An extended Cost-Benefit Analysis for evaluating Decisions on Security Measures of Public Decision Makers

Eyal Adar[1], Christian Blobner[2], Reinhard Hutter[3], Kenneth A. Pettersen[4]

[1]WCK - White Cyber Knight, Tel Aviv, Israel
eyal@wck-grc.com
[2]Fraunhofer Institute for Factory Operation and Automation IFF, Magdeburg, Germany
christian.blobner@iff.fraunhofer.de
[3]CESS GmbH Centre for European Security Strategies, Munich, Germany
hutter@cess-net.eu
[4] University of Stavanger, Stavanger, Norway
kenneth.a.pettersen@uis.no

Abstract: Investments in security and/or security enhancing measures are marked by a potential of increased effects in certain security contexts, i.e. ramifications of security measures and their effects can not only be felt on a single cost-benefit dimension but on various related parameters which influence decisions on these measures. This is especially true for security related decisions by public decision makers. In the public domain, objectives have to be assessed that include an evaluation on a quantitative cost base as well as on non-quantifiable "qualitative" criteria. These qualitative factors reflect the multi-dimensional effects of security decisions and measures, which often present themselves as public goods. The FP7 funded project ValueSec proposes an analysis approach for potential effects of security related decisions of public decision makers that is based on the three pillars of "Risk Reduction Assessment", "Cost-Benefit-Analysis" and "Qualitative Factors Analysis". A combination of these individual approaches in a comprehensive toolset will support public decision makers in their decision making processes. The ValueSec project follows an application oriented approach in validating the developed toolset in realistic use cases. The use cases will include realistic scenarios and potential measures to be taken in a critical infrastructure context, e.g. in smart energy grids, airports and public mass transportation. ValueSec addresses planning and realizing of preventive and protective measures, not the actual operational/ contingency[1] measures and decisions of response forces in case of an incident.

Keywords: cost-benefit analysis, decision support, security measures, quantitative and qualitative assessment

[1] This restriction is given by the task description of the EU. Decision support processes and tools in the operational/ contingency phase have by and large different requirements like real-time capability, interfacing to existing Command and Control systems etc.

The environment for security related public decision making

The need for security is an inherent and basic need of human beings [1] and the provision of a safe and secure environment is one of the main objectives for public stakeholders. With the establishment of a secure environment, direct and consequential damages should be minimized and collateral benefits can be reaped, such as personal well-being and human as well as economic development. Security as a good, however, also entails characteristics that preclude its efficient provision on markets.

A secure environment is all encompassing, meaning that no citizen can be excluded from it and each citizen benefits from it in the same manner. Also the "consumption" of the secure environment by one citizen does not impede on the consumption of the same environment by another citizen. This non-exclusiveness[2] and non-rivalry[3] in consumption classify security as a prime example for a so called public good.

The provision of public goods through market mechanism is difficult, to say the least, as every citizen benefits from the provision of the good "security" but has little incentive to voluntarily contribute to its provision. This calls for responsibility and action of public stakeholders, i.e. the government, in the provision of the public good security. Governments have to create the legal and organizational and financial framework to provide security through a mandatory contribution system, i.e. mainly taxes. Public stakeholders, therefore, play a dominant role in the security environment. With the global economic downturn, started in 2008, the cost effective use of public funds has become of increasing importance for decision makers and the discussion of the financial crisis' influence on the security environment started also on the European level.[2] However, monetary and budget constraints do not form the only vector of decision making for public stakeholders.

Security related decision making in the public sphere needs to take into account a complex socio-economic and political environment, which often cannot be transferred into monetary terms. A cost benefit analysis in the field of security related public decision making therefore always has to consider combining quantitative and qualitative factors. This of course increases the complexity of analysis and demands a com-

[2] National governments provide a secure environment e.g. through investments in police forces and defense forces (personnel, training, equipment, etc.) but also through investments in other infrastructures. These are mostly financed through taxes paid by citizens. The non-exclusiveness in the case of security means that even a potential "tax-dodger", i.e. someone who is purposefully not paying taxes, still benefits from the secure environment. The fact that s/he does not pay taxes to finance the measures to provide for this secure environment does not change the fact that s/he is able to "consume" and/or benefit from the secure environment. S/he is a so-called "free-rider".

