Possible future opportunities for risk and capability assessments in the Baltic Sea Region

FROM GAPS TO CAPS

Possible future opportunities for risk and capability assessments in the Baltic Sea Region

From Gaps to Caps - Project funded by the European Commission, DG ECHO
Project number: ECHO/SUB/2014/693890
Full name of project: "Risk Management Capability on Gaps Identification in the BSR"
Short name of project: "From Gaps to Caps"
Project Coordinator: Fire and Rescue Department under the Ministry of the Interior of the Republic of Lithuania
Editors: Björn Karlsson, Ass. Prof., University of Iceland and Director General, Iceland Construction Authority; Anthony Jay Olsson and Marlene Riedel, Council of the Baltic Sea States Secretariat

Introduction

There is a strong link between security, risk and capability to manage risk. Taking into account that risk is a combination of consequences of an event (hazard) and associated likelihood/probability of its occurrence and having in mind that security is a state or process characterized by risk, it is reasonable to assume that knowing value (described qualitatively or quantitatively) of risk security is entirely determined. Deeper considerations of this statement show that there are some doubts about this assumption. Of course, security is inversely proportional to risk. It means that the higher level of risk the lower level of security. Although this is a true description, it says nothing about the question to what extent a protected object is secure. This question can be formulated in another equivalent way, for example: what is resilience of the protected object? To solve this problem, it is necessary to answer the next question: how can we manage the risk to get its value (quantitatively or qualitatively) at an acceptable level. In short, how to manage the risk to be as secure as we desire. These very short considerations show a logical way in searching solutions of creating the security optimal structure. Namely, the following steps should be done:

1 Risk assessment (Project 14.3)
2 Assessment of risk management capability (From Gaps to Caps)
3 Resilience assessment (future challenges).

The From Gaps to Caps project s a continuation of the 14.3 project and should be considered as a necessary step to solve problems related to the development of a resilience assessment methodology. An elaborated methodology will allow a comparison of different resiliences among the Baltic Region States and optimize the regional security structure.

In this report the methodology of capability risk management is described and a direction for a further discussion about resilience and security is indicated.

Baltic Sea Region Methodology

The here proposed methodology is mainly based on the work on national risk and capability assessment of the Swedish Civil Contingencies Agency (MSB). In this methodology, scenario analysis which allows to assess the ability to prevent and to respond to crisis plays the central role. It is important to underline that during scenario analysis, there is a hidden assumption that an unwanted event connected with an identified hazard has occurred. Because of this assumption the scenario analysis is actually a conditional risk analysis (scenario describing a real situation provided an unwanted event has happened). This means that the process of capability assessment, until this step is distinguished from the risk assessment process, does not need to determine a probability of occurrence. In short, in the capability assessment process, the probability of occurrence of a "bad" event equals to 1.

The methodology is user-friendly, practical and creates conditions for scenario analysis of a good quality. The methodology can be and should be used for capability assessment, including scenario analysis, in any context and by actors (experts), different than authorities responsible for crisis management. Moreover there is a strong linkage between hypothetical scenario, actual events and exercises.This is the reason why Task D of the Gaps to Caps project plays next to Task C an important role in the capability assessment process.*

In many cases, desk officers and policy makers responsible for security at a certain level of administration are not operative, so the methodology is considered a general concept and serves as a tool which should be used by organizers (term "organizers" is used in a broad sense) of a security system at the administrative level. This characteristic of this methodology causes, that in most cases, experts from different branches should be involved in the capability assessment process.

The selection of proper experts is one of the most important factors to a successful of capability assessment and one of the necessary steps in capability risk management process. It seems that the way the experts are selected, needs special procedures and should not be based on intuitive feelings. Therefore, an elaboration of the selection procedures is a future challenge.

* Task C of the Gaps to Caps Project has been lead by the University of Iceland and focused on the formulation of a methodology on risk management capability assessment for the BSR. Task D, lead by the Hamburg Fire & Rescue Service in Germany, compared evaluations of previous incidents and emergencies and exercises in order to compile conclusions on differences/ similarities of best practices and main gaps, while planning and assessing capabilities in the BSR.

