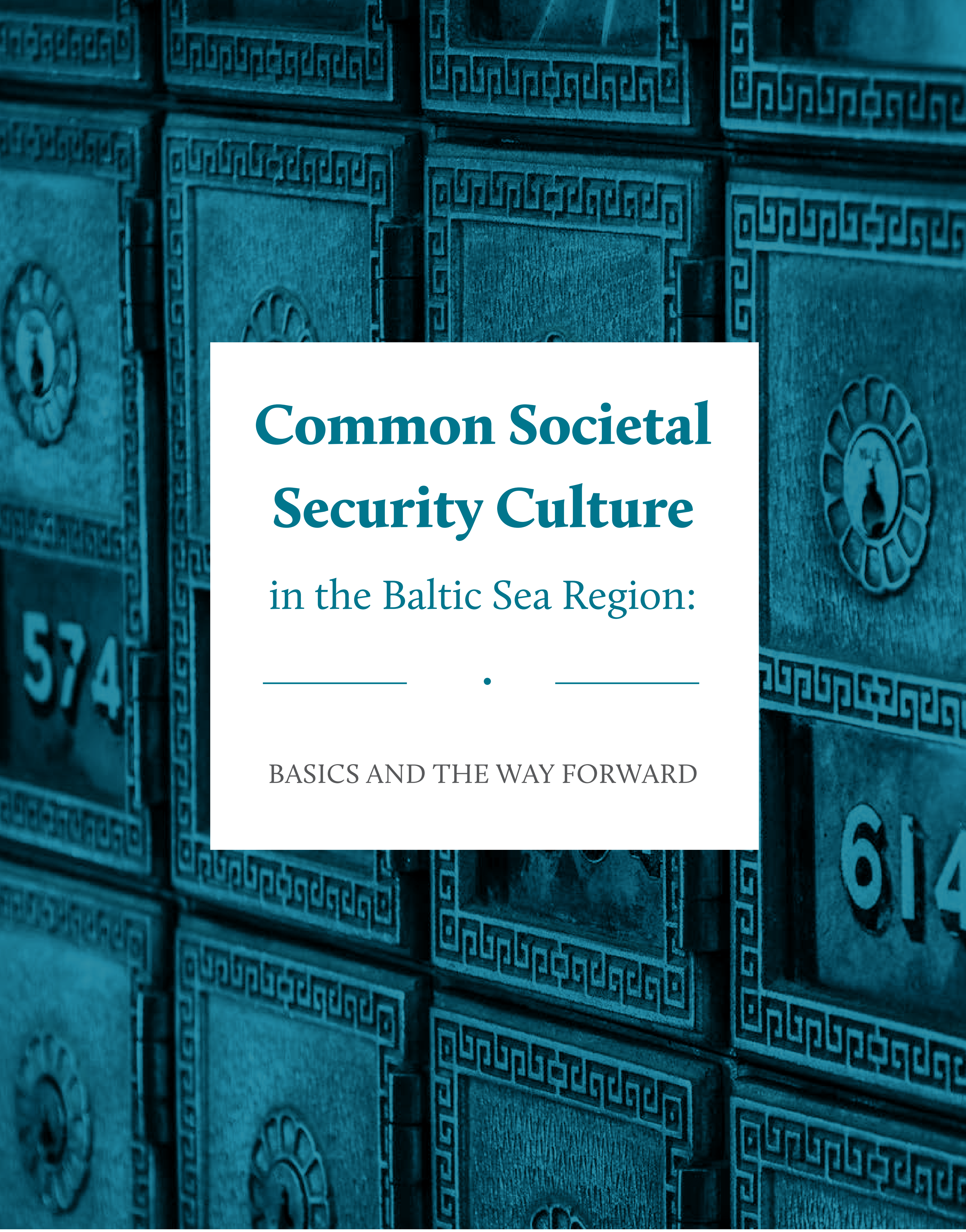


Common Societal Security Culture

in the Baltic Sea Region:

BASICS AND THE WAY FORWARD

SECURE

EUSBSR
EU STRATEGY
FOR THE BALTIC
SEA REGION

Interreg
Baltic Sea Region

EUROPEAN UNION

EUROPEAN
REGIONAL
DEVELOPMENT
FUND

CONTRIBUTORS

AUTHOR:
Professor Jerzy Wolanin, Main School of Fire Service, Warsaw

CONTRIBUTIONS/EDITING:

Civil Security/Policy Area Secure team,
Council of the Baltic Sea States (CBSS) Secretariat:
Janusz Gąciarz, Senior Adviser for Civil Security
Jacek Paszkowski, PA Secure Adviser
Andriy Martynenko, Project Officer
Nina Jernberg, Project Assistant Civil Security

Published by: Council of the Baltic Sea States Secretariat
Layout and design: Mill Studio
Photo credits: www.unsplash.com

Website: Policy Area Secure, EU Strategy for the Baltic Sea Region (EUSBSR) www.bsr-secure.eu
Social Media: Facebook @BsrSecure, Twitter @BSRSecure

Stockholm 2017: Council of the Baltic Sea States (CBSS) Secretariat

Interreg
Baltic Sea Region
EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND

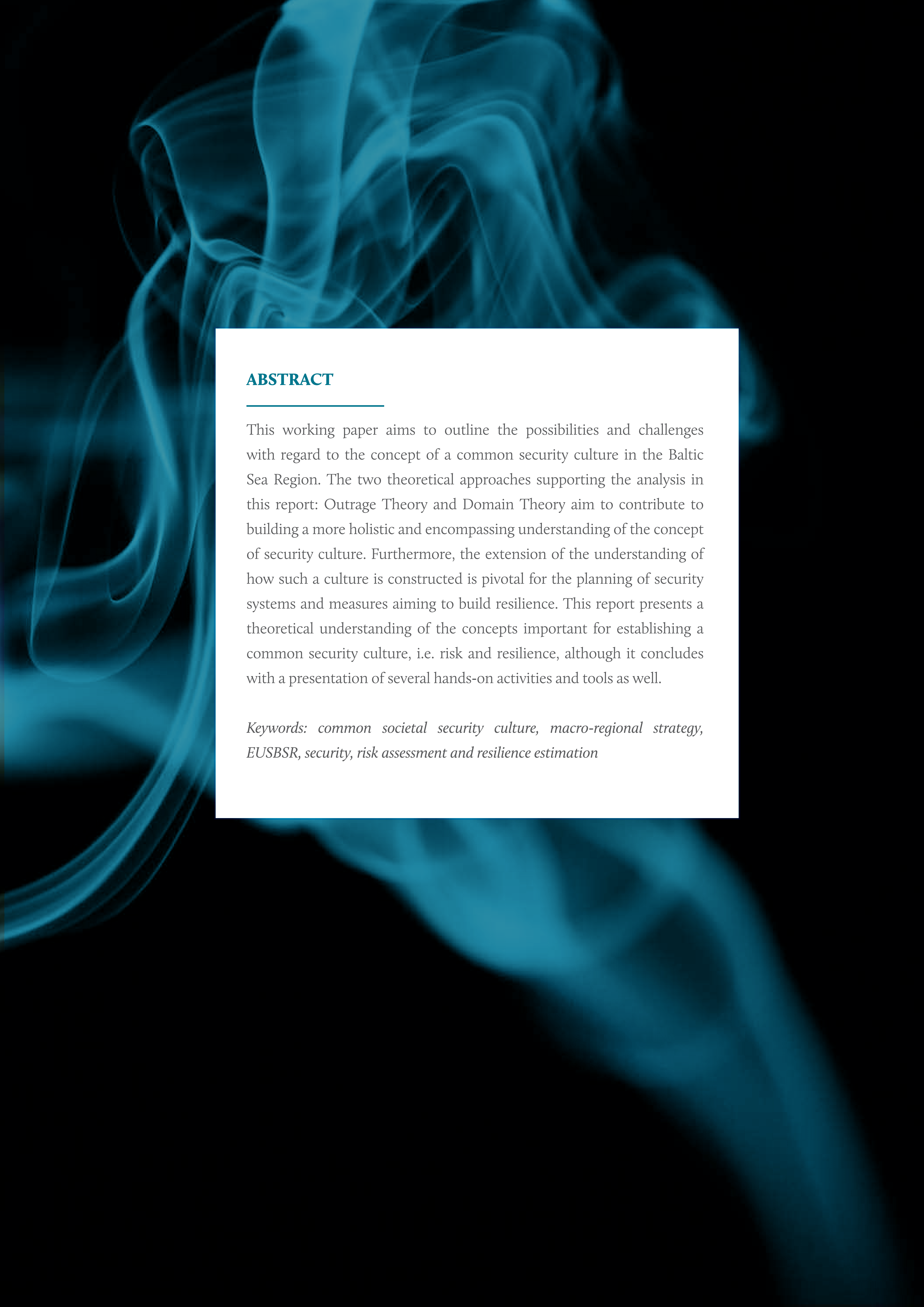
This publication has been produced by Policy Area Secure, which is funded under the European Union's European Regional Development Fund, Interreg Baltic Sea Region Programme 2014-2020. However, the content of this report does not reflect the official opinion of the European Union.

The Council of the Baltic Sea States (CBSS) Secretariat is co-coordinating Policy Area Secure in the European Union Strategy for the Baltic Sea Region (EUSBSR) together with the Swedish Civil Contingencies Agency (MSB). However, the content of this report does not reflect the official opinion of the Council of the Baltic Sea States (CBSS) Secretariat, or the Swedish Civil Contingencies Agency (MSB). Responsibility for the information and views expressed therein lies entirely with the author, and/or the contributors.

EDITORIAL NOTE

This paper was commissioned by Policy Area Secure (PA Secure) within the EU Strategy for the Baltic Sea Region (EUSBSR), and authored by Professor Jerzy Wolanin from Main School of Fire Service, Warsaw, with contributions and editing provided by the PA Secure Team at the Council of the Baltic Sea States (CBSS) Secretariat.

The paper presents a comprehensive set of recommendations regarding the implementation of a common societal security paradigm, and a 'common security culture', as a base for facilitating collaboration on civil security issues in the Baltic Sea Region. The report constitutes a theoretical foundation, and a background for understanding of the recommended actions within PA Secure. However, this theoretical undertaking is interlinked with another process within PA Secure; the formulation of a 'Joint Position on Enhancing Cooperation in Civil Protection Area', adopted by the 15th meeting of Directors General in Civil Protection in the Baltic Sea Region, and its annex: the Action Plan suggesting concrete areas for enhanced cooperation – these documents should be understood as complementary to each other.



ABSTRACT

This working paper aims to outline the possibilities and challenges with regard to the concept of a common security culture in the Baltic Sea Region. The two theoretical approaches supporting the analysis in this report: Outrage Theory and Domain Theory aim to contribute to building a more holistic and encompassing understanding of the concept of security culture. Furthermore, the extension of the understanding of how such a culture is constructed is pivotal for the planning of security systems and measures aiming to build resilience. This report presents a theoretical understanding of the concepts important for establishing a common security culture, i.e. risk and resilience, although it concludes with a presentation of several hands-on activities and tools as well.

Keywords: common societal security culture, macro-regional strategy, EUSBSR, security, risk assessment and resilience estimation

TABLE OF CONTENTS

Introduction

1. AIM OF THE REPORT

This report aims to present a theoretical basis of civil protection issues, along with models for the estimation of vulnerability and resilience. The aim is that this theoretical ground will enable policy makers, practitioners, and stakeholders, active in the field of civil protection, to grasp the complexity of these issues, and at the same time make them easier to understand. This report is part of the output of the project entitled Enhanced Cooperation in EUSBSR Policy Area Secure: Identifying and evaluating the options, and aims to supplement the clear recommendations for actions put forward in the *Action Plan on Enhancing the Cooperation in the EUSBSR Policy Area Secure* (Annex I to the Joint Position on Enhancing Cooperation in Civil Protection Area), with a sound theoretical dimension.

2. OUTLINE OF THE PAPER

This report consists of five sections. The first section discusses the aims of the report and the operationalization of the concepts used, as well as providing background information concerning the context the report addresses. The next section presents the theoretical aspect, which involves two main perspectives, Outrage Theory and Domain Theory. The section explains how the notion of security can be understood through the lens of risk perception from different perspectives, as well as security systems and decision-making processes in different domains. The theoretical discussion is followed by a number of charts summarizing the indicators of risk perception and resilience. These tables are built upon the theories presented earlier. The section ends with an outline of a model for estimating resilience, followed by a brief discussion. The fifth section presents potential activities related to the different phases of the cycle of civil protection: prevention, preparedness, response and recovery. The concluding remarks summarize the significance of the report and discuss its prospective utility in the future.

3. SOURCE OF THE ISSUES UNDER DISCUSSION

The current paper stems from the need to develop a conceptual framework that can guide various efforts aimed at responding to political willingness to cooperate in establishing high standards of safety and security in the Baltic Sea Region, and the willingness to build a macro-regional mechanism to strengthen the capacities to respond to major emergencies, as well as setting a professional milieu enabling efficient communication between relevant agencies.