[3] A secure environment can be "consumed" in the way that it e.g. provides the opportunity for citizens to safely walk the streets of a city without the fear for his/her own health or life. Non-rivalry results in the fact that, to stay in the same example, the consumption of the secure environment by one person does not change another person's opportunity to consume the same secure environment, i.e. s/he can walk the street as safely as the first person or as any other person on the street for that matter. The secure environment as a good cannot be exhausted through joint consumption of multiple citizens.

prehensive and extended cost-benefit approach. A good example, however not security-specific, of multi-facetted government decision support can be visited in [6].

The project ValueSec – Mastering the Value Function of Security Measures – funded by the European Commission – develops a methodology and toolset based on an extended cost benefit approach to enable public decision makers to plan and execute better security related decisions. The project follows the objective of highlighting potential consequences of security decisions and ensuring measures to become more transparent and thereby supporting decision makers in better analyzing decision alternatives at hand.

Decision making contexts

Security related decisions in the public sphere encompass a wide range of possible contexts. To limit the scope of analysis, the ValueSec project defined five decision making contexts in which the project's methodology and toolset will be evaluated and validated. The decision making contexts chosen for the project are

1. A public mass event
2. Public mass transportation
3. Communal security planning
4. Air transportation and
5. Cyber security

The scope of possible measure in these contexts and the variety of factors influencing planning and decision processes are considerably large. Therefore, the principle idea of building a "general purpose decision support system" within reasonable time and with reasonable resources would be an illusion and ultimately not feasible.

With the definition of these decision making contexts, the project is able to cover at least a diverse range of possible decisions in security, encompassing different threat and vulnerability scenarios, different affected stakeholders (in the sense of public planners, operators of affected systems as well as of the affected public), different decision-making processes as well as different levels of decision making.

In the scope of critical information infrastructure protection, especially decision making context number five is relevant. Here the project will addresses an application scenario based on the security of Supervisory Control and Data Acquisition, so called SCADA systems in the energy sector. Concretely, the project will compare measures to be taken to prevent multilayered malicious activities performed by targeted tools able to propagate and exploit unique vulnerabilities specific to the attacked target in specific use cases. The aim of the measures is to prevent an advanced Stuxnet-like attack spectrum on the SCADA systems of energy providers.

This type of attacks on the energy sector would lead to grave consequences for various stakeholders, industries, households and governments that depend alike on secure energy provision and would be directly and indirectly affected by its degradation or shutdown. This scenario will show a high economic and social impact. With its cross functional interfaces to all elements of the economy and the public sphere, even a short-term wide-scale disruption of the energy supply could lead to the collapse of other critical infrastructures, such as the provision of food supplies, the provision of health services, manufacturing and service industries, banking and public services.

The development of a project use case includes the further definition and prioritization of objectives and measures together with relevant stakeholders. Potential measueres to counter and/or prevent a Stuxnet-like attack spectrum on the SCADA systems of energy providers are (non-exhaustively) listed in Table 1 below. These measures are classified according to risk treatment options, which are modeled on [7] but where the original category of risk reduction is further split up into the reduction of the probability of an adverse event happening and into the reduction of the impact of said event in case it happens.

Similar analysis on expected impact of security measures are being developed for the other 4 context scenarios. They may also include effects on risk transfer and risk retention.