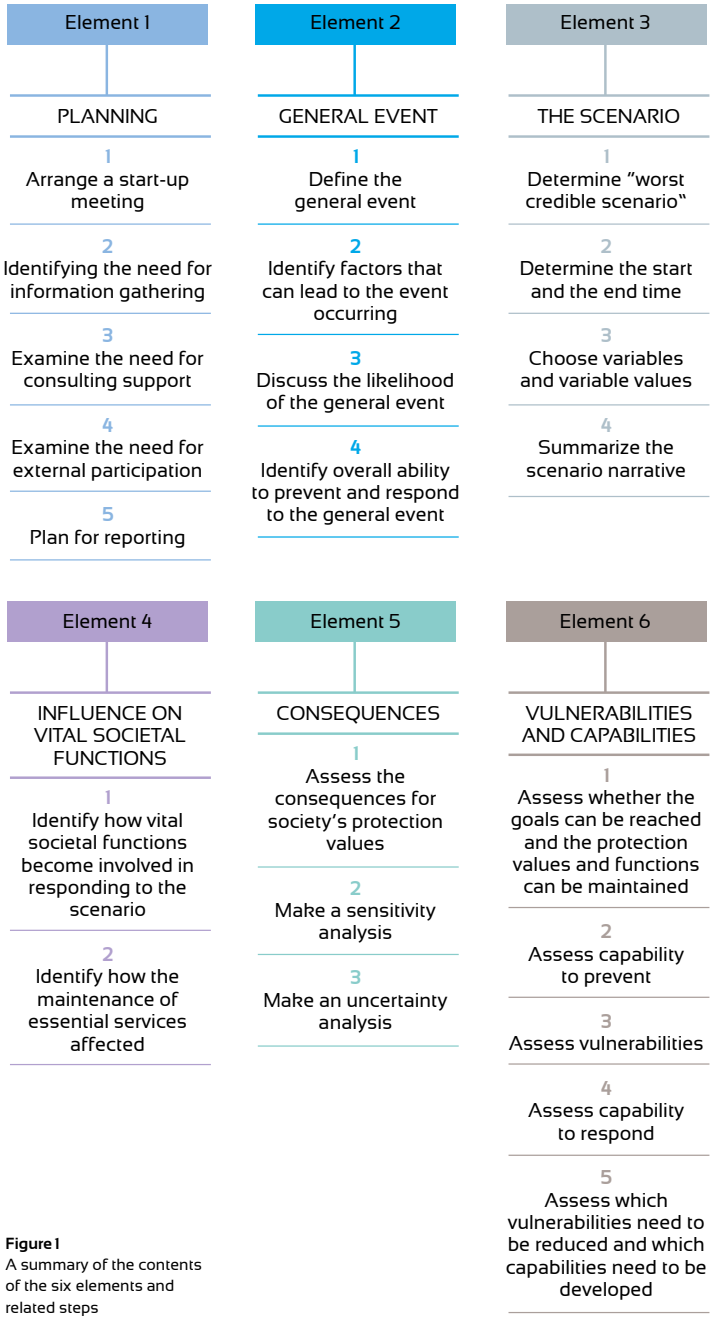

Figure 1
A summary of the contents of the six elements and related steps

Another problem and challenge which is related to the experts themselves, is their very own work. There are many methods experts are working with and due to the purpose of this project and limitation of subject, only a few commonly used methods are listed - yet without any descriptions.

1 Foresight.
2 Delphi Method.
3 Expert Panels.
4 Brainstorming.
5 Lateral Thinking.
6 Mindmapping.
7 Cloud Diagram in Logical Thinking Process
8 And many others.

Elaborating one or some of these methods, for capability assessment purposes is the next big challenge in possible future works.

The BSR methodology embraces and is based on six fundamental elements.

A first glance at the scheme (fig. 2) shows that there are two branches of the presented procedure. The first branch is related to risk assessment, while the second one is connected to capability risk assessment. Until element 3, each step is common for risk management capability assessment and risk assessment. To be more precise, until likelihood and consequences estimation both assessment procedures are identical. This is a common branch of both estimations. The only exception are the EU Guidelines serving only as an estimation of ability to assess risk management capability.

A first remark is that this common branch of both procedures indicates an important property of resilience estimation. This is because, on the one hand, resilience is a function of risk and capability to manage that risk. On the other hand, generally speaking, resilience is a measure of possibility of the crisis situation occurrence. So, risk and ability to manage it, are inseparable if issues of avoidance of this crisis situation emergence are considered.