There is a multitude of socio-cultural backgrounds and institutional structures in the BSR countries which constitute a diversified environment for handling safety and security issues. The historical, political and cultural differences between countries in the BSR generate a variety of social attitudes towards safety and security issues; this along with diverse institutional arrangements in the countries can pose challenges to cooperation. Therefore, there is a need to find a standard for the crucial elements of safety and security systems, to enable greater coherence and compliant approaches across the region. The search for improvement by finding a common denominator for the various existing approaches and institutional structures – and a common security culture provide a foundation for such a practice. The concept of a common security culture can thereby act as an overall framework for introducing workable solutions for various challenges in the safety and security sector.

How civil protection is understood and organized change over time and it is influenced by the historical legacy and contemporary events. This is also the case with concepts such as security and safety. The operationalization of these is highly dependent upon the political level, and it is certainly not a task solely for research and the academia. Therefore, any discussion of security would be incomplete without a reference to politics.

In contemporary Europe, security means something completely different than it did in the direct aftermath of WWII, and during the era of the Cold War. Since the inception of the Cohesion Policy and the integration in the European Union, the discourse has changed fundamentally in the European setting. The EU Strategy for the Baltic Sea Region (EUSBSR), a macro-regional strategy aiming to increase regional integration, has changed the security agenda in Northern Europe, and cooperation between relevant organizations, networks, and actors has increased in the region since the Strategy was launched in 2009. Within the EUSBSR, Policy Area (PA) Secure aims to establish a comprehensive framework for cooperation built on the societal security paradigm and aims to build common capacities and capabilities for societal security. The question is, however, whether this intensification of partnership and newly established networks are based on a solid ground, whether this process is not only founded on cooperation between governmental agencies or professionals mandated to handle security issues within public administrations, but embedded in the core societal structures, in cultures as a driving force for people's everyday behavior. In other words, this question can be formulated as follows: do the populations of the Baltic Sea Region exhibit a common emotional attitude towards specific regional threats and/or hazards?

The macro-regional concept is founded upon the notion that neighboring countries have common challenges defined by the specific geographical context, and actors and stakeholders can address those challenges more efficiently through cooperation[1]. This is no doubt the

[1] European Commission, 2014. Macro-regional strategies, retrieved 2016-11-10, from: www.ec.europa.eu/regional_policy/en/policy/cooperation/macro-regional-strategies/

case of the environmental dimension of the Baltic Sea: since decreasing the eutrophication of the Baltic Sea or reducing GHG or pollution in the area cannot be a commitment on the part of a single actor if results are to be achieved. However, the question this paper aims to answer is whether there is a basis for a common security culture in the Baltic Sea Region, which requires cooperation for increased effectiveness of security and prevention measures, or if such a culture could possibly be established to advance future collaboration, particularly as part of Policy Area Secure within the EUSBSR.

Not only does the conceptualization of civil security, safety and protection change over time along with the structures of political and operational collaboration regarding those issues, but also the definition and perception of threats evolve, as well as the analysis of global and regional conditions. It is important to be aware of these changes, and the current state of play of the conceptualizations, perceptions and analyses. The definitions of security, safety and protection are highly dependent on the definitions of risk and threat. Currently, the growing frequency of terrorism in the world, shows that these kinds of threats have become a highly relevant issue to consider from the point of view of civil protection in the nearest future, and this shows that a 'new' more complex security context in contemporary Europe – and in the Baltic Sea Region – along with 'new' threats, has arisen.

4. KEY CONCEPTS

4.1 CONCEPTUALIZATION OF SECURITY AND RISK

Security is a complex process, involving cultural, social, economic, organizational and technical activities the function of which is to ensure the degree of resistance and protection against damage of various types of values, assets and social actors (individuals, communities, organizations and institutions) that make up a specific community. Security is a process mediating between assets that have to be protected, i.e. individuals, various levels of social organization as well as elements of infrastructure. The security process is an instrument to avoid or reduce risks, and ultimately reduce the scale of damage and losses incurred. This process is twofold in its essence. It has a negative aspect, which amounts to defending against all possible dangers, regardless of whether they are of physical, virtual or psychological in character. It has also a positive side, which concerns cooperation in order to prepare for different types of hazards, construct technical systems which enable effective protection, perform social interactions and establish social and organizational relationships which enhance resilience. This complex character of the security process makes it possible to define it in a variety of manners, using different perspectives and emphasizing its various aspects. Since the purpose of this paper is to outline the basis for a common security culture, it is rational to choose the simplest possible denomination of the term *security*, and to focus on the aspects of the phenomenon that are relatively less exposed to the influence of peculiar features of the local cultural, social, political and economic background.

In this report, the term security is defined as a state of affairs or/and a set of permanent processes which occur within a natural environment or/ and are conducted within civilizational spaces that are characterized by risk. From this point of view, risk has become a fundamental concept in the theory of security. The value of risk (expressed quantitatively or qualitatively) is a parameter that fully characterises security, since security and risk are two sides of the same coin. In this sense, risk can be considered as a measure of security. In other words, being aware of the value of risk means to know "all" about security.

In the handbook "Being Secure in the Baltic Sea Region" [2], civil protection capabilities are analyzed in relation to "all main hazards". Scenarios have been developed in order to draw attention to them, in the respective identified and prioritized areas. The advantage of applying the term 'risk' to security in the context of civil protection stems from the fact that it is risk that is commonly understood as characterizing the identified areas where the community needs to tackle threats and emergencies. In this report, risk means, roughly speaking, the likelihood of occurrence of unwanted harmful events. In more general terms, risk is the possibility of an event causing negative consequences, whether of material, organizational, psychological or symbolic nature. The essential trait of such an event is that it disrupts the normal functioning of the community, or a specific part of that community. This means that to describe risk, it is enough to determine the likelihood of occurrence of unwanted events.

Risk is not an absolute and fully objective measure; rather it is related to the properties of objects exposed to threats, including their vulnerability, susceptibility and resilience. Furthermore, there is another important dimension hidden in this definition: a psychological one, which is strictly related to risk perception. The subjective (e.g. cognitive and emotional) dimension of risk becomes one of the most important aspects of security when it comes to preparedness and response to emergencies. In the end, it is people who are the ones reacting to danger, taking action to save their own and others' lives and health, to mitigate damage, to resolve the situation, and to restore the normal state of affairs. Therefore, their perceptions of the situation, understanding of what is happening and attitude towards everything they are confronted with is of utmost importance for security and for a community's capability to tackle hazards. The emotional content of risk perception has multiple implications for security. First of all, it may determine motivation to engage in preventive activities. However, far more importantly, risk perception influences the behavior of potential victims during an actual occurrence of a threat or disaster.