Table 1 Potential Measures for ValueSec Cyber Security Use Case classified according to risk treatment

No.	Measure	Risk Avoidance	Risk (propability) Reduction	Impact Reduction	Risk Transfer	Risk Retention
1	Setting new policy to enforce strong partitioning between network zones	X	X			
2	Setting new policy to enforce monitoring of suspicious activities	X	X			
3	Setting new policy to enforce risk and vulnerability assessment	X	X			
4	Setting new policy to enforce strong restrictions that will prevent usage of disk-on-keys and connection of technicians pc's to the IT of the energy segments	X	X			
5	Setting central security emergency team to identify and communicate threats and		X	X		

	needed countermeasures					
6	Setting a central Certification Authority (CA) team to produce keys that will sign and approve installed application within the energy embedded systems	X	X			
7	Setting out of band sensors, and support of local teams to monitor directly the behaviour of the grid (not via the control systems that might be manipulated)			X		

With respect to the description of the decision making context of cyber security, the application scenario and the use case (based on individual measures or a set of measures from Table 1), decision makers have to formulate objectives on which they base their decisions. As an example the following objectives of decision makers are assumed:

1. Prevent damage to the energy grid
2. Prevent death and injury of citizens
3. Prevent damage/disruption to:
    a. Public Services, Infrastructures
    b. Corporations
    c. People at home and out
4. Minimize the impact if the event occurs
5. Minimize economic costs
6. Minimize social costs (e.g. political / electoral consequences, environmental damages)
7. Regard simplicity of and obstacles to, implementation
8. Reasonable time of implementation

To accommodate a cost-benefit analysis of the individual measures as laid out above with the decision makers' objectives as framing conditions, a comprehensive analysis approach is necessary that incorporates different aspects of decision and effects analysis. Apart from a classic cost-benefit approach, which, among others, compares investment and maintenance cost with potential loss of revenue in case of a malicious event, further analysis components are necessary to support decision makers.

The ValueSec toolset as designed so far will be able to produce results covering all 8 objectives as listed. It will be left to the decision maker and possibly to the organization or people supporting him, how results of the different categories will be weighted in a specific decision.

Three pillars of analysis

The ValueSec project addresses only a special kind of decision making. It is concerned with assessing decision alternatives on a strategic, i.e. medium- to long-term horizon. The methodology and the subsequent tool, by the mission set by the EU, will not support decisions on a tactical and/or operational level in the warning and response phase. The aim of the analysis is to support the decision maker in a systematic way and to enable the decision maker to compare different decision alternatives. These alternatives are characterized as measures or a group of measures addressing a specific threat. As depicted in Table 1, these measures can be very diverse in their way of implementation but their main objective, the elimination or the reduction of a risk[4], is the same. It has also been mentioned, that the point of departure for the ValueSec methodology is not the “classical” risk analysis. In fact ValueSec depends on the fact that such a risk analysis has been carried out beforehand to identify specific risks and to derive potential countermeasures to face these risks. Only after this step, security measures or alternative security measures will be defined to which the ValueSec methodology can be applied to, see also Figure 1.

As explained above, the decision making of public stakeholders in the field of security is embedded in a complex web of interdependences, which can obscure the full costs and benefits of decisions, and their consequent actions, as effects occur in different dimensions but are sometimes hard to identify, to trade-off against each other, and to attribute to the specific decision. This complexity has to be reflected in the way decisions should be supported analytically. Potential effects of decisions have to be made transparent and have to be analyzed on different levels. The ValueSec projects, therefore, follows the establishment of a comprehensive analysis framework based on three pillars of analytical methods and tools. These three pillars are:

- RRA = Risk reduction assessment: Calculating the expected reduction of risks by the security measure(s) in question
- CBA = Cost benefit analysis: Comparing those positive and negative effects of the measure(s) which can be expressed in monetary terms
- QC = Analysis of qualitative factors: Evaluating all criteria influencing the decision which cannot be expressed in quantitative terms.

There will be a certain dependency between the individual pillars, relying on the input from others. This is indicated by the red arrows in Figure 1, e.g. for the calcula-

[4] Whereby the elimination or reduction of the risk could be achieved by either reducing the probability of occurrence of an adverse event or by the reduction of the event’s impact or both. Furthermore, there is no restriction in the inherent characteristic of the measure. The main prerequisite is that the measure to be assessed is a more strategic rather than an ad-hoc tactical measure.

tion of monetary benefits, the CBA will require numbers about the reduced damages to infrastructure.

