(How) can the chosen investment increase objective security?
Explanation:	It is obvious that the investment should increase security. Can the expected increase of objective security be measured? Will the investment help to preserve the status quo? What kind of change will the process trigger? Who will be affected by this process? Will the incidents reported to the police, for example, be reduced after the investment was taken?
Criterion 2: **Title**	Increase of subjective security
Criterion 2: Description (Mouse-over)	Will the chosen investment have positive effects on perceived security?
Explanation:	Who is going to be affected by this investment? Is it possible that for certain groups of individuals (e.g. clients) the investment will cause a decrease of their perceived security, while for other groups (e.g. employees) it will increase subjective security? If a decrease of subjective security related to the investment is expected, is it expected to be compensated by a plausible increase of objective security? One could think, for example, about security checkpoints at public buildings. For some people these checkpoints will increase feelings of insecurity, since they are reminded of a potential attack, which relates to the feeling that this building is not a safe place to be. The checkpoints could, at the same time, decrease the possibility of such attacks.
Criterion 3: **Title**	Prevention
Criterion 3:	Is the investment preventive?

Description (Mouse-over)	
Explanation:	Sometimes security investments are considered even though no security-relevant events have happened. Can a net gain of security be achieved through this investment? Remember the outcome of the security problem description. Are the problems that shall be addressed by the investment based on actual or potential events?
Criterion 4: **Title**	Public demand
Criterion 4: Description (Mouse-over)	Is there a public demand for the investment?
Explanation:	What are the circumstances that have increased the demand for this investment, besides actual/objective security problems? Is the investment only of symbolic value? Is the demand for this investment a consequence of changed societal and political priorities, which are related to previous developments (process of “securitization”)? As an example think about the development of airport security measures after 9/11.
Criterion 5: **Title**	Security addressee
Criterion 5: Description (Mouse-over)	Will the investment have different effects for different groups of individuals?
Explanation:	Are there different levels of vulnerability for certain groups of individuals to be expected? Will different groups benefit more or less from the investment under consideration?
Criterion 6:	Resilience

Title	
Criterion 6: Description (Mouse-over)	Some events cannot be prevented or anticipated. Is the investment rather focusing on enhancing resilience than prevention?
Explanation:	Resilience is understood as the capability of a system (group of individuals) to recover from a disruption and return to normality.

References

Boin A., and McConnell A. (2007): "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience", *Journal of Contingencies and Crisis Management,* Vol. 15, No. 1, March 2007.

Gabriel U., Greve W. (2003): The Psychology of Fear of Crime. Conceptual and Methodological Perspectives. In: British Journal of Criminology Vol 43 (3)

Lyon D., (2007): Surveillance Studies, An Overview, Polity Press, Cambridge

Waever O., (1995): Securitization and Desecuritization, in *On Security,* ed. Lipschutz R., Columbia Univ. Press, New York

Wolfers A., "National Security as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 4 (1952)

Zedner L., (2000): The Pursuit of Security, in *Crime Risk and Security,* eds. Hope T. and Sparks R. Routledge, London

2.2 Rights and Ethics

Mareile Kaufmann (PRIO)

The charter of fundamental rights of the European Union 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, for example in the name of counterterrorism and migration control.

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" (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., unpublished).

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-centred security as point of origin, article 6 can create tensions with other articles. In the context of counterterrorism, for example, the focus of 'securing the citizen' has been re-directed at the citizen, putting every citizen under suspicion and violating 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. 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 a lot of them are in fact administrative measures (i.e. administered by the police). Every citizen has the

right to petition (e.g. the European parliament; Article 44. Article 45, the freedom of movement and of residence, is again a very central aspect for the assessment of 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 defence (Article 48), the principles of legality and proportionality of criminal offenses and penalties 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.

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 a DESSI dimension. A general attempt of grouping such ethical considerations and values can be found below.

Ethics can be implicit referring to the level of behavioural 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 defence forces as 'military ethics', but also in philosophies, oaths, commandments or creeds.

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.

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, fulfil 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 takes into account when assessing security measures together with professionals, for example by conducting interviews with decision-makers and by having organized a criteria selection workshop.

The interviews conducted with decision-makers showed that societal and ethical aspects of decision-making are very important, not least because they can also become sensitive issues in public debate. Of all different dimensions, such as economy and security gain, the general impacts on society was finally ranked as the most important one. This dimension of fundamental rights and ethics is an essential part of social life and seeks to operationalize such impacts through selected criteria on rights and ethics.

As the feedback from the assessment workshop showed, assessing the whole charter of fundamental rights is too broad. A grouping of rights and ethics was a first step to narrow the number of criteria down to a manageable size. The main output of the workshop/blog was that this dimension needs a manageable amount of criteria, which are clearly formulated and not too broad. The right to private life, freedoms and the

right to non-discrimination were mentioned as core criteria on the assessment workshop. The relevance of the inclusion of different groups and minorities was pointed out as one important aspect of this dimension.

To narrow the number of criteria down even further, we excluded ethical values that were covered by other dimensions, such as “Lawfulness”, which is covered by the dimension “Legal Framework”. “Innovativeness and Constructiveness” are implicitly covered by several dimensions such as Economy and Political Significance. “Profitability, Efficiency and Effectiveness” are implied in the assessment of Security gain/loss and Economy. “Professionalism” again is a general value when devising the investments in the first place.

During the selection we furthermore paid specific attention to those rights and ethics, which are covered in scientific research, which again focuses on privacy and non-discrimination.

A final selection criterion was to avoid mentioning the same criterion twice, namely once expressed as right, once as ethical norm.

Aiming to capture a level between juridical expertise and a lay person-level for assessing such criteria, this dimension covers three (groups of) rights - Privacy, Freedoms, Non-Discrimination – of which the last two are interconnected with the ethical norms of diversity, equality and value-pluralism.

This dimension furthermore covers two ethical values, which are especially important during the implementation phase of security measures: transparency, and social cohesion. The latter criterion implies other ethical norms, such as trust and confidence.

Finally, this dimension includes an overall criterion connecting rights and ethics with each other: proportionality (of the measure). This criterion is in fact an assessment with three steps following specific ethical considerations: Is the measure suitable and necessary to answer a problem (referring to ethical norms of strength and responsiveness)? And is it proportional (referring to ethical issues such as function creep and exclusion)? As the last criterion of the dimension it aims at binding the other assessments of this dimension together.