In this report the definition of risk will encompass all elements of the risk concept: perceived risk and security, i.e. the individual's or the group's

[2] Council of the Baltic Sea States (CBSS) Secretariat, 2014. Being Secure in the Baltic Sea Region. A handbook of a priority area. Lithuania: KOPA.

subjective experience, as well as real risk and security. Both the subjective and the objective aspects are important in terms of ensuring effective operation of civil protection systems, with the establishment of safe and secure society, as its consequence. In this perspective, risk becomes a fundamental concept in building a common security culture, because identifying, assessing and attributing every possible threat are steps towards determining the entire structure of security management, at all levels of governance.

4.2 SECURITY AS A PROCESS AND DOMAINS OF SECURITY

An important aspect of the definition of security is that it is a process, and to make the analysis clearer we can assume that this process is structured in the same way as the cycle of civil protection. This means that it consists of the following phases: prevention, preparedness, response and recovery. In an effort to strengthen societal security, different activities are demanded in each of the civil protection phases, and a multitude of actors needs to be involved and undertake the measures needed. Each phase of constructing security measures provides the actors involved with a specific demand to assess the level of security achieved so far. When we have an assessment of the level of security at our disposal, there is a possibility to make an estimation of resilience. When risk is assessed, it needs to be calculated in each of the phases and the resulting values should then be summed up. It is important to note that each phase includes several actors – both societal services and the public's responses.

Security as a process can be interpreted as a sequence of specific activities related to risk: identifying risks and threats, risk avoidance, risk reduction, risk management and ensuring the normal functioning of the community.

In addition to analyzing security as a process, it is equally important to recognize that security is a multilevel phenomenon. This dimension of security is reflected in the notion of different domains of security: individual, micro-societal, local (municipalities and counties), regional, national, macro- regional and global. By referring to different domains of security, the idea is to highlight that at every level of social organization (from individual actor to the global level), security has its specific traits: the range of risks and threats, patterns of perceiving and attributing meanings to various aspects of a security situation, the spectrum of actions undertaken in response to the identified emergencies. Domain is a term related to social organization, i.e. its actual scope and structure depend on the way a given community is internally structured (e.g. regarding territorial organizations, legally recognized societal entities etc.). A given domain of security comprises such actions on the part of an individual or a collective which may expose individuals, groups, property or infrastructure to threats, or, conversely, protect them against possible danger.

The important questions relating to security as a process and to security domains can be formulated as follows:

1. What activities related to prevention, preparedness, response and recovery/preventive intervention should be initiated within each security domain?
2. How is it possible to reach each and every relevant actor within each domain in order to make sure the security process is most effective?
3. What are the criteria for risk acceptance in each domain?
4. How can we measure risk in each domain, and how is risk perceived?

Security as a process and security domains will be further elaborated in the theoretical section (2.).

Security considerations have changed over time in relation to these different domains. These differences in perspective have implications for the implementation of prevention and security measures. Contemporary thinking refers primarily to the protection of human beings (individuals), reflecting the dominating system of values, in which the well-being and integrity of the individual are principal values. In the past, particularly during the Cold War, policy makers were considering protection of groups as a primary objective, with emphasis on protection of civilian populations against a nuclear attack or use of other weapons of mass destruction. In 1980s and after the end of the Cold War, the focus shifted to protection against disasters, mainly natural. But since the Chernobyl accident, increasing attention has been paid to man-made (technological) disasters. Today, due to the growing number and scale of terrorist attacks, security challenges are shifting again, and are much more frequently related to intentional acts than to accidental events. This evolution of approach towards security makes the notion of disaster one of the key issues in constructing a system capable of providing both individuals and societies, as complex organizations, with a sufficient level of resilience and capacity to maintain their vital functions.

Theoretical framework

This section will present two different – albeit connected – theoretical approaches toward risk and security. The first approach is Outrage Theory, which contributes to the understanding of the complexity of risk perception, and of why the public and the experts who plan security systems perceive risks differently. The second approach is Domain Theory, aiming to contribute to the understanding of decision-making processes in different domains, including the impact exerted by potential external influence. In a conclusion to this section, the theoretical dots will be connected and an outline will be presented of how the theories can support the construction of a common security culture. Let us, however, begin by highlighting the social aspect of disaster.

5. DISASTER AS A SOCIAL PHENOMENON

The last twenty-five years have been characterized by a dynamic growth of disaster studies, and a profound change in how the concept is understood. New challenges have emerged, namely climate change, globalization and increasing migration, which have imposed a redefinition of the term 'disaster', making it much broader in scope than the classic definition whereby the phenomenon is characterized as sudden, rapid, impetuous and destructive on a massive scale, but relatively short-lasting and limited in terms of territorial range.[3] The new aspects of disasters contemporary societies suffer from are: their much longer formation and duration, the persistence of their effects, as well as multistage mediation between the causes and the disruptive effects conditioned by social, political and economic factors.

According to D. E. Alexander, these new aspects of disasters which need to be considered are connected with four factors: the relationship between *capital and labor* and its impact on disaster risk management, *corruption and human rights issues* (e.g. insecure infrastructure as a consequence of breaking the rules of constructing codes and technical norms; limited access to the information allowing to prepare for a disaster), migration caused by poverty and deprivation of means to satisfy the needs (whether it is caused by global economic competition and exploitation, or warfare, or irreversible effects of climate change), the impact of welfare on social attitudes towards responsibility for catering for one's own security (externalization of responsibility to the state and/or other public institutions; lack of self-reliance).

All these processes have a deep and complex influence on security. Corruption leads to the rise of distrust to public institutions and their ability to guarantee equal security to every member of society. The same effect is caused by violating fundamental human rights because it brings about an unjust differentiation between individuals and social groups regarding access

[3] David E. Alexander, 2016. The game changes: "Disaster Prevention and Management" after a quarter of a century. *Journal of Disaster Prevention and Management*, 25(1), pp. 2-10.

to proper security systems. For example, global economic competition stimulates the movement of capital, which changes profoundly industrial relationships across regions. As a consequence, the mobility of the labor force is increasing, and some societies are endangered by depopulation, while others are exposed to a large influx of migrants. The last process contributes to multiculturalism in modern societies. In relation to this, disaster risk management should take the cultural aspects of crisis management into consideration as well. The new challenge is characterized by differences in risk perception among migrants and their reaction in case of a disastrous event in their new home environment, or while they are on the move. Another factor causing differentiation of risk perception and reaction to threats is a divergence of social attitudes among social groups due to their diverse socio-economic status, and in particular to varying degrees of their dependence on welfare state redistribution mechanisms.