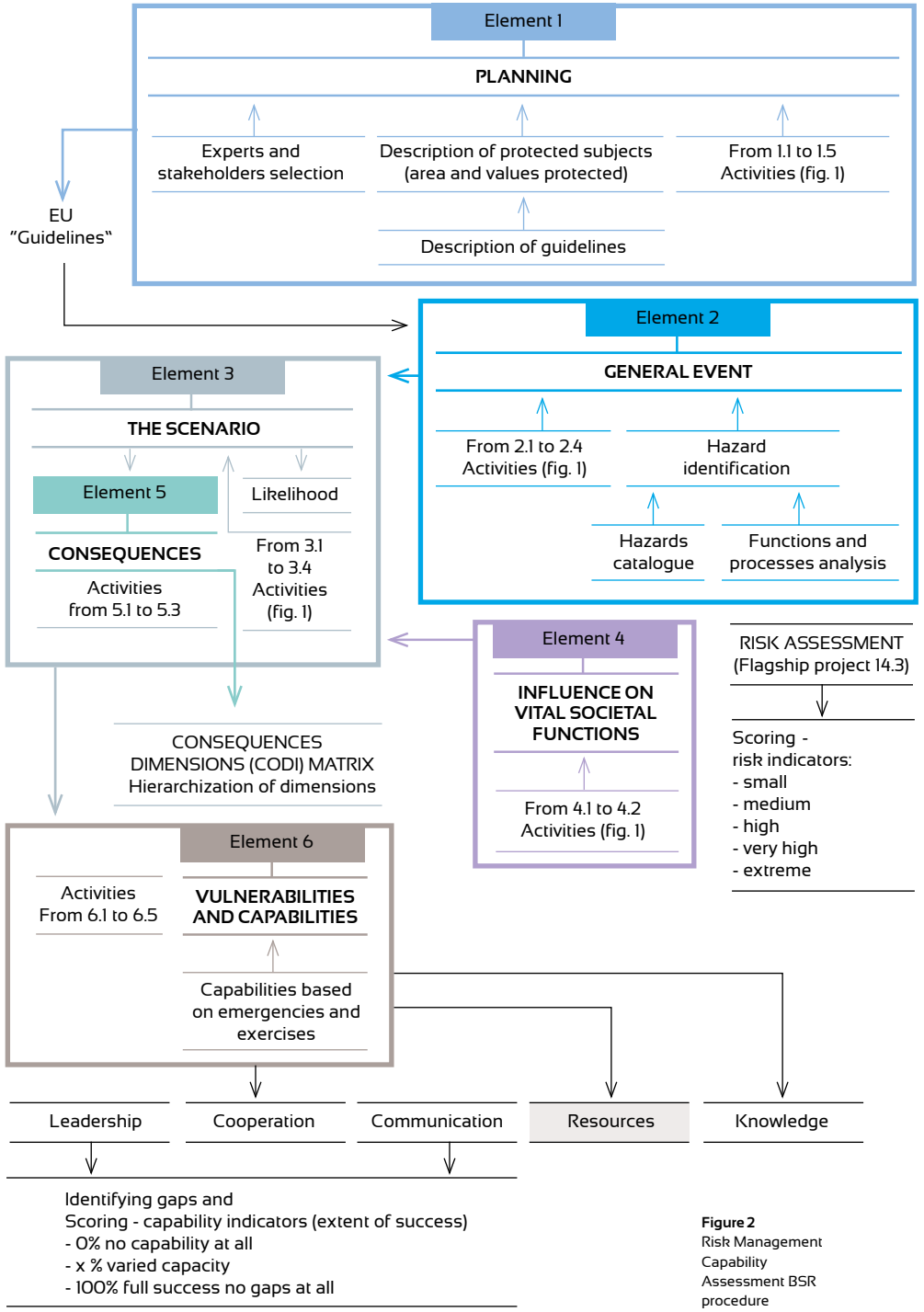

Figure 2
Risk Management Capability Assessment BSR procedure

At second glance, what should be done in relation to the illustrated scheme, is that risk assessment and the ability to manage it, should be strictly connected to the equivalent threat. Following on from this, the same scenario as well as the same possibility of the general event occurrence (the last one, if it is necessary, in the case of assessment of capability risk management process) should be also linked.

Last but not least, it should be mentioned that the elements overlap each other and it is practically difficult to separate them entirely. For instance, Element 3 contains the entire Element 5 because describing the scenario is nearly impossible without describing the consequences of the general event.

Besides the aforementioned, it is worth to indicate that the whole BSR procedure includes results The first matrix is the RISK MATRIX following the 14.3 project. The next one is the CODI(fied) MATRIX which confronts consequences with dimensions. The CODI Matrix allows to prioritize dimensions and to assign them to each dimension's proper weight. For example: the "worst credible scenario" (Element 3) including consequences (Element 5) for a threat could be:

1 fatalities,
2 wounded,
3 huge damages,
4 disturbances of functioning of some institutions (Element 4),
5 difficulties to get places of work (Element 4).