Rights and Ethics	
Description:	This DESSI dimension assesses whether security measures potentially infringe upon fundamental rights (as recorded in the European Charter) and to what extent security measures follow a general set of ethical norms. Certain security issues are notoriously difficult to solve so that boundaries between legality and infringement upon rights seem blurred (e.g. when counter-terrorist measures weigh heavier than

	rights to privacy). Such blurred boundaries pave the way for states of exceptions and diverting interpretation of rights and ethics. To avoid potential infringements, the following criteria will not only bring human security into focus when assessing security solutions. They also offer a structured approach to reflect on ethically relevant issues, which are crucial for the development and implementation phase of security measures and directly interlink with acceptability of the measure. For reasons of feasibility, three (groups of) rights were chosen from the complete charter, which cover the core aspects relevant to the assessment of security measures: the right to privacy, freedoms, and the right to non-discrimination. The other three criteria were chosen from a vast catalogue of ethical norms. This selection includes those criteria, which are relevant for planning and implementing security investments: transparency, social cohesion, proportionality. Two general guiding questions for this dimension are: Is the security investment in line with fundamental rights and ethical norms? Does it include precautionary measures to reduce possibilities of infringement, abuse or function creep?
The discussion on the dimension	The interviews with decision-makers, which were conducted when developing these dimensions and criteria, show that societal aspects are at the core of decision-making. Fundamental rights and ethics embody one dimension relevant to address such societal aspects. The biggest challenge was to narrow the criteria of this dimension down to a manageable size. Excluding those criteria, which are implicitly covered in other dimensions (such as “effectiveness”, which would be covered in the economic dimension or the SGL), limited the choice of criteria. A second selection mechanism was the relevance of rights and ethics as already described in security research (privacy, non-discriminations and other freedoms are core themes). A final selection principle was to avoid mentioning the same criterion twice, namely once expressed as right, once as ethical norm. Ethical norms and rights are often interconnected and can in fact be understood as a continuum reaching from personal values to institutionalized rights. Aiming to capture a level between juridical expertise and a lay person-level for assessing such criteria, this dimension covers three (groups of) rights – the right to private life, freedoms, the right to non-Discrimination- and two ethical values, which are especially important during the implementation phase of security measures: transparency, and social cohesion. Finally, this dimension includes an overall criterion connecting rights and ethics with each other: proportionality, including also an assessment of security investments in terms of their suitability and necessity.

Criterion 1: **Title**	Private life
Criterion 1: Description (Mouse-over)	Does the security investment respect private zones, the right to private data, the right to your own picture etc.?
Explanation:	Example: The right to privacy is often discussed in relation to technological solutions, surveillance measures and data-retention.
Criterion 2: **Title**	Freedoms
Criterion 2: Description (Mouse-over)	Does the security investment respect freedoms of thought, conscience, religion, expression and information?
Explanation:	Example: The debate on censorship classically relates to freedoms of expression and information.
Criterion 3: **Title**	Non-discrimination
Criterion 3: Description (Mouse-over)	Does the measure discriminate against any societal group? Does it allow for diversity, equality and value-pluralism?
Explanation:	Example: Profiling measures are generally known for infringing upon the right to non-discrimination.

Criterion 4: **Title**	Transparency
Criterion 4: Description (Mouse-over)	Are the security investment itself and its effects easy to understand? Is it clearly communicated what the measure includes and entails?
Explanation:	Example: For political reasons and potential referendums on security measures a clear communication of advantageous and detrimental consequences is necessary.
Criterion 5: **Title**	Social Cohesion
Criterion 5: Description (Mouse-over)	Does the security investment further trust and confidence in the government and within society (between citizens)?
Explanation:	Example: If security investments openly infringe upon fundamental rights they might not only alienate the citizen from the government, but also create a culture of distrust, separation and fear among society.
Criterion 6: **Title**	Proportionality
Criterion 6: Description (Mouse-over)	Is the security investment suitable, necessary and proportional to the problem?
Explanation:	Should the measure not follow these assessments of suitability, necessity and proportionality, the investment should be re-planned. The assessments of criteria 1-5, as well as Security gain or loss and Social Implications, can also help to assess proportionality.

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.

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

2.3 Legal Framework

Alexander Neumann, Reinhard Kreissl (SWFB)

The debate on the legal regulation of security investments and measures covers a wide array of issues. In continental legal and political philosophy law is conceived primarily as the institutional medium guaranteeing individual freedom vis-á-vis the overwhelming powers of the state. Limiting the intrusion of the state into the sphere of civil society is one of the prominent tasks of modern law. Starting from this scenario rooted in modern theories of the state, the debate of liberty vs. security has gained momentum in the recent past (for a critical account of this debate see e.g. Zedner 2007).

This so-called "trade-off model" has triggered heated debates about the individual rights to privacy and the limits of state intervention into the lives of the citizens. At the same time it has become clear that the classic link between norm-breaking behavior and public reaction (based on criminal law) is weakening. While norm-breaking behavior can be identified after the fact, a security threat can only be hypothesized as a future event. It makes a difference whether a person is punished for having planted an explosive device in public space or whether a suspect is treated as a person who might perform such an act in the future. The latter is not based on hard empirical evidence but on risk assessment using an actuarial logic (Feeley / Simon 1994; Ericson / Haggerty 1997). From the perspective of legal theory the classic toolkit of modern law has severe problems when it comes to handling the category of risk (see for the German debate Prittwitz 1993). The logic of risk has no built-in limits and the logic of law loses its grip in face of a culture promoting the idea of a risk-based threat analysis. The logic of risk not only prevails in the field of criminal law, replacing the offender with the dangerous individual. Similar forms of reasoning can be found in occupational health and safety regulation or in consumer protection laws (see e.g. Hutter 2001). One of the most concise accounts of this fundamental shift from "danger" to "risk" (or from damage to threat) from the perspective of social theory is to be found in Luhmann's seminal paper on risk and danger (1993). Luhmann defines the logic of risk as being based on the consideration of future negative effects of present choices: Under the paradigm of risk an actor has to assess probable future consequences of choices s/he makes in a present situation since he will be held accountable for all future damages. Whereas tort law looks at past events, risk law looks to an undetermined future that is only accessible in terms of actuarial calculations.

With regard to the legal regulation of security measures it is very difficult to find good criteria beyond strict normative principles and these principles tend to lose their grip in public discourse when large-scale-disasters are envisaged that require urgent and serious action curtailing entrenched constitutional liberties of modern western societies.