To sum up these considerations, risk perception is a socially and culturally differentiated phenomenon and as such it determines the social construction of disaster: the understanding of its essential traits and measures necessary to respond to its occurrence. In the contemporary world the key causes of disasters are: environmental change (mainly climate change), an increase of population associated with displacement and migration (facilitating inter alia pandemics and epidemics), social and political conflicts followed by warfare and terrorism. Some of the mentioned processes are interlinked, e.g. climate change that causes long-lasting droughts and desertification reinforce emigration from the suffering regions, and increasing migration flows to Europe, which may aggravate otherwise moderate and managable risks and threats. The impact of cultural factors makes perception of risks and disasters of social, economic and political background much more complicated and challenging in terms of developing an effective response as well as adapting individuals, communities and entire societies to their impact. These processes are affected by culturally embedded patterns of interpretation, i.e. attributing meaning and sense to a given situation, as well as socially and psychologically grounded emotional reactions, which set motivation for choosing specific behaviors and denying the others.

6. OUTRAGE THEORY

6.1 THE 'NEW' DIMENSION OF RISK

The classic definition of risk says that it is the likelihood of occurrence of unwanted events (i.e. hazards). Since subjective reactions to hazards have been recognized as a significant factor determining the response to threats and incidents, there is a need to add another dimension for a complete understanding of risk, namely outrage. Outrage is connected with risk perception. This dimension enhances the understanding of risk and risk perception, and the relationship between the 'real' threat, the actual occurrence of a damaging scenario, and the objects subjected to it. For example, the most lethal risks are not necessarily the ones frightening or angering people the most[4]. These subjective and emotional elements exert real influence on risk and are equally significant as independent factors determining individual and collective behaviors in the event of an emergency. P. M. Sandman highlights that societies often perceive risks in an incorrect way, since emphasis is put on the parts of risks that have the most significant emotional impact, at the same time as experts frequently perceive social unrest incorrectly, since they disregard it as irrational. In essence, communities pay too little attention to the classic risk element, i.e. *hazards*, while experts pay insufficient attention to the perception of risk by the public, i.e. *outrage*. The distinction between the two aspects of risk lies in the differences of definitions. "*To experts in risk assessment, risk is a multiplication of two factors: magnitude (how bad is it when it happens) times probability (how likely is it to happen). You take your best measure of magnitude and your best measure of probability, you multiply them by each other, and you come out with something like expected annual mortality*".[5] Risk can also be defined by other quantifiable indicators, like the volume of material losses.

From the point of view of the public there are several additional dimensions to the definition of risk. P. M. Sandman identified over 20 "outrage factors", and the most important ones include:

- **Voluntariness** - a voluntary risk is much more acceptable to people than a coerced risk, because it generates no outrage
- **Control** - almost everybody feels safer when prevention and mitigation are in their own hands, and consequently risk is perceived as much lower than when they are in the hands of a government agency
- **Fairness** - differences in exposure to a great risk which are unjust and do not have objective rationale imply greater outrage amongst people who must endure such greater risks than their neighbors
- **Process** - the perception of and the emotional response to a specific situation depends very much on past experiences related to the agency responsible for tackling the problem. Do people encounter trustworthiness or dishonesty, concern or arrogance? Were they consulted before the real decisions were made? Were their opinions been taken into account or ignored?
- **Morality** - the moral qualification of a specific threat has significant influence on the strength of the reaction to it, and in particular on recognizing some hazards as "acceptable risks"
- **Familiarity** - familiar risks provoke less emotional response than those which are unknown, and have never been experienced before
- **Memorability** - memorable accidents make the risk easier to imagine, thus "riskier". The Chernobyl accident exerts a dramatic impact on the way the public reacts to any information about technical failures in nuclear power plants

[4] Sandman, Peter M., 1988. Risk Communication: Facing Public Outrage. Management Communication Quarterly, 2(2), pp. 235-238.

[5] Sandman, Peter M., 1993. Responding to Community Outrage: Strategies for effective Risk Communication. Falls Church: American Industrial Hygiene Association (AIHA) Press, p. 6.

- **Dread** - for example, fast-acting diseases are more dreaded than others
- **Diffusion** in time and space - the more diffuse the specific threat is, and the less losses are caused by a single incident, the more probable that such a threat will be assessed as “acceptable”.[6]

These factors are intrinsic to risk perception and co-determine what is recognized as unwanted events by people. In order to be able to understand the concept of risk holistically, one needs to grasp both these components. Risk can, therefore, be understood as follows:

Risk = Hazard + Outrage[7]

or **risk is a function of hazard and outrage:**

$$R = f(H, O)$$[8]

The perception of risk is associated with cultural factors in many ways, but the most important is to understand that cultural patterns set the framework in which information (events, facts, data) is interpreted and an emotional content is assigned to it. Thus, in order to ensure that the response to threats is coherent and predictable across the entire society, a common security culture is needed. Its essential parts include common patterns of risk perception and rules of making decisions on implementing security measures. In the Baltic Sea Region, due to the differences between the countries, establishing such a culture is a challenge, but there are sufficient similarities in terms of political, economic and social structures which can facilitate this process.

The crucial role in the process of constructing a security culture, and in particular in spreading and unifying risk perception is played by communication, namely risk communication. In relation to this type of communication, there are several important aspects which need to be considered in order to ensure effective cooperation between various actors in agreeing on the common understanding of risks and similarity of attitudes toward the notions of prevention, preparedness, and response.

The strategic importance belongs to the tripartite multi-dimensional risk communication between:

1. Experts and society;
2. Experts and decision-makers;
3. Decision-makers and society.

[6] Sandman, Peter M., 1987. Risk Communication: Facing Public Outrage. EPA Journal (U.S. Environmental Protection Agency), November 1987, pp. 21–22.

[7] Ibid.

[8] Sandman, Peter M., 1988. Risk Communication: Facing Public Outrage. Management Communication Quarterly, 2(2), pp. 235-238.

6.2 RISK COMMUNICATION

To communicate risks is not an easy matter, because a majority of hazards cannot be calculated and expressed in a simple manner. Therefore, usually the expression *risk assessment* is used and this means that the content of communication is disputable and its reception depends on the sender's credibility, links to accumulated experiences of the recipients and the context on which its interpretation depends. Since risk perception concerns different social groups, playing different roles in the society and having diversified interests (e.g. decision-makers, householders, inhabitants of cities, towns and villages, members of different organizations, members of different ethnic group, cultures and sub- cultures), this also becomes a political issue. Risk communication involves inevitably a number of public institutions: governments at all levels of social organization, professional agencies and specialized services, media, NGOs and opinion-makers. All these actors – and many others – mediate between different social groups as well as different levels of public administration in an attempt to understand risks, to adapt themselves to the possibility of risk occurrence and to construct an effective framework for cooperation in the event of an accident. There are many parties that need to be targeted by the communication of risks, and the latter should be specifically tailored for each group. The fundamental issue that needs to be explored is the question how to properly communicate risks to different groups in an area of such a diversity as for example in the Baltic Sea Region.