Following these three pillars, decision alternatives, i.e. specific measures or a set of measures, will be evaluated individually through the three individual analysis approaches. The results thereof will be consolidated and integrated[5] to form a comprehensive analysis and support for a public decision maker. The *Risk assessment pillar* will provide for an assessment of the potential change in the risk situation after the specific measure will be implemented based on a reference scenario describing the situation "as-is". In effect the analysis will indicate in how far the specific measure contributes to the reduction of risks. The aim of the analysis in this pillar, therefore, is not to carry out an overall risk analysis of the situation at hand. This had to be done beforehand and the result of the "pre-ValueSec-risk-analysis" is the measure to be assessed in this pillar. The objective of this analysis pillar then is to take the measure and assess their potential effects on the risk situation should it be implemented.

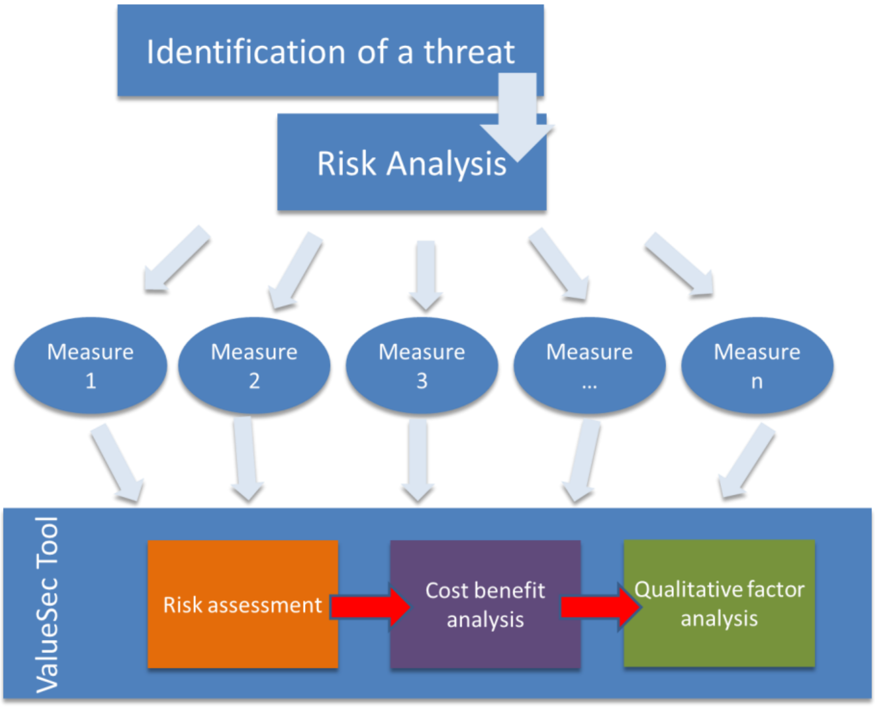

Figure 1 Positioning of ValueSec with respect to classic risk analysis

The *Cost benefit analysis pillar* provides an analysis of factors that can be expressed in monetary terms. The analysis takes into account different costs and benefits categories, such as, among many others, investment and maintenance or personnel

[5] This method of consolidation still has to be defined in detail.

and training. [3] The pillar also includes a monetary analysis of the costs and benefits that come into effect due to the implementation of the measure and which relate to the reduction and/or elimination of the risk at hand, e.g. the monetary benefit of infrastructure that is not destroyed. The cost benefit analysis will have to be put in a temporal context, i.e. it has to show how costs and benefits are distributed over time, and put into the risk context, showing how the change in the risk situation influences the occurrence and quantity of costs and benefits. The *Analysis of the qualitative factors pillar* assesses the potential effects of a measure on criteria, which cannot be expressed in monetary, physical, logical or other quantitative terms. These factors include decision criteria in different categories, analyzing effects on, e.g. societal and individual, ethical, political, (non-monetary) economic, environmental and technological levels or with respect to law and regulations. [4] This paper will primarily elaborate on this latter pillar.