Having identified all kinds of consequences, it is possible to construct the CODI Matrix as follows (see Fig. 3)

The analysis of the CODI Matrix shows that in our case the most important dimension (biggest gap) is "cooperation". This is because the number of boxes with X indicating this dimension is the highest. One possible way to assign weight to each dimension could be by assigning fractions given by dividing the number of indicated boxes for a given dimension by the total number of indicated boxes. In our case, for the "cooperation" dimension this fraction (weight) equals 3/9 (weight 3/9 indicates that there are three ticked boxes out of nine). Then for "communication" and "resources" one can assign 2/9 for each of them and 1/9 for "leadership" and "knowledge". It is advisable to consider this way of prioritizing the gaps within each dimension. Maybe, for decision makers, it is enough to

Figure 3
An example of CODI Matrix construction

	Fatalities	Wounded	Huge Damages	Disturbances of functioning	Difficulties to get to work places
Leadership				X	
Cooperation	X		X	X	
Communication	X	X			
Resources		X	X		
Knowledge					X

indicate only one dimension to be improved as a very first step of building up the security system. In short, the CODI Matrix codifies the priority of each dimension and indicates a direction for risk management capability enhancement.

The next issue to be considered is an answer to the question "what is estimation of risk management capability done for?" One possible answer is to estimate resilience of the region (state, community, county etc.) by constructing a Resilience Matrix (Vulnerability? or Crisis Situation?) Below, it is illustrated how it can be done using the BSR procedure.

Namely, after the entire BSR procedure, we identified gaps within each dimension and scoring capabilities indicators as well. Having scoring capability and scoring risk we can construct the Resilience Matrix as it is presented in Fig. 4.

Figure 4
An example of Resilience Matrix

Capability / Risk	Small	Medium	High	Very High	Extreme
100%	High	Resilience			
80%	(Low possibility of	crisis situation)	Tolerable	Resilience	No Resilience
60%			(high possibility of crisis situation)		or unique facilities
40%	Acceptable	Resilience	Too Low	Resilience	or extreme event
20%	(possible crisis	situation)	(Very high possibility	of crisis situation)	(always crisis situation)

Using the same BSR procedure in different countries, different states or regions, it becomes possible to compare resilience between them and find out where weak points exist.

The indicated purposes for using risk management capability assessment are not the only ones. Of course, all the aspects discussed by now can be considered challenges for future work. This present discussion is only taking general problems into account in regards to the building up of the security system in the BSR. In practice, almost all issues need to more clarified and determined a more detailed fashion in the future.

Keeping these remarks in mind at the present stage of the elaborated BSR procedure, some details of each step of capability assessment will be described very briefly.

In the following, all these considerations will be conducted step-by-step according to the BSR procedure.

Element 1

PLANNING

1 Arrange a start-up meeting

2 Identifying the need for information gathering

3 Examine the need for consulting support

4 Examine the need for external participation

5 Plan for reporting

Expert and stakeholders selection: Although this step seems to be easy it needs some attention. First of all it should be underlined that every kind of management should use the Total Quality Management technique. This technique requires from the authorities which are responsible for security, special knowledge related to management methods. During the recruitment process the authorities should take into account the following selection criteria:

- Universality of experts
- Proper number of expert team
- Independent thinking and future vision formulation skills.

Planning: Planning is based on two pillars: "description of protected subjects (and protected values)" and five "activities".

- It would be useful to elaborate guidelines on how such a description should look like. The guideline allows the experts team from different countries to describe the subjects more or less in the same way. This, in turn, gives the possibility to compare the final results of the entire procedure. This is one of the challenges which, at least, should be considered in the future designing of the security system.
- Activities in the Planning stage consisting of the five following steps should be done.

1 Start-up meeting
2 Information gathering
3 Consultant support
4 External participation
5 Reporting.

Here, it can be added that besides describing the assets to be protected, special attention to their elements, which are most vulnerable to the considered hazard, should be paid. For instance, this means that when we are talking about the protection of peoples' lives, we should distinguish between groups which are more vulnerable than others. In this case, a situation from a "hazard point of view" for children, elderly people and people with disabilities should be considered. Another typical example would be the description of critical infrastructure or a vital one for societal processes. Of course, this overlaps with Element 6 but without a description of the most vulnerable elements of protected assets, it would be far away from their correct characterization and could create some difficulties in the next steps.