In order to meet the communication challenges, risk should not only be assessed by quantitative measures, as qualitative measures are also needed to complement the data in regards to the outrage variable; in other words, a holistic assessment of risk, encompassing both elements, can only be realized through the use of a *mixed methods approach*.

The *value of outrage* reflects the degree of emotional response in relation to a hazard (i.e. conventionally understood risk). Moreover, heightened emotional states can be attributed both to individuals and groups. P. M. Sandman[9] suggests that outrage is not only strong emotions, but also justified emotions. The latter qualification makes outrage the real driving force of social actions that has to be included in an analysis of emergencies, because it may change seemingly harmless risks into serious damage. In this context, it is especially important to stress that outrage is:

- as real as a hazard;
- as measurable as a hazard;
- as manageable as a hazard;
- as much a part of risk as a hazard.

Risk communication is the key to managing outrage. Therefore, all communication activities related to public awareness campaigns are of the utmost importance for establishing a security culture that facilitates resilience. Education programmes addressed to children, youth and adults

[9] Sandman, Peter M., 1993. Responding to Community Outrage: Strategies for effective Risk Communication. Falls Church: American Industrial Hygiene Association, p. 8.

are of the same importance in the long-term perspective.

It is from this theoretical perspective that the main question of this report is derived - whether the populations of the Baltic Sea Region exhibit a common emotional attitude towards specific regional threats and/or hazards. The collective emotional response influences the value of risk, and thus has an influence on security per se, which means that this is important to take into consideration while discussing issues connected to resilience.

Important recommendations for action aimed at developing a common security culture stem from Outrage Theory. The first step is to determine what are the common, widespread concerns regarding the risks which in the opinion of the inhabitants of the region represent the greatest. What are people most afraid of? When do they expect support and assistance from the public institutions? What triggers the most emotional reactions and makes people committed to counteract and cooperate? Answers to these questions would serve as a basis for outlining a frame of reference for actions contributing to establishing a unified approach to security issues in the Baltic Sea Region.

7. DOMAIN THEORY

In the analysis of the notion of security culture, the starting point is preferably each individual's role in the security system, and each individual plays a double role. On the one hand, s/he is subject to protection, and on the other hand, s/he is a significant element in the entire security system. The latter statement is related to the basic assumptions of *Domain Theory:*[10] an individual's decisions connected to personal security are of various kinds. Some of them may pose a danger, whereas others allow the individual to avoid dangerous situations. Moreover, the decision to avoid danger should be supported by an external security system.

The security system covers a wide range of different forms of social organization. It starts with primary or natural groups (i.e. family or kinship, neighborhood). In these groups, advice or psychological assistance support the security system. In the other end of the spectrum is the state security system, which is supported by the professional medical service or voluntary organizations (like for example the Red Cross). The state security system should be considered to be only a support tool for making safer decisions – red lights telling us not to cross a street for instance – whereas the final decision is taken by the individual according his/her own understanding of the situation. This constitutes the ***individual security domain*** (ISD), which has an immanent feature – a certain degree of independence is engrained. This means that external access to the individual's decision-making is limited. However, the individual domain is an integral part of the larger ***state security domain*** (SSD), one cannot take for granted that decisions taken by every individual will strictly follow the rules/patterns imposed by state regulations

[10] Wolanin Jerzy M., 2006. Domains of Safety Communications. Scientific Letters of the University of Zylina (Slovakia), 3(2006), pp. 52 – 53.

or recommendations suggested by public authorities. This domain is the area where an individual's actions may cause a threat or help avoid danger, depending solely upon the person's individual free decision-making potential. Support to make more secure decisions can, however, come in form of raising awareness through education provided by actors located at the other security domain.

Exposure to threats – or the circumvention of them – is not only connected to individual decisions, it can also be attributed to the group. An individual's closest environment, including their family, friends or neighbors, is termed the *micro-societal domain* (MSD). Security management in the MSD is in many cases similar to management in the ISD, but there are also differences.

First, the MSD includes all elements of the ISD and functions in relation to larger security domains. An example is household security, where a household has the possibility to hire an external security service. Even though the police have the responsibility for protection of individuals, such a decision can be made by members of the community. Members of the MSD have a choice either to rely on police protection or to hire additional security services. In this situation, expansion of the micro-societal domain into the local security domain or the state security domain occurs. There are, however, no clear boundaries between the domains, they can be expanded or narrowed down. The next domain level, external to both the ISD and MSD, is the *domain of local security* (DLS). In this domain, the local community has the capability to make decisions regarding threats. External to all three of the above-mentioned security domains – the ISD, the MSD, and the DLS – is the *state security domain* (SSD), where state authorities make strategic decisions regarding security policies and activities. These four domains are the most prominent ones; however, it is possible to determine a *regional security domain* (RSD) or a *global security domain* (GLD) in relation to specific issues. We will return to this issue later in the discussion.

Some general conclusions can be drawn from the theory presented above:

1. Providing security to citizens has no absolute character. Every domain has its own particularities and demands specific instruments to ensure the best possible solutions for security.
2. Depending on the type of domain, its influence varies.
3. Security is not universal or homogeneous, but rather varied and highly heterogeneous.
4. Domains differ from each other by the scale of interaction, but also by the level of autonomy from each other.
5. Subsequent domains, beginning with the individual one are more advanced and complex, which means that the calls for different tools used in security management vary.
6. Domains are a natural reflection of the nature of security, meaning that all protection measures and systems should be harmonized between domains, and the construction of security systems should be based on Domain Theory.
7. The best results are achieved by building security systems bottom-up; however, in many cases a top-down approach is necessary.
8. As a rule, however, every higher level should support the lower one(s).

The concept of security domains shows how complicated security management can be. In the context of Outrage Theory, as discussed above, it is clear that one of the most important challenges for the security systems is proper communication, adequate to the risks at stake and well adapted to the emotional background of actors who are active at every domain.

Security is a public good, which means that every individual – without exception – should have equal access to it. However, inequalities in access to security measures are an inevitable consequence of the differentiation of people's socio-economic status. There are many individuals who cannot afford to buy security services, and how this issue is solved within the public sphere has fundamental significance for the functioning of security systems at all levels. This issue will be further elaborated in the following section.

7.1 THE CONCEPT OF VULNERABILITY

The phenomenon of vulnerability exists in each domain; however, the meaning of vulnerability is not consistent across the domains. Thus, when vulnerability is characterized, it is necessary to indicate which domain is concerned.