An important factor to be considered with respect to supporting the decision of public stakeholders is the overall decision-making process. Stakeholder consultations during project workshops [5] and through the cooperation with the project's end-user partner Valencia Local Police as well as with the Valencia municipal government showed that

- Technical/ supporting personnel aggregate information to weigh alternatives and prepare decisions for public stakeholders / politicians / policy makers.
- Decision-making processes follow different iterations and are marked by different stages.
- Different kinds of information / different types of analysis are associated with different stages in the decision making process

The elaborations above allowed for the derivation of a conceptual decision making model, which in the course of the project, will be implemented it in a set of connected tools, i.e. the ValueSec toolset, for typical security measures ("Use Cases") in the framework of the different contexts. The decision rational follows the premise that decisions shall be taken following the assessment of individual measures or of sets of closely related measures, according to framework conditions set out by decision parameters, such as threats and risks, budget restrictions as well as political and societal needs; thereby the assessment combines the concepts of value, cost and risk as set out in the three pillars of analysis.

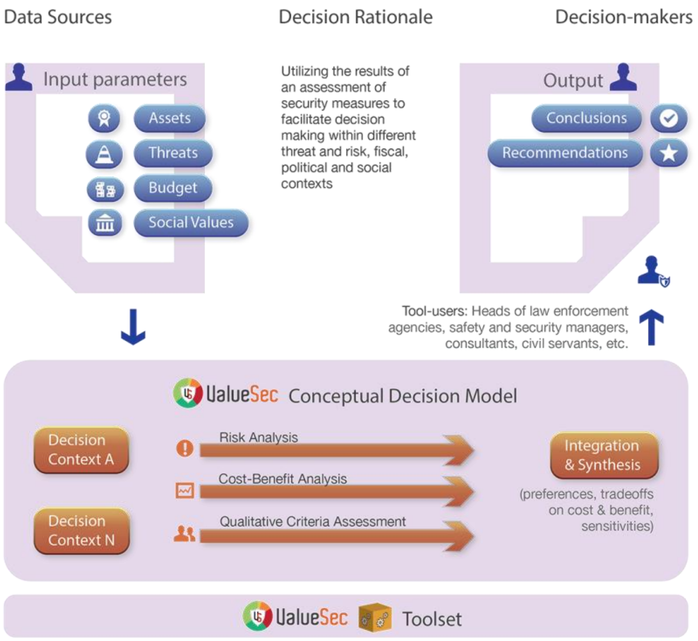
Data Sources
Decision Rationale
Decision-makers
Input parameters
Assets
Threats
Budget
Social Values
Utilizing the results of an assessment of security measures to facilitate decision making within different threat and risk, fiscal, political and social contexts
Output
Conclusions
Recommendations
Tool-users: Heads of law enforcement agencies, safety and security managers, consultants, civil servants, etc.
ValueSec Conceptual Decision Model
Decision Context A
Decision Context N
Risk Analysis
Cost-Benefit Analysis
Qualitative Criteria Assessment
Integration & Synthesis
(preferences, tradeoffs on cost & benefit, sensitivities)
ValueSec Toolset

Figure 2 Conceptual ValueSec Decision Model [3]

Figure 2 illustrates the interplay of the different components in the analysis process as envisaged by ValueSec. The process is marked by three distinct steps. A first step is the acquisition of input data and the definition of data sources that will be the base for the analysis of alternatives by the ValueSec tool. This data consists of scenario specific data such as threat assessments, specific costs or vulnerabilities associated with the decision alternatives, i.e. quantitative data in most cases. Also qualitative data is required as input. However, this data may or may not be scenario specific, when describing e.g. society's general attitude towards privacy or other social values. This step consists of setting up the assessment system with the necessary information for the ensuing analysis.