Finding an adequate legal toolkit for a society that perceives itself no longer in terms of norms and norm-breaking, but in terms of future events and emerging opaque threats, is one problem that has to be considered, when planning legal frames for security investments. Another problem is the legal regulation of new technologies becoming operative in security systems. Radical critics of traditional law (e.g. Lessig 1999) have suggested to treat computer code as an equivalent to legal codes with regard to the governing of human conduct. Others have attempted to adapt new emerging techno-social hybrids (see Brown 2006) to traditional modes of legal reasoning (see Teubner 2006). From a social theory perspective one might ask to what extent the socio-

ontological foundation of modern law (and modern society) still can provide the basis for the system of legal categories supporting contemporary law. Are fundamental categories such as public and private, the concepts of life and death, the distinction between machines and humans still universally applicable (see Kreissl and Ostermeier 2009)? In legal theory, the new problems of regulation emerging with new technologies have triggered a complex debate about the limits of law (see e.g. Faulkner et al. 2012).

The points raised here should be understood as a very brief sketch of contemporary debates focusing on the problems of legal governance or legal regulation. The legal governance of security (or security technologies) is one of the key issues in these debates. What can be observed are attacks on fundamental rights, entrenched principles of the rule of law and the “Rechtsstaat” and, hence, a counter-factual stance should be maintained to keep these principles operative. Nonetheless it should be kept in mind, when discussing the legal framework for security investments, and in particular when these investments include state-of-the-art technologies that the regulatory gap between law and technology makes it difficult to catch up with the legally relevant questions emerging from an application of these technologies in the context of security policies.

Legal Framework	
Description:	The dimension “Legal Framework” addresses a selected list of problems that can arise when the implementation of a security investment is considered. These problems cover several areas of legal expertise from labour law to legal regulations limiting (or extending) the powers of police and other actors in the security field. Since security investments frequently involve surveillance measures, data gathering and intelligence work, privacy and data protection regulations are of utmost importance here. The legal regulations to be considered emerge from different sources, from European law to statutes established by local or communal legislative bodies. Furthermore, there are legal regulations with different binding force, starting from well-entrenched constitutional principles to different forms of soft law (e.g. codes of conduct, codes of practice, resolutions and declarations). Finally, one has to consider the different purposes of legal statutes. A law can limit the range of actions in a given field, but law can also be used to control the application of a technology in practical settings. This unfolds a four-dimensional frame of reference addressing the field of regulation, the source of the statutes, the different binding forces and the type of regulatory regime. These four aspects can be rephrased as questions to address the problems of the overall Legal Framework:

	What is the field to be regulated? Where is the source of the regulation (EU, national, non-state)? What is the binding force? What are the mechanisms of regulation?
The discussion on the dimension	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". Any security investment can involve a change in existing organizational procedures, the implementation of a new technology (hardware or software) or any combination of different elements (organisational process, data-processing, hardwired technology). Following the ramifications of all legal problems arising with any given security investment, can be a formidable task. When effects beyond national borders have to be taken into account, it has to be decided which (national) legal regulations are applicable. 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 relevance of classic legal regulation in the domain of new technologies. 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. For the purpose of assessing legal aspects of a security investment the legal framework will concentrate on a series of "sensitizing" questions requiring close scrutiny for any given investment. When considering the problems of a legal framework, two different approaches can be taken: one approach simulates a corporate lawyer's perspective by focussing on legal obstacles to be considered when designing and implementing a given security investment that is considered non-negotiable. The main goal of the corporate lawyer is to circumvent litigation against the corporation implementing the security investment. The other perspective would focus on legal issues in a more comprehensive way, by scrutinizing a given security investment in the context of a specific reading of the law, emphasizing the "rights" aspect of law rather than the litigation aspect and thus searching for a solution that is compatible with entrenched "rights". The set of criteria will combine the two approaches and raise a series of questions that are of importance for the legal dimension of an investment.

Criterion 1: **Title**	Data protection
Criterion 1: Description (Mouse-over)	When a security investment involves processing of personal data, data protection regulations have to be considered.
Explanation:	This is the most obvious dimension in the context of contemporary security investment. 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. If the technology applied does not actively produce data but uses data from other sources to be processed for security reasons, data protection regulations still have to be considered.
Criterion 2: **Title**	Accountability
Criterion 2: Description (Mouse-over)	Who is responsible for the proper functioning and/or failures of the security measure?
Explanation:	Law is the central institutional means in modern societies to handle the problem of accountability. Using a legal toolkit, actors can determine who is responsible for what. In the field of security systems malfunction or misuse are common problems. From a legal point of view one has to determine with whom the legal responsibility resides. What is the responsibility of the operators? What is the responsibility of the system providers?
Criterion 3: **Title**	Range of use
Criterion 3: Description	What is the precise form of use for a security investment?

(Mouse-over)	
Explanation:	Many security investments involving technological systems 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 above-mentioned criteria “accountability” and “data protection”.
Criterion 4: **Title**	Hazards to operatives
Criterion 4: Description (Mouse-over)	Is the security investment conform with labour protection laws, regulating the exposure of employees to hazardous conditions at their work places?
Explanation:	The operation of technological security systems sometimes requires employees to work under hazardous conditions. Hence the potential hazards to operatives, who are exposed to radiation or the like, have to be considered within a legal framework, e.g. in determining the limits of exposure. Hazards to operatives can be become a crucial criterion in the decision process.
Criterion 5: **Title**	Environmental hazards
Criterion 5: Description (Mouse-over)	Does the security measure produce any environmental effects?
Explanation:	Does the security investment have any effects on the environment and are environmental regulations involved in the specific solution for the security problem at hand? For the general public, who are exposed to security technology hazards, limits of exposure have to be determined according to relevant legally defined standards.

Criterion 6: **Title**	New legal provisions
Criterion 6: Description (Mouse-over)	Does the security investment include the use of novel technologies or procedures not covered by existing laws?
Explanation:	If e.g. police powers to stop-and-search are increased, or a new technology (e.g. UAV) is introduced, new regulations may have to be adopted. These new regulations my raise questions of legitimacy and may be in conflict with fundamental norms. Hence it is necessary to evaluate any new propositions against existing legal principles.

References

Brown, S. (2006) ‚The criminology of hybrids. Rethinking crime and law in technosocial networks', in: *Theoretical Criminology* 10 (2), S. 223-244.

Ericson, R. and Haggerty K. (1997) *Policing the Risk Society.* Oxford: Oxford University Press.

Faulkner A. et al. (2012) Introduction: Material Worlds: Intersections of Law, Science, Technology, and Society, in *Journal of Law and Society* Vol. 39 / 1. Pp. 1-19

Feeley, M. and J. Simon (1994) 'Actuarial Justice: The Emerging New Criminal

Law', in Nelken D. (ed.) *The Futures of Criminology,* pp. 173–201. London: Sage.