The importance of such a point of view may be shown in a simplified example related to ISD. Whether to cross a road or not is a decision on the part of an individual no matter if a red light is on or not. The red light is there as a service offered by another security domain (i.e. DLS), guiding and supporting the individual's decision-making. However, there are two aspects related to the crossing-of-the-road situation and vulnerability. First, there is a technical dimension to paying attention; all people do not have the same capability to pay attention. Second, the lower the awareness of an accident occurrence mechanism the higher the vulnerability of any given individual. The lowest awareness level is attributed to children making them the most vulnerable. Thus, this is a group which needs special attention. In our example the technical warning equipment only facilitates making a decision independently of the individual's age. The example illustrates how the Domain Theory allows us to describe the vulnerability of a specified protected target group and to understand the role of external domain influence. Red light as a facilitating tool does not deliver one hundred percent security for an individual because her/his choice may be different. The person has to be aware of the meaning of the red light to be able to take an appropriate decision. This is important for the understanding of the mechanism of external domain influence (or lack thereof) on the individual security domain, in relation to vulnerability. In the situation when an individual is making a decision whether to cross a road or not, two types of barriers are at play: *systemic barriers* related to the red light itself and *supplementary barriers* related to the individual decision-making. These barriers can either reinforce or contradict each other. The issue of barriers will be further elaborated on in the following section.

7.2 SYSTEMIC AND SUPPLEMENTARY BARRIERS AND RESILIENCE

S*ystemic barriers* are connected with the domain of local security (DLS) or the state security domain (SSD), and the supplementary barriers to the *individual security domain* (ISD). When *systemic* and *supplementary barriers* reinforce each other, they amplify the security system and make its reliability stronger, but when they contradict each other the reliability of the security system is weakened.

Systemic barriers depend on the organization of response to a threat, which is a standard way how the security system works. An example of this type of barrier is the operational arrival time of the first rescuers in the case of an emergency. Let us assume an example where the operational time is estimated to 15 minutes, and the reliability of the system is 0.75 (75% responses are on time). But, if people are aware of the kinds of hazards that could possibly occur, and the standardised manner in which the system responds, they can be well trained on how to behave in an emergency situation, in order to secure themselves and diminish damage. Statistical data shows that such a good preparedness of people (e.g. training in first aid), which is classified as a supplementary barrier, reduces the number of victims by about 10%.

The sum of all barriers is stronger than each of them separately. The systemic and supplementary barriers are one out of two dimensions of *resilience*. The second dimension is the value of estimated risk. This means that by knowing the reliability of both kinds of barriers and the estimated risk, it is possible to assess resilience.

8. CONNECTING THE THEORETICAL DOTS

Both Outrage Theory and Domain Theory provide tools for further understanding of risk and security. This understanding is important in regard to both assessing to what extent we can assume that there is a common security culture in the Baltic Sea Region or at least some prerequisite for it, and advocating efforts leading to the establishment of such a culture or its further development. Risk in terms of hazard and outrage – risk perception – is related to the different security domains, and the decision-making processes taking place on each level. Risk perception is connected with the individual security domain, influencing the individual's decisions. At the same time decisions made by an individual are influenced by the external security system (i.e. domain). The classic definition of risk (i.e. as a hazard) is related to the state security domain, where national policies are formulated as well as implemented in the form of established security systems. The security culture is shaped by both aspects of risk, and by the structure of different domains. Furthermore, understanding the complexity of the concepts is necessary for an analysis aimed at a common security culture as a framework for cooperation. In addition to understanding how risk and security are connected, the systemic and supplementary barriers can further the understanding of obstacles embedded in the effort of building resilience. Communication is a process that binds these various elements, both in terms of information flow between different security domains, as well as in terms of mutual exchange of indicative signals between public security departments and specialized agencies and individuals, social groups and communities, all those subject to protection.

Models, Figures, and Tables

9. RISK PERCEPTION

A number of factors exert an impact on how risk is perceived. The table below aims to show various elements which constitute a cognitive map where a specific risk can be qualified as more or less threatening, more or less damaging, requiring stronger or weaker preparations. Identifying the position of a specific risk in relation to the suggested criteria makes it possible to assess whether the threat is lower or higher from the point of view of a person or a group making a decision on security settings. For example, if a risk is related to a man-made, uncontrollable, accidental and involuntary event, it is usually perceived as higher than a risk posed by a natural and immediate – albeit frequent – event.

Table 1: Selected elements having an impact on risk perception[11]

Criteria	Risk Perception	
	Perceived as lower	Perceived as higher
Source	Natural	Man-made (technological)
Voluntary character	Voluntary	Involuntary
Disclosing	Immediate	Delayed or unnoticed
Severance	Common: a few endangered persons	Disastrous: a lot of endangered persons
Limitation	Controllable	Uncontrollable
Profit	Obvious	Obscure
Familiarity with risk	Known	Unknown
Frequency	Frequent	Accidental
Necessity	Indispensable	Superfluous (luxury)

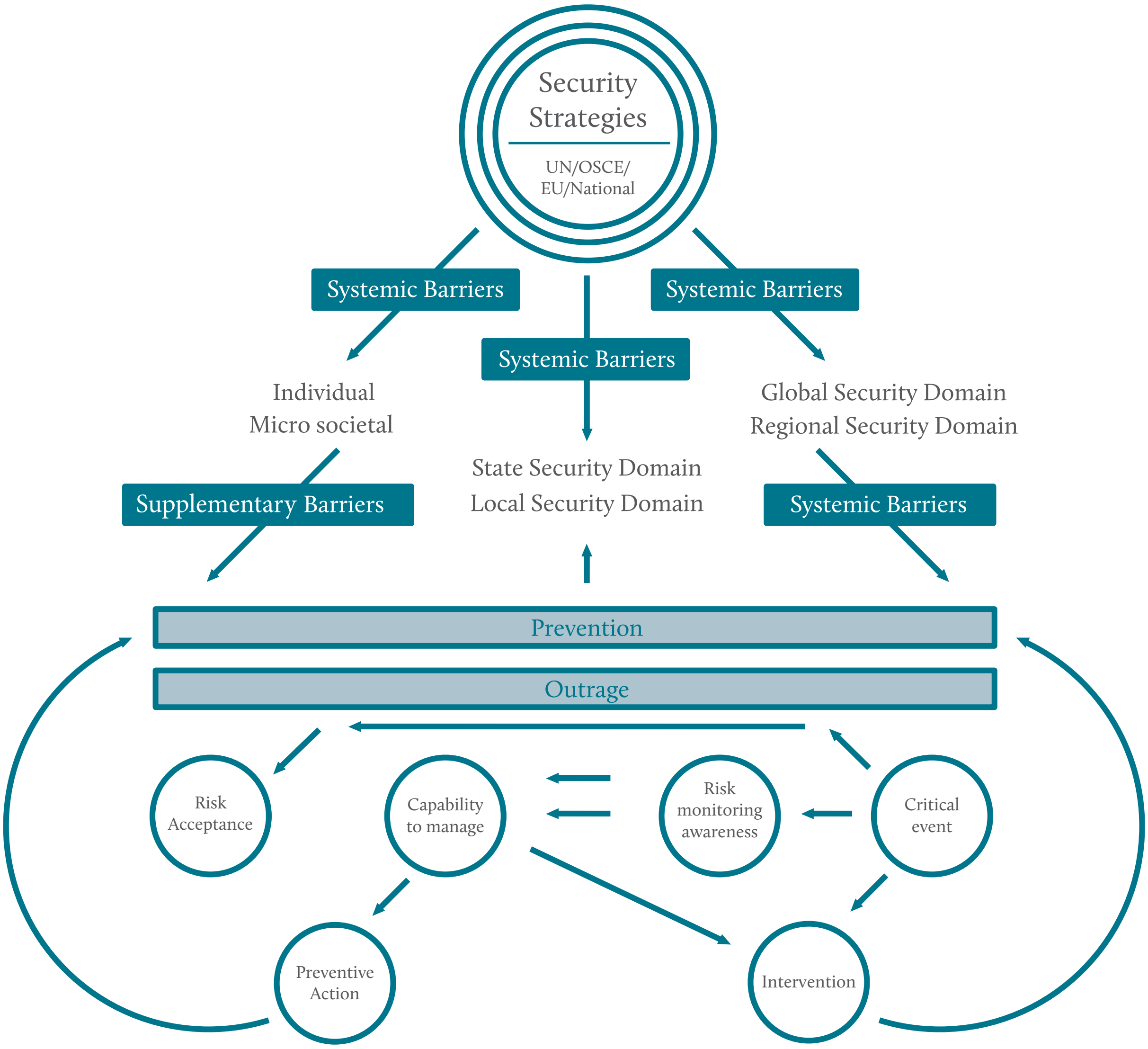
The Criteria used to compare the values related to different elements - which are necessary for assessing the risk entailed by specific events - can be converted into statistical variables. If these variables are used for statistical analysis, it is easy to create dummy variables based on these categories, which means that this is a relevant basis for data collection on certain events. These variables can be applied to risk perception analysis performed by experts and also to a description of risk perception by the public.