In the second step, the analysis, the ValueSec toolset will be used to evaluate the different security measures at hand, i.e. the decision alternatives. These will be assessed according to the three pillars as laid out above. With respect to the analysis it has to be noted that the ValueSec toolset will not necessarily recommend specific security measures and advertise the result as "the best" or "the optimal" decision. The main aim of the analysis experiments is to make the potential effects of different alternatives more transparent in order to empower decision makers making informed and well rationalized decisions and making trade-offs between alternatives based on their set of preferences and framework conditions.

This factor has to be considered with respect to the third step in the analysis process, the integrated analysis of the different results, and the reporting. The reporting function therefore will have to rely on easily accessible, preferably graphical, representations of cost-and-benefits associated with the individual measures to be assessed.

ValueSec risk reduction assessment focusing on cyber security

The ValueSec approach depends on the combination of different methodologies and different tools. Not only will the three aforementioned pillars have to work coherently to ensure a consistent analysis of decision alternatives but also different tools within these pillars will be employed to take account of the particularities of the decision making situation at hand. This is especially true for the *Risk reduction assessment pillar* of the analysis. As mentioned above, ValueSec considers five different so-called decision making contexts. These individual contexts have been chosen to cover a wide range of decision scenarios and offer the potential to assess various forms of potential measures. This wide range of application, however, also means that different forms of risk assessment might be needed in different decision making contexts. A risk assessment in the context of a public mass event is certainly different than in the context of air transportation and different than in cyber security. This fact is addressed in the ValueSec project by employing different tools for risk assessment in the different decision making contexts.

The use case of cyber-security, e.g., is driven by the application of the Lancelot software solution, provided by White Cyber Knight. One of the main differences between the cyber-security and the other use cases is the fact that unlike in the other decision making contexts, in cyber-security the inter-connectivity between different IT systems and infrastructures create a very complex posture of risk simply because a risk found at one end of the IT infrastructure might have a cascading effect on the other end of the same IT infrastructure or on other IT systems that might seem unrelated at first.

In today's modern environments there is a strong and growing linkage between "traditional" IT systems and IT systems which control physical devices. Together, they create the Critical Information Infrastructures (CII), which enable controls and command over physical daily critical resources such as electricity, water, etc.

The connectivity and complexity of these CII makes it very hard to understand how a potential cyber-risk on the CII may affect the entire infrastructure and possibly pose a threat to human lives and endanger the "real" world just as it endangers the cyber space.

Lancelot developed by White Cyber Knight enables and end to end approach to this challenge by providing a pragmatic way to map and connect different resources of the IT and CII and later on assess how a risk found on one resource (or asset) may affect other resources of the same infrastructure. The end to end approach of Lancelot is based on the End to End Security Assessment methodology (EESA) that looks and assesses processes that are composed of different resources. By using the EESA methodology, Lancelot can highlight risks that might seem minimal at first, but because of the inter dependencies they actually affect the entire CI, a fact that depicts them in an entirely new light.

After the risk assessment phases, Lancelot will pass the calculated risk on the CII to the other pillars to continue with the cost-benefit analysis and the social impact assessment.

Analysis of qualitative factors supporting quantitative approaches

The specific characteristics of security in general, and of critical infrastructures as providing critical services in particular, and having a high degree of interconnections and interdependencies with the society and the economy [8] demands holistic analysis approach as described above. Additionally, the property of "security" as a public good further require looking beyond a simple cost-benefit analysis purely based on monetary / quantitative cost-benefit factors. Previous work on quantitatively based cost-benefit analysis can be found especially in the field of ICT security, see e.g. [9] and [10]. However, interdependencies and ramifications of security related decisions in the public sphere exist and/or occur to a large part on qualitative dimensions.

A large body of research on these interdependencies has been collected by the EU research project EUSECON - A New Agenda for European Security Economics[6], coordinated by the DIW German Institute for Economic Research. ValueSec used this research as a starting point to map out the space of potential effects and their potential interrelations and knock-on effects of security decisions on the politico-economic sphere.[7] A non-exhaustive documentation of the effects space can be found in [11].