Hutter B.M. (2001) Regulation and Risk. Occupational Health and Safety on the Railways. Oxford, Oxford Univ. Press

Kreissl, R. and Ostermeier L. (2009) Wer hat Angst vorm großen Bruder? Datenschutz und Identität im Zeitalter des elektronischen Kapitalismus Sichtbarkeitsregime, in Krasmann, S. et al. (Hg.):

Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 25, 2009, p. 281-298

Lessig, L. (1999) *Code and other Laws of Cyberspace* New York, Basic Books

Luhmann, N. (1993) *Risiko und Gefahr*, in Luhmann N. Soziologische Aufklärung 5, p. 131-169. Opladen, Westdeutscher Verlag

Prittwitz, C.v. (1993) *Strafrecht und Risiko*. Frankfurt/M. Klostermann

Teubner G. (2006) Elektronische Agenten und große Menschenaffen. Zur Ausweitung des Akteursstatus in Recht und Politik, in ZfRSoz 27, p. 5-30

Zedner, L. (2007). 'Pre-crime and post-criminology?', *Theoretical Criminology*, Vol. 11, pp. 261-281.

2.4 Social Implications

Walter Peissl (OeAW-ITA)

The European Commission's Impact Assessment guidelines (European Commission 2009a; European Commission 2009b) provide a comprehensive approach to social impact assessment. Other dimensions in the DESSI procedure also cover some of the respective issues. Thus this section only lists relevant criteria which are not covered elsewhere. There is a broad range of potential social impacts. Security investments can have impacts on almost all criteria of this social dimension.

As stated above, we suggest to analyze "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). In all domains, which are covered by the criteria above you may find impacts on these levels. Sometimes the focus is more on the individual level e.g. in the employment-criterion; whereas other criteria focus more on the Meso- or Macro-level e.g. Governance and good administration or Culture.

Micro-societal (individuals)

The first level deals mostly with the sphere of social life and daily actions of individuals being affected by the measure. Affected persons may be customers of a company, which want 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 citizens of a state introducing electronic fingerprints on passports. However, citizens, customers, clients or passengers should not be considered the only elements of analysis. Employees of the institutions, companies or 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 is: 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 the ones who are "scanned" as well as those who are "scanning". The latter – field operatives running the system – are important, because technology technological security system 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 impacts of security investments on the implementing organisation or whole groups. If for example a public transport service decides to install biometric access controls, considerations on a meso-societal level include changes within an organization. Does this investment involve a special training of the existing field operatives or can security checks be done without the use of staff members? What does this mean for the whole organisation? The meso-societal level shall basically reflect upon the effects of the investment for a company/organisation

and will have a strong focus on the internal acceptance of the measure. At the same time, a security measure may also affect a specific “group of passengers”. They may 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 are the possible consequences for the society on the whole. 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 fear has become a normal social mental state when visiting an airport. This short 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/Douglas (2000) or “Social Sorting” (Lyon 2003).

There is also a temporal dimension 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. The DESSI process wants to draw attention of end users and stakeholders who are using the “DESSI machine” towards wider societal impacts and to encourage them to check their investment on possible side effects on society.

Social Implications	
Description:	The purpose of security investments is to raise security – or sometimes at least to raise the presumption of (subjective) security – or to minimise risk. Both may be achieved inter alia 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. Hence, it is necessary to gain insight into people’s thoughts and beliefs. 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. *Overall guiding question:* Does the security investment affect social life in any positive or negative manner? We suggest to analyze the social implications on three levels:

	• How does the security investment impact the social life of individuals confronted with this investment, e.g. their health or working conditions? (Micro-Level) • How does the security investment impact the social life of groups of individuals or organisations confronted with this investment, e.g. does it discriminate specific groups or minorities? (Meso-Level) • How does the security investment impact the social life in general, e.g. does it improve or impair working conditions or equal opportunities for all? (Macro-Level)
The discussion on the dimension	The social dimension is a very complex field with many different parameters to check. In order to analyze impacts in this field, "social implications" need to be operationalized. The bases of the following list of criteria are the European Commission's Impact Assessment guidelines (European Commission 2009a; European Commission 2009b). They provide a number of types of potential social impacts, which need to be considered in our assessment of social implications: 1. Employment and labour markets 2. Standards and rights related to job quality 3. Social inclusion and protection of particular groups 4. Gender equality, equality treatment and opportunities, non-discrimination 5. Individuals, private and family life, personnel data 6. Governance, participation, good administration, access to justice, media and ethics 7. Public health and safety 8. Crime, Terrorism and security 9. Access to and effects on social protection, health and educational systems 10. Culture 11. Social impacts in third countries This comprehensive list comprises areas, which are already covered by other dimensions within the DESSI procedure. For that

	purpose we use only some parts of the listed categories.

Criterion 1: **Title**	Employment and labour markets
Criterion 1: Description (Mouse-over)	How does the security investment influence employment relations, labour markets and job quality?
Explanation:	Security investments may have direct impacts on (groups of) individuals working in the field. The focus here is on the social rather than the macro-economic perspective, which is covered by the economic dimension. Operationalizing questions could be: • Does the security investment facilitate new job creation/job losses? • Does the security investment have an impact on the reconciliation between private, family and professional life? • Does the security investment impact job quality? • Will the security investment change daily routines and if yes, who will be affected by the measure in a positive or negative way?
Criterion 2: **Title**	Social inclusion
Criterion 2: Description (Mouse-over)	Does the security investment lead directly or indirectly to greater equality or inequality?
Explanation:	Social inclusion deals with issues such as equality, participation, deliberation and public engagement. As information may be a

	prerequisite of deliberation you may ask: • Does the security investment make the public better informed about a particular issue? • Does the security investment affect equal treatment and equal opportunities for all? • Does the security investment affect participation or deliberation possibilities? • Does the security investment impact on cultural and linguistic diversity?
Criterion 3: **Title**	Governance and good administration
Criterion 3: Description (Mouse-over)	Does the security investment affect the involvement of stakeholders in issues of governance?
Explanation:	• Does the security investment affect the autonomy of the social partners in the areas for which they are competent? • Does the security investment, for example, affect the right of collective bargaining at any level or the right to take collective action? • Does the security investment affect political parties or civic organisations? • Does the security investment affect the media, media pluralism and freedom of expression?
Criterion 4: **Title**	Health and educational system
Criterion 4: Description	Does the security investment affect the health and educational systems?