The "description" and "activities" together can be named "Context" similar to the one in the risk assessment procedure.

EU "Guidelines: Having the "context" in mind, and looking for the answers to questions on civil protection and disaster management such as: "Do we have the capability needed to deal with the risk we are currently facing?", according to the guidelines for assessment ofrisk management capability, the questionnaire on national risk and capability assessment should be filled out.

Element 2

Determining "General event" is a key point in the entire procedure. First of all, it should be "representative" for all significant events. One the one hand, the event should be hazardous enough. On the other hand, it should not be unrealistically hazardous. Therefore the term "credible event" is introduced. In risk assessment methodology, there is the term "ALARP risk limit" (risk should be "As Low As Reasonably Practicable" to be taken into account). Therefore, it seems reasonable in connection to the term "credible event", to introduce the term "AHARC" which means As High As Reasonably Credible, describing a worst case scenario event. Limits of "ALARP" and "AHARC" determine a framework of risk management.

It could be interesting to find or at least estimate these limits quantitatively or qualitatively on a BSR scale.

However, before selecting an "AHARC" event, one needs to identify all possible hazards threatening protected assets. This step is called "hazard identification". Creating a catalogue of all possible hazards seems to be very useful. In such a catalogue, there could be, not only all kinds of identified hazards, but also their resources indicated, as well as, categories of subjects affected (people, property, another values, and so forth). The catalogue could also include bodies responsible for the protection against a given hazard and those responsible for rehabilitation.

It seems to be very useful to create such a catalogue for common hazards in the BSR.

Simultaneously, for "hazard identification", it is worth to analyze vital processes which can be affected by the given identified hazard and include the results of the analysis into the hazards catalogue. It is necessary, besides the "general event", to consider secondary effects of this event. The last ones are strictly related to the influence on functioning of the aforementioned processes.

The creation of the catalogue seems to be a challenge worth to consider.

GENERAL EVENT

1 Define the general event

2 Identify factors that can lead to the event ocurring

3 Discuss the likelihood of the general event

4 Identify overall ability to prevent and respond to the general event

THE SCENARIO

1 Determine "worst credible scenario"

2 Determine the start and the end time

3 Choose variables and variable values

4 Summarize the scenario narrative

INFLUENCE ON VITAL SOCIETAL FUNCTIONS

1 Identify how vital societal functions become involved in responding to the scenario

2 Identify how the maintenance of essential services is affected

Element 3

Element 4

Although these two elements are shown on the scheme separately, there is a strong link between them since, in reality, the step "influence on vital societal functions" together with its two activities belongs to one of the categories of the "consequences" analysis. However, special attention needs to be paid to such kind of consequences resulting from its vital meaning. Critical infrastructure (IC) belongs to this category). In some cases, it is difficult to estimate the consequences of some IC element malfunctioning, especially the secondary effects when a cascading effect occurs. Analysis of IC malfunctioning is important and an unsolved problem until today.

The Scenario: The scenario step includes four activities. It is obvious that the AHARC event scenario description should be taken into consideration calling it "worst scenario" or better "worst credible scenario". That is the scenario on AHARC limit with worst consequences. The problem is whether the "worst credible scenario" should be considered after all. On the one hand, it allows to check if emergency preparedness is good enough (it cannot be worse). On the other hand, such "big" but still credible events and their following consequences (as described in "worst scenarios") are very rare. The financial issue emerges here. Is it economically justified to be prepared for an event which might never happen and, for instance, to store special equipment which might remain for many years rather useless? Maybe it is better to elaborate a "standardized middle size event" with so called "dimensioned consequences" while still having in mind (and to plan) a worst case scenario. This issue should be reflected beforehand. The next but smaller problem is, that although "triggers" of the critical event are relatively easy to determine, the end of the critical event is more ambiguous. The end is often defined by the moment when the sudden emergency situation subsides which is not very clear because, thinking for instance of a hurricane: the wind has stopped blowing but the emergency situation still continues. Maybe it would be more clear-cut if the defined end of the event would be the situation when the event has stopped "producing" its consequences?