To operationalize the use of qualitative factors in the analysis process the ValueSec consortium derived a selection of approximately 120 individual qualitative criteria, which were grouped according to the following main categories [4][8]:

- Society,
- Individuals,
- Law and regulations,
- Rights and ethics
- Politics,
- Economics,
- Technology and science and
- Environment

The derived qualitative decision criteria will be used to enable a qualitative analysis of the decision alternatives. For this the decision maker will be asked to first describe the relative importance of the main categories as well as the relative importance of the individual criteria in a group using specific weights[9]. This is to define the main decision drivers and to eliminate "irrelevant" categories and criteria. The weighing

[6] See http://www.economics-of-security.eu/eusecon.

[7] A knock-on effect could be for example that a terrorist attack severely decreases the touristic attractiveness of a region, which decreases the tax income of the region from the tourism industry. This might influence the financial stability of a region, which is heavily dependent on tourism, leading to the cut-back in government services and increase in overall unemployment through job losses in the tourism industry and the loss of public sector jobs.

[8] The full list of criteria can be accessed through this document and will not be reproduced here.

[9] It will also be possible to add new criteria to the existing list to take account of additional criteria relevant for individual decision makers.

will be performed exclusively by the decision-maker and/or the technical personnel supporting him/her in the decision making process. The ValueSec tool may provide for pre-defined set weights, e.g. stating that ethics might be more important than environmental criteria. However, these will only be of recommending character. The assigning of weights lies solely with the decision maker and should present the decision maker's preference for the individual categories and the criteria.

For each of the relevant criteria the decision maker is then requested to define generic value functions, i.e. defining in how individual effect characteristics / parameters of said criteria (e.g. low - medium - high or negligible - catastrophic) relate to values on a normalized scale. Setting-up the weighting scheme of the analysis system will be performed on a "decision-making-context-basis" as different context and decision makers will have different preferences.

For the analysis of the qualitative decision criteria, the decision maker then revisits the previously defined decision drivers and assesses the potential effects for each criterion based on his/her expert knowledge and/or further expertise. Additional expertise can for example be gathered through stakeholder consultations, expert interviews or other forms of involving third parties affected by the decision or knowledgeable about the domain. The previously defined value functions are used to describe the potential effects per criterion, which will then be transferred to a normalized scale for the analysis. Based on this information the ValueSec toolset will provide the decision maker with an analysis of qualitative criteria, identifying specific influences of specific decision criteria, allowing for sensitivity analysis and for the trade-off between criteria.

Interaction of the three pillars and decision support

The proposed ValueSec methodology breaks up the decision analysis in three distinct elements, dealing with the influences of specific measures to influence a risk, on the costs and benefits of implementation and on qualitative factors, which are hard to put into specific and relevant numbers. With this break-up of the overall analysis and the establishment of three individual pillars of analysis, ValueSec enables the decision maker to in the first place assess the three categories influencing a decision. It also enables the decision maker to perform trade-off analyses with respect to the results of the individual pillars and with respect to the different decision alternatives.

On the one hand the analysis results of the individual pillars can be regarded as single results of the individual modes of analysis, on the other hand they have to be regarded in the common decision making context and application scenario. Additionally, results of the individual pillars influence the analysis in subsequent pillars. The ValueSec tool proposes the sequence of risk assessment → cost benefit analysis → qualitative criteria assessment. The relation of results in this sequence can as an example be described as follows:

- The risk assessment describes in how far the security measure will reduce probabilities and/or impact values

- The cost benefit analysis takes account of the reduced probabilities and impact in monetary terms for the assessment of conditional costs and benefits, e.g. costs and benefits that occur based on the (reduced) probability and impact in the adverse event assumed.
- The qualitative criteria analysis takes into account potential costs and benefits of measures for its assessment of individual qualitative criteria, e.g. if increased cost jeopardize the political viability of a measure.