(Mouse-over)	
Explanation:	• Does the security investment have an effect on the education and mobility of workers (health, education, etc.)? • Does the security investment affect the access of individuals to public/private education or vocational and continuing training? • Does the security investment affect universities and academic freedom / self-governance? • Does the security investment affect the financing/organization/access to social, health and care services?
Criterion 5: **Title**	Culture
Criterion 5: Description (Mouse-over)	Does the security investment have an impact on citizens' participation in cultural manifestations, or their access to cultural resources?
Explanation:	• Does the security investment have an impact on the preservation of cultural heritage? • Does the security investment have an impact on cultural diversity?
Criterion 6: **Title**	Social impacts in third countries
Criterion 6: Description (Mouse-over)	Does the security investment have a social impact on third countries that would be relevant for overarching EU policies, such as development policy?
Explanation:	• Does the security investment affect international obligations and commitments of the EU arising from e.g. the ACP (African, Caribbean and Pacific Group of States) -EC

	Partnership Agreement or the Millennium Development Goals? • Does the security investment increase poverty in developing countries or have an impact on income of the poorest populations?

References

European Commission, 2009a, *Impact Assessment Guidelines SEC(2009) 92*, 15 January.

European Commission, 2009b, Part III: Annexes to Impact Assessment Guidelines SEC(2009) 92, 15 January.

Lianos, M. and Douglas, M., 2000, Dangerisation and the End of Deviance, *Brit. Journal of Criminology 40*, 261-278.

Lyon, D. (Ed.), 2003, Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination, London: Routledge.

2.5 Acceptability

André Gazsó (OeAW-ITA)

Risks are considered to be acceptable if they are insignificant and adequately controlled. This means that any means or method chosen to reduce the still existing risk (residual risk) leads to a state of safety which is generally accepted by society respectively a decision maker responsible for managing risks. In many cases acceptable risks are equivalent to those everyday risks that people normally accept in their lives. Under these circumstances little efforts are made to avoid these risks. In contrast unacceptable risks (alternatively intolerable risks) are risks society deems unacceptable, regardless of the benefits that may arise from the activity that causes the risks (e.g. technologies, substances or activities that bear a high hazard potential – independent from its probability of occurrence; nuclear technologies, especially nuclear fission – even in its “peaceful use”, would be a typical example).

The complementary consideration relates to the underlying technology, substance or activity to be rated as acceptable or unacceptable: Whether a risk minimization option (and a security investment is such a measure) will be regarded as acceptable or not depends on risk evaluation criteria which can be taken from (1) science, (2) technology, (3) economics and (4) political and societal considerations. In any of these cases there is a decision to be taken whether a certain residual risk (a risk below a certain threshold, mainly related to the potential damage) is low enough to be accepted (i.e. capacities of the concerned people are high enough to compensate still occurring damages).

The acceptability of risk can be significantly influenced by different means of risk treatment. The primordial risk source may be removed or substituted by another equivalent technology or activity (e.g. in the case of nuclear energy a nuclear power plant by an alternative energy technology, given that this energy technology is able to generate the same amount of base load with the same reliability. In this case primarily economical, but also technical criteria will influence the acceptability of the new technology, while mainly health and ethical criteria will have led to the substitution of the technology).

In general criteria to assess the acceptability of a technical solution will be related to the available scientific and technological knowledge (state of the art-criteria) which normally include not only the precondition of technical feasibility but also the condition of economic feasibility. Normally, technical safety threshold levels are considerably more rigorous than will be acceptable according to economic criteria. Measures based on considerations regarding the available (and usable) knowledge (i.e. led by cognitive discourse) will be oriented towards principles such as ALARA (as low as reasonably achievable) or ALARP (as low as reasonably practicable – emphasizing economic feasibility again). Another criteria influencing technology choice based on knowledge (expressed as state of the art) are the principles of best available technology (BAT) and best available control technology (BACT). These can be considered as complementary principles for ALARA/ALARP.

A different group of acceptability criteria can be derived from aspects of human attributes and/or behavior (psychology and social sciences). These characteristics influence the way we perceive, assess and evaluate potential damages (risks that is) in a considerable way. Thus, the same factors influencing risk perception will also affect the acceptability of a certain risk. The main factors are voluntariness and controllability of a technology or activity. If an activity has been started or an application has been chosen on a voluntary basis, the risk associated with this activity is regarded as lower, more or less independent of its actual hazard potential (personal health risks stemming from cigarette smoke would be a suitable example). Additionally, if an activity or technology in question is perceived as in principle under control and possible losses can be compensated by the affected groups by themselves, this activity or technology is regarded as considerably more safe. Both factors are further affected by the level of trust which exists towards a certain risk information source or risk management authority. Other psychological and sociological factors which have an impact on the way how we rate and evaluate risks (or in other words: how high a certain residual risk may grow) are the familiarity with a certain technology (how good it is known), the actual life situation we are living in (Are we able to avoid risks by our own means or not? Are we able to change our life situation such as profession or place of residence?). These questions depend partly on economic factors (income, money put aside), on physical factors (age, health) and on the status of our family and social relationships (e.g. young families with small children will rather be willing to move in a case of emergency than old people. The situation in the aftermath of the Chernobyl accident illustrates this phenomenon: The people who returned to the city of Pripyat were mainly old people).

A third group influencing our assessment of acceptability can be derived from political (and thus ethical) considerations. They represent aspects connected to our concepts of justice and are closely related to human rights aspects. A main factor is the perceived distribution of possible damages and the main consideration that we are normally sharing risks (possible losses or gains) with other persons or groups. The distribution of possible benefits and possible damages can be equal, more or less symmetric, or unequal (unsymmetrical), both in the sense of amount and the group of recipients. A situation where for example the benefit of a certain technology will be gathered by only one small group and possible damages will be spread over a rather large group will normally be regarded as not acceptable regardless of the actual amount of loss and or benefit. Additionally, risk acceptability is influenced to a certain degree by the fact by whom the decision to accept a certain risk is eventually taken. There are several cases which can be distinguished: 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). In other cases the 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). Last but not least the decision is taken by a different group than the risk recipients either uninformed or after employment of a proper risk assessment method. All cases would lead to separate and different evaluations regarding the acceptability of a certain risk.