Element 5

CONSEQUENCES

The Element 5 besides four activities consists of a pair of inseparable steps, namely: likelihood and Element 5 consequences. In those cases only events and their scenario are considered and taken into account as well as a hidden assumption is made. It is assumed that events had happened and their probability equals 1. In other words, the discussion concerns a special kind of risk, the "conditional risk". In actual fact, there is a search for the answer to the question "what if something happens?" In short, the BSR procedure is a "what if- analysis" in certain parts of its procedure. Therefore, in many cases of the procedure use, the likelihood of an event occurrence is not so important. As it was mentioned before, Element 4 in fact describes a certain category of consequences. Element 3 and Element 4 are the last steps which should be mainstreamed in risk analysis. The next steps of the procedure are related to capability risk management assessment only.

1 Assess the consequences for society's protection values

2 Make a sensitivity analysis

3 Make an uncertainty analysis

Element 6

VULNERABILITIES AND CAPABILITIES

Capabilities based on emergencies and exercises: Until this step, the BSR Procedure was rather theoretical according to experts; this step though is of more experimental character. In many cases, this step examines many theoretical assumptions which are taken into account by experts during proceeding. Thus, Task D and Task C of the Gaps to Caps project have stopped to be purely theoretical. The focal point of both tasks is the step "vulnerabilities and capabilities" with its five activities in Element 6. It should be kept in mind that Element 6 overlaps with Element 1 when describing the vulnerability of protected subjects. Thus, both theoretical and experimental factors are confronted with capability to overcome threats in five dimensions: leadership, cooperation, communication, resources, and knowledge.

To get a possibility to use the described capabilities, it would be convenient to introduce their measure.

First case - if successful (this means that after activating first responders and after ending an event its consequences are at the acceptable level the last one is a challenge worth to be considered) there are obviously no gaps at all. Success related to protected subjects resilience is 100% and our security system has 100% of effectiveness (0% of gaps).

1 Assess whether the goals can be reached and the protection values and functions can be maintained

2 Assess capability to prevent

3 Assess vulnerabilities

4 Assess capability to respond

5 Assess which vulnerabilities need to be reduced and which capabilities need to be developed

Second case - if the general event happens and our response totally fails, this means that there is a "huge" gap causing a disastrous situation. Success related to protected subjects resilience is 0% and effectiveness of our security system equals to 0% (100% of gaps). Thus it becomes possible to measure the gaps' volume from 0% to 100%.

The question is: "when can it be said that 100% of success or 0% of success or another number included in this interval is achieved?"

A very rough answer is that for some parameters of security, it can be measurable. For instance, if the operational time of the arrival on a scene after alert is 15 min. and it takes place for all alarms, then there are no gaps at all (100% of success). But if only 75% calls are served according to this standard, then the gap equals to 25% (e.g. in Poland, according to the governmental strategy, the value of this parameter is to be raised to 80% by 2020). Another example is the lack of equipment in some cases. If in 5 calls out of 100 happen that there is lack of proper equipment to cope with a dramatic event, this means that our gap is 5% (effectiveness equals to 95%). In many cases (unfortunately in most of them) it is impossible to calculate or to have experience data relating to success or failure of the security system. Then again, expert opinions and methods can help to estimate the effectiveness of the security system.

A discussion about gaps measures is the fundamental question for comparing resilience in different countries in the BSR. Besides this, a total regional resilience could be assessed.

Having the risk assessed and the gaps measured (effectiveness of the security system), a Resilience Matrix (RM) can be constructed (fig. 4). This matrix can be constructed for a prioritized dimension or after averaging with certain weight sizes of gaps for each dimension (see also Codi Matrix (fig.3).

It seems that the last discussed issue could be the subject of future work or projects, although it is quite challenging.

The described tool is very useful but it is born in mind that this tool is rather useful for authorities, services and other organizations which have competencies to prevent events, to cope with disaster or to restore lost values after an event. But what about the population, who needs to be protected ? Should they be only passive witnesses or somehow active

participation at each phase of crisis management which includes risk management capability assessment?

Some tragic situations are unavoidable, for instance, terrorist attacks. How should the bodies responsible for security communicate with the population about their behaviour before and during the attack? How can the tragic consequences of such events be mitigated?

Another issue which should be taken into account in the future, is the population's perception of risks (threats). It seems to be obvious that the perception of threats influences the population's behaviour (this issue is directly connected to security culture). The population's behaviour, in turn, influences the security system effectiveness.

The fundamental question here is: "How to involve the population to mitigate consequences of unavoidable events?"

FLAGSHIP

COUNCIL OF THE BALTIC SEA STATES

SECURE

Co-financed by the EU Civil Protection Financial Instrument

HÁSKÓLI ÍSLANDS