Within this framework the decision maker is then able to perform trade-off analysis between the individual pillars and between measures to select the decision alternative that most suits his/her preferences. For this it has to be noted that the main objective of the ValueSec project is not to “optimize” security in the different contexts. The ValueSec tool provides a supporting mechanism helping the decision maker to find and justify his solution , i.e. the methodology and the tool will not be able to tell the decision maker which alternative to choose, but will deliver data, arguments and recommendations in support of or possibly also in denial of certain security measures. . The decision making power will stay with the decision maker and will not be relegated to a decision support tool. The main objective of the tool is to present the decision maker with a transparent overview of the potential effects of his/her decision and enable him/her to make better informed decisions on this basis.

Conclusion

The ValueSec approach provides for a systematic incorporation of qualitative decision criteria for the cost-benefit analysis of security related decisions by public stakeholders. Together with a Risk reduction assessment and a quantitatively oriented Cost-benefit method, the analysis of qualitative factors form the three pillars of a comprehensive Cost-benefit analysis approach. This approach is necessary due to the specific and different/ individual characteristics of security contexts e.g. in critical infrastructures and their multiple interfaces to various segments of the society; to households, industries and the policy level alike. Furthermore, “security” as a public good has an inherent social dimension which needs to be reflected in security decisions.

The ValueSec approach consequently provides an analysis approach which not only brings together these individual three pillars of analysis but also enables decision makers to perform trade-offs between these different pillars and base their decisions on a sound analytical framework.

The toolset under development will be tested and demonstrated in realistic use cases. The person and organization to be supported will primarily be the public decision maker. This has been set by the EU security research call. It is the strong commitment and intent of the consortium to extend and offer it to the private and commercial decision maker as well.

References

[1] Maslow, A.H. (1943). "A Theory of Human Motivation", Psychological Review 50(4): 370-96.

[2] Mölling, C. and S.-C. Brune (2011) “The Impact of the Financial Crisis on European Defence”, Directorate-General for External Policies of the Union, Directorate B, Policy Department, http://www.europarl.europa.eu/document/activities/cont/201106/20110623ATT22404/20110623ATT22404EN.pdf, retrieved November 15, 2011.

[3] Rosqvist, Tony; Minna Räikkönen; Markus Jähi and Liisa Poussa (2011) “D2.2 Data model and decision Model”, ValueSec Project, http://www.valuesec.eu/sites/default/files/2011.12.19._VALUESEC_WP2_D2%202%20_Data_Model_and_Decision_Model_FINAL.pdf, retrieved June 8, 2012.

[4] Mareile Kaufmann (2012) “D3.3 Evaluation of methods and tools, and the required improvements”, ValueSec Project, http://www.valuesec.eu/sites/default/files/D3.3_Evaluation_of_methods_and_tools_and_the_required_improvements.pdf, retrieved June 8, 2012.

[5] Poussa, Liisa; Minna Räikkönen; Markus Jähi; Tony Rosqvist; Helena Kortelainen and Riitta Molarius (2011) “D2.5 Report on workshop user needs and requirements”, ValueSec Project, http://www.valuesec.eu/sites/default/files/VALUESEC_D2.5_Workshop_user_needs_and_requirements_FINAL.pdf, retrieved June 8, 2012.

[6] Kevin Foley, Booz Allen Hamilton: “using the value measuring methodology to evaluate government initatives”, Proceedings of the 2006 Crystal Ball User Conference.

[7] Dorfman, Mark S. (2007) Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall.

[8] ESRIF (2009)Esrif Final Report. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf, retrieved June 8, 2012.

[9] Sklavos, N.; Souras, P.: „Economic Models and Approaches in Information Security for Computer Networks“, International Journal of Network Security, Vol. 2, No.1, pp.14–20, Jan. 2006

[10]Drugescu C.; Etges, R.: „Maximizing the Return on Investment on Information Security Programs: Program Governance and Metrics”, Information Security Journal: A Global Perspective, Vol. 15, Issue 6, Pages 30 – 40, 2006

[11] Blobner, Christian (2011) “ValueSec D2.3 Relational Concept between Security and Politico-Economic Sphere, ValueSec Project, http://www.valuesec.eu/sites/default/files/D2.3_Relational_Concept_between_Security_and_politico-economic_Sphere.pdf, retrieved June 8, 2012.