Acceptability	
Description:	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 which is used in subsequent standards. 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 (here: security investment), 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".
The discussion on the dimension	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 notions of acceptability in one common concept and to add qualitative aspects to technical methods.
Criterion 1: **Title**	Economic acceptability - (cross-risk) comparison

Criterion 1: Description (Mouse-over)	Can the acceptability of a new or unfamiliar risk be compared to already experienced behaviours towards known risks?
Explanation:	If a society has already rated certain risks as being acceptable it can be reasonably followed that a similar option associated with the same or a lower risk might also be acceptable.
Criterion 2: **Title**	Balance of costs and benefits
Criterion 2: Description (Mouse-over)	Is the risk measurement in question economically acceptable? Has a cost-benefit analysis already been done?
Explanation:	Cost-benefit analysis tries to compare the cost and benefits of a variety of options by comparing (on a quantifiable basis) opportunities and risks (i.e. possible gains and losses related to a certain decision). Normally, the expected benefits and expenditures associated with a certain option are converted into monetary units.
Criterion 3: **Title**	Precautionary principle – ALARA
Criterion 3: Description (Mouse-over)	Does the security investment lead to a reduction of a certain risk to a reasonably achievable level? ALARA: principle to reduce a certain activity connected to adverse consequences to a level that is as low as reasonably achievable (ALARA).
Explanation:	Without economical, political and social restrictions this approach requires that every disadvantageous effect is reduced as far as (technically) possible (ALARA). Normally, the reduction efforts are limited by the consideration whether this management measure is still

	economically or politically reasonable.
Criterion 4: **Title**	Best available control technology (BACT)
Criterion 4: Description (Mouse-over)	Precautionary principle – BACT: Is the security investment in question based on the best available technology?
Explanation:	The principle of best available control technology (BACT) prohibits every adverse effect that could be prevented with a control technology which is available and has been proven as effective.
Criterion 5: **Title**	Voluntariness and Controllability
Criterion 5: Description (Mouse-over)	Has the security option been chosen by the concerned people and on a voluntary basis?
Explanation:	Do the concerned people have the possibility to control the application of the security measurement (at least to a certain degree)? Voluntariness: If an activity has been started or an application has been chosen on a voluntary basis, the risk associated with this activity is regarded (perceived) as lower. Controllability: If an activity or technology in question is perceived as in principle under control and possible losses can be compensated by the affected groups by themselves, this activity or technology is regarded as considerably more safe Level of trust: depends on the amount of perceived reliability of organisations and their representatives which are responsible for risk treatment (risk management). Sub-criteria encompass factors as perceived competence of the communication partner, objective and fair behaviour in the communication / participation process, and a certain consistency regarding the predictability of arguments and

	behaviour based on past experience
Criterion 6: **Title**	Fair distribution of risks
Criterion 6: Description (Mouse-over)	Are risks and benefits distributed fairly or not?
Explanation:	Distributional justice: whether possible risks and benefits are distributed fairly or not, equal (or symmetrical) distribution of expected (i.e. possible) benefits and losses Vulnerability: whether a certain activity is 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 Representativeness: whether all relevant groups, especially those groups which could be affected by a certain risk in an extraordinary way, have the possibility to engage themselves in the risk decision process and whether their value considerations are represented in the final decision.

References

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)

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)

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

Ortwin Renn, Risk Governance. Coping with Uncertainty in a Complex World, Earthscan/London, Sterling, VA, 2008

2.6 Political Significance

Marie Paldam Folker (DBT)

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 democratic values such as equality, political tolerance, accountability, transparency, participation, rule of law or control of the abuse of power is often critically described as the problem of striking the right balance or trade-off between security and democratic principles (Cas 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 counterterrorism, the "logic" of inevitability and necessity narrows the choices of how to define a security problem and the choices of selecting adequate security measures and relevant security actors. This is the 'downside of securitization' (Ole Wæver, personal communication). 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." Thus securitization brings with it depoliticizing effects by eliminating the possibility of democratic actors, such as citizens and policy makers, to influence security decisions (Ole Wæver, personal communication).

Accordingly, the DESSI dimension draws attention to the fact that the way the security agenda is framed as a matter for experts and authorities risks undermining the public perception of the possibility of anticipating, participating and exercising choices on adequate security measures. Security decisions involve choices - choices regarding if something needs to be done, what is to be done, how much and how it is to be done. By insisting on the possibility of choice DESSI seeks to expand the territory between the traditional dichotomy of threat and response.

A contemporary characteristic of modern societies is the interrelated security concerns cutting across climate protection, interstate conflict and adequate food supplies. Seemingly competing security logics of different security fields can be distinguished by the level of authority for decision-making. It is relevant to question how widely acknowledged it is in the general public to base decisions on specific expertise and to what extent it is accepted to question a security agenda from a non-expert view. Whereas it is still possible to raise doubts about the causes for climate change, after 9/11 there is more limited acceptance of critique towards measures against counterterrorism. According to Ole Wæver (personal communication) security inter-issue competition has created a 'conceptual inflation' of the security concept. Ironically, it is exactly this 'security inflation' that seriously challenges the logic of necessity. 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 try to 'translate' between different security fields but we lack a proper language for grasping and acting on the interconnections between security fields and for devising socially robust decisions on security investments. While investigation and decision-making within different security fields will

be based on scientific and technical expertise, the translation is also a task for non-experts.

Political Significance	
Description:	The dimension Political Significance seeks to unpack the political implications of security decision-making and proposed security investments. The previous decades have seen a proliferation of 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 local, regional, national, EU and global levels of security decision-making. The 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 face of insecurities. Guiding questions are: Is there a debate on the security issue? Does it empower new public agents? Does it help addressing political issues of a given security investment?
The discussion on the dimension	The criteria of the dimension Political significance have been identified and refined through interviewing political scientist and Professor Ole Wæver, by literature review and stakeholder discussion during the DESSI workshop “Making better security decisions – How do we get there?” November 8, 2012 in Copenhagen. According to workshop participants, the dimension should capture political significance in terms of welfare, wealth, civil rights and equality of citizens. The dimension describes how relevant the security investments are for citizens, political actors, their relationship and the political and public debate. Political opponents, people affected by a security decision or the media may boost the political nature of security investments. The dimension should also highlight the role and responsibility of the media for creating public debates on the political implications of security measures. In the workshop it was pointed out that it makes a difference whether ‘security issues’ are about people at large (as general populations) or about a small group (e.g. judges) and a political institution (e.g. court houses). The first kind naturally has a larger ‘audience’ of interested citizens than the second kind. When furthermore the security measure itself will be seen as relatively

	'technical', it is probably not to be expected that the public will be drawn to the issue. Democratic involvement is not a case only of 'allowing'/inviting larger publics into deliberations — people should also be 'free from politics', i.e. allowed to not be involved in a security issue.
Criterion 1: **Title**	State-citizen relationships
Criterion 1: Description (Mouse-over)	Does the security investment change the relationship between state and the citizen in terms of power relation or trust and if so, how?
Explanation:	The existence of the state embodies a delegation of power from the free citizen to the state, by which the citizen gives up some autonomy. In exchange for that, the state delivers collective services in terms of, for example, democracy, protection against enemies, a basic supply of food and water, healthcare, an education system etc. This bargain between the state and the citizen rests on the trust that the state will not misuse the delegated power. Any change in the power delegation, in the trust or in the services that the citizen can expect, indicates a shift in the relationship.
Criterion 2: **Title**	Political culture
Criterion 2: Description (Mouse-over)	Does the political culture change under influence from the insecurity or from the countermeasures against it?
Explanation:	The political culture of a country reflects its historical development. Thus, it can be influenced by history - incidents, events, conflicts, ideologies, economic or ecological change etc. Such influence needs not be negative, since it proves the ability of a society to adapt. But resistance to change may in other

	situations be better than adaptation, for example as seen from a democratic or equality perspective. Insecurity and the possible countermeasures to it can affect a political culture. Is this a real issue – and if so, does the change go in the right direction?
Criterion 3: **Title**	Potential for political abuse
Criterion 3: Description (Mouse-over)	Can the security investment be misused politically to take control over society or specific societal groups? Does it include a risk of total societal control?
Explanation:	The criterion on political abuse should add a reflection about the need for a "precautionary principle" towards the ultimate failure of the security investments – namely that it installs a risk of totalitarian control. This may be evaluated on a gradual scale – from a positive effect against totalitarian political development, over no effect, to a new risk for societal control. It resembles the criterion on "State/citizen relationships", but focuses on the risk for a deliberate misuse of the investment, whereas the other criterion focuses on incremental change in the state/citizen relation.
Criterion 4: **Title**	Democratic participation
Criterion 4: Description (Mouse-over)	Does the security investment impact democratic participation, means of exercising political standpoints, or the free exchange of viewpoints?
Explanation:	Being able to exercise participation is one of the main pillars in democracy. It includes the rights to meet, engage in public political discussions, to become member of a political party, to stand up for election and to vote in elections. Further, it involves the democratic participative culture of contributing to the management of our societal institutions by for example involving

	oneself as citizen representatives in public boards or attending and contributing to civic meetings or even protesting. To what extent does the security investment change the width and depth of such democratic participation by political actors and citizens?
Criterion 5: **Title**	Relations of expertise and non-expertise
Criterion 5: Description (Mouse-over)	Does the security investment change the role of experts and lay people in society? Do any of them gain more power through the security investment?
Explanation:	This criterion addresses the distribution of authority and power in the societal handling of security issues. It draws attention to the institutional power of security actors (intelligence services; security industry; police and military) on the one hand and alternative approaches to security (mediators in society; humanitarian organisations; peace-movements) on the other. It also comprises the layman/expert-relation in terms of their influence on non-expertise issues – such as answering the question of the acceptability of insecurity or security measures. The criterion rests on the belief that lay-people (including politicians) should judge normative questions and experts should deliver facts and insight.
Criterion 6: **Title**	Public debate on (in)securities
Criterion 6: Description (Mouse-over)	Does the investment change our way or ability to publicly scrutinise security issues themselves? Does it open up or close down the security debate?
Explanation:	The role of security investments is to protect/increase our rights – such as the right to speak freely. However, there can be many mechanisms at play in the public debate, such as differences in the access to the discussion (which “public” gets involved?), how

	potential public concerns are identified and mediatized (who sets the agenda?), or how open the access to knowledge is (who controls the information?). This criterion explores the impact of the investment on what could be termed as “the paradox of security discourse”: The larger the insecurity the bigger the risk of a highly controlled discourse.

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.

Cas, J. (ed.) (2009). Towards privacy enhancing security technologies - the next steps.; Wien (149 Seiten). Http://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

2.7 Economy

Petra Wächter (OeAW-ITA)

2.7.1 Overview: European Security Market

Security economics is a newly established research field which focuses on economic concepts and methods addressing causes, functionality and consequences of security-political activities (Brück and Engerer, 2009). No widely accepted definition of what security economics exactly is and what it covers exists so far. The most commonly used and broad description states that *Security economics is understood as those activities affected by, preventing, dealing with and mitigating insecurity including terrorism, in the economy* (Brück et al., 2008). This comprehensive definition makes it hard to distinguish between other areas closely related to security investments, e.g. defence sector.

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. Information about security revenues and expenditures is not always disclosed and many provided data are based on interviews the reliability of which is unknown (Künzel et al., 2009). Hence, the numbers obtained can serve as rough estimations of economic activity rather than exact measures. Regarding labour opportunities in the security market, Eurostat assesses the number of employees in private security services with about 1.1 million in 2008 (Martí Sempere, 2011a) and employees in the equipment market are assessed with about 54,000 in 2004 (ibid.).

On the demand side of the security market, governmental institutions are the main consumers, serving as the principal security provider to society. Governments usually demand high-end products and services to demonstrate their effectiveness in generating security. Security acquisition in the public sector is usually not centralized in one specific institution, because different goods and services are purchased according to the function of the demanding institutions (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 focus on the protection of their businesses including employees, clients and their company. Especially private organisations with a large numbers of costumers, such as shopping malls, are considered as important investors in security measures. Individuals invest in security equipment mainly to protect their homes.

Estimates about the security market from the supply side show the following distribution: video surveillance 23%, access control 14%, intrusion detection 22.8% and fire detection 43.5% (Martí Sempere, 2011a). While fire detection is not in the focus of the DESSI project, we assume that investments in video surveillance might be one of the most relevant ones, because the past has shown that these investments have a large share on physical security market.

2.7.2 Public and private investment

Public investment: Governmental (national, regional and local level) and public institutions are the principal security provider to society through legislative and executive power on the one hand and as large demander for security goods and services on the other. The important question arises, how the investment is financed and which budget has to be increased or decreased. Especially in the case of low- and middle-income countries security and defence-spending may not only increase budget deficits, but crowd-out economically and socially significant investment, thus jeopardizing economic development. On a more general level, a fundamental question may be how much governments spend on security investments and how these expenses are justified.

Private investment: 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 customers. Special cases are critical privately operated infrastructure (providers) with a high societal relevance, such as electricity grids, oil and gas pipelines and other energy grids, transportation (especially air transport), food chains, and health sector. A special case is if the person or the enterprise responsible for the investment is not the one who benefits and neither the one who suffers if the security measure fails. Therefore, as suggested by Anderson and Moore (2006), any analysis of security investments should start with an analysis of stakeholder incentives. Misaligned incentives of the investors lead to inefficient or low-quality measures and can possibly lead to an increase in long-term vulnerability (Moore, 2010). Another challenge constitutes information asymmetries. Within a general lack of data about security investments the tendency to underestimate the investments could be observed (Moore, 2010). Firms tend to underreport incidents because they fear the loss of trust and reputation among their clients and operators of critical infrastructure do not want to reveal information because of the fear of drawing attention to potential vulnerabilities. As a consequence, it is neither clear how much firms invest in security measures, nor how much they are losing to criminal activities. This lack of data on the costs of insecurity makes it even more difficult to manage the risk.

The analysis of security investments should also take into account who the company is that receives the investment assignment. It should furthermore be questioned if this company complies with certain criteria, such as reliability or social and environmental standards, which have to be fulfilled. In this context, transnational impacts are also of importance. Especially in the security equipment market, main products are at least partly produced outside of Europe, such as video surveillance equipment, which is usually manufactured in Taiwan, Korea, or China. The investors should consider production conditions for workers and also the environmental impact in the production process, also concerning distances of transport. Investments outside of the EU provoke cross-border investment flows and result in relocation of economic activities. Foreign investments underlie certain legislative regulations regarding trade conditions. It is therefore an important question if the imported goods are affected by such regulations.

2.7.3 Macroeconomic impacts

Effects on other sectors or regions: The focus on assessing impacts should not only lie on the respective organization, but also on the effects on closely related

industries and markets (defence industries, building monitoring and management industry, industrial automation and control industry, scientific instrumentation industry, ICT industry). Changes in the security regulations at transport hubs, for example, could increase transaction costs of trade (time and volume) and additional market segments may be influenced. The investment may also have a specific impact on certain regions or nations which are disproportionately affected.

Share of investment in security industry: The decision to invest into a specific security solution may have remarkable regional or even national impacts on the security industry. Such impacts are reflected in respective regional or national data on economic investment. An example would be high governmental expenditure on defence such as new drones.

Employment market and employment conditions: Research on the employment market in the security branch in Europe has shown that the majority of employees work in security services (Martí Sempere, 2011a). Analysis, as addressed with Criterion 6 of this section, 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 the production sector or the service sector (abroad or in the home country)?
- How many workers will the measure employ?
- How are the working conditions regarding time (full time jobs or part time; working by day or by night; time contracts; payment conditions) and other related questions.

Economy	
Description:	In standard economic theory, the decision to implement a certain security measure depends on whether the benefits outweigh the costs. The fundamental problem that occurs is that decision-makers often regard the investments in security technologies and services mainly as cost-factors and oversee long term-effects. The underlying reason is that direct investment costs can be easily identified whereas the benefits can only be identified in case of damage, except in case of human damage where it can hardly be monetarily quantified at all. It is almost impossible to assess what the optimal levels of the protective measures are, and 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 unfeasible (Jackson et al., 2007). The DESSI tool therefore intends to develop a more holistic view on the economic impacts of the security investment rather than just looking at the monetary side. 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.
The discussion on the dimension	The dimension Economy should not only address management decisions about security investments but seeks to assess the impacts of the investment in the economic environment. Basically, microeconomic as well as macroeconomic models and concepts provide explanations about economic dynamics and consequences. Microeconomic effects include: • Direct costs • Operating costs • Indirect and side costs • Non-monetary costs • Opportunity costs • Externalities • Organizational impacts (including possible administrative burdens on businesses) (European Commission, 2009) • Costs of misuse • Problems of free-riding Macroeconomic effects include: • Effects on specific regions, sectors or sensitive

	infrastructure • Effects on labour market • Large government expenditures: governmental crowd-out • Innovation and research • International relations
Criterion 1: **Title**	Direct Costs
Criterion 1: Description (Mouse-over)	What are the direct costs dedicated to the envisaged security investment and what are its operating costs?
Explanation:	The question regarding how much the investment costs 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. Some of the literature about investments in security industry recognizes a proclivity towards over-investing in protective measures at the expense of pro-active measures (Brück et al., 2008).
Criterion 2: **Title**	Indirect Costs, Side Costs and Lock-in Effects
Criterion 2: Description (Mouse-over)	What are the Indirect Costs, Side Costs and Lock-in Effects?
Explanation:	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 in their job. That means that they receive the salary no matter if the investment takes place or not. Moreover, side costs should also be considered. Side costs are additional costs caused by the investment, 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 activities that are affected by the selected investment alternative, like gains or losses of reputation or trust or time-consuming security procedures. These costs cannot be expressed in monetary terms although the consequences may have economic impacts. Security investments may cause short or long term economic dynamics in the respective organization: e.g., lock-in effects prevent organizations switching from one system to another, because it would cause high costs. Another important field concerns the inter-dependencies with other security investments that may be accompanied by unexpected costs.
Criterion 3: **Title**	Benefits
Criterion 3: Description (Mouse-over)	What are the potential benefits that can be gained by the security investment?
Explanation:	Benefits should not only include monetary gains (e.g. by the avoidance of certain incidents, if possible to assess) but also immaterial goods and values such as trust in the respective organization or reputation. Who benefits from the investment?
Criterion 4: **Title**	Externalities

Criterion 4: Description (Mouse-over)	Externalities are any unintended positive or negative effects caused by the security investment that affect non-involved third parties.
Explanation:	In security investment decisions, 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, even though it is not the primary intention to pollute the environment. Prominent examples are rare materials necessary for the production of video-cameras. Related mining-action causes severe environmental pollution and the extensive use of rare materials leads to over-exploitation. Waiting a lot of time in the airport due to longsome security checks causes negative externalities to the cafeterias, because people do not have the time to take a coffee any more. A positive external effect would be, for example, because of increased security measures in a public building, neighbours also feel more secure.
Criterion 5: **Title**	Innovation and Research
Criterion 5: Description (Mouse-over)	Can the security investment stimulate or hinder further research and development?
Explanation:	The investment can facilitate the introduction and dissemination of new production methods, technologies and products. This includes also the promotion or limitation of academic and industrial research. Moreover, it has to be considered if the investment affects property rights, such as patents, trademarks, copyright or other know-how rights. Additionally, the investment can promote or limit greater productivity and resource efficiency.

Criterion 6: **Title**	Macroeconomic Effects
Criterion 6: Description (Mouse-over)	Does the investment induce macroeconomic effects that address the economic impacts on larger economic scales?
Explanation:	The question of macroeconomic effects aims at the interconnectedness and interdependency of different areas of economic activities and its actors and institutions. Macroeconomic effects should be considered specifically in case of large, mainly governmental security expenses. Most relevant macroeconomic impacts include private and public demand side (also addressing governmental crowd-out), effects on other economic sectors and geographic regions and effects on employment markets and employment conditions.

References

Anderson, R. and Moore, T. (2006): The Economics of Information Security. Science 314 (27), 610-613

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

European Commission (2009): Impact Assessment Guidelines SEC(2009). European Commission

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

Moore, T. (2010): The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection 3 (3-4), 103-117