[11] Klein R. A., 1997. Monograph on Risk Assessment for Emergency Services. Leicester: Institution for Fire Engineers (Publications) Ltd.

10. SECURITY DOMAINS

Figure 1 illustrates in a simplified manner how security is a result of interaction between different domains and a number of factors within a specific domain. It is important to note that the structures of the processes are identical across all domains, although there are differences regarding meaning and scale. The individual security domain and the micro-societal security domain contribute to security by setting up supplementary barriers, while systemic barriers are the function of the local, state, regional and global domains. Outrage is highly relevant for risk communication, and therefore, in order to work out the most effective ways of risk communication, it is important to avoid distortions and disturbances when responding to an emergency. The structure outlined below can support the exploration of resilience since it gives a clear view of all the different aspects of the security process.

Figure 1: Security as a process: interaction between domains, barriers and crisis management cycle.



10.1 SECURITY DOMAINS AND VULNERABILITY

As described earlier in the theory section, vulnerabilities have to be taken into consideration in the planning of security systems. These vulnerabilities might have an effect on the decision-making processes, which means that external security measures can have a varying impact on different individuals' decisions. The table shows a range of vulnerabilities related to different social levels of the society, and indicates which issues need to be taken into account in relation to policy and implementation of security systems.

Table 2: Selected hazard-independent parameters and potential indicators of vulnerability at different 'social levels' (source: after Schneiderbauer & Ehrlich 2006).

SOCIAL LEVELS	PARAMETERS	INDICATORS
Individual and household	• Age; • Income; • Health/disability; • Education; • Savings; • Individual and family insurance; • Neighborhood network; • Access to information;	• Average age; • GDP per capita; • Malnutrition of children <5; • HIV/AIDS infection rate; • Productivity per capita (primary sector); • Number of mobile phones, TVs, radios/p. capita;
Administrative Community	• Infrastructure/accessibility; • Presence and quality of civil protection, including early warning/emergency plan/disaster management capacities; • Disaster preparedness; • Degree of autonomy/participation in decision making procedures and access to resources;	• Traffic infrastructure/road network; • Density of rural population; • Level of urbanisation; • Level of corruption;
Country	• Regulatory environment; • Armed conflicts with involvement of national government; • Population structure; • Economic system; • Economic dependency; • Infrastructure/services; • National disaster planning; • Forecast and early warning system; • Emergency management system and capacities; • Insurance services;	• Type of government/number of signed international agreements; • Number and intensity of conflicts; • Number of IDPs (internally displaced people) and refugees; • Fertility rate; • Sex ratio; • Age average; • Trading activities – rate of GDP; • External aid as ratio of GNI; • Contribution of primary sector to GDP;
Region	• Climate; • Regional political stability;	• Climate records and their long- term changes; • Number and intensity international conflicts;
Cultural Community	• Status of community; • Armed conflicts with involvement of the community; • Gender inequality; • Perception of risk and approach towards emergencies (cultural beliefs); • Coping strategies (incl. farming methods and land tenure system;	• Political discrimination of ethnic groups; • Economic disadvantages of ethnic groups; • Cultural restrictions of ethnic groups; • Intra and inter communal conflicts and their intensity; • GDI (Gender Development Index)[*];

[*] GDI- Gender Development Index looks at life expectancy, and levels of education and income amongst women and men.

10.2 VULNERABILITY AND RESILIENCE ESTIMATION

Resilience and vulnerability can be seen as antonymous in the context of state, county or community security, and this plays a key role in the conceptualization of a security culture. The table below shows the complexity of the notion of security in relation to the community level which can also be used for an analysis of the Baltic Sea Region as a whole. One challenge in assessing resilience is to identify indicators with validity corresponding to what one aims to measure. Qualitative data and subjective indicators are needed in order to establish validity in this respect since there is a need to understand the subjective experiences on the part of the affected populations and individuals. The analysis should, therefore, include context-specific, qualitative and subjective information.[12] The question of reliability is always at stake when indicators are qualitative in their character, but the nature of resilience is too complex to establish validity without recourse to such indicators.

The table below shows how vulnerability can be estimated in general terms, and how the indicators determine its level. The left-hand column shows how a high degree of vulnerability is determined by the values of the indicators. For instance, when the *geographic isolation of the community* is high, vulnerability increases; on the other hand, for vulnerability to be high, the *degree of self-sufficiency* has to be low. In the right-hand column, it is shown which values of the indicators correlate with low vulnerability, approaching the value of resilience. The examples include a low level of *geographic isolation of the community* and a higher *degree of self-sufficiency*. Thus, depending on the indicator, the high or low values can either be positively or negatively associated with vulnerability.

Table 3: Security as a process: interaction between domains, barriers and crisis management cycle.

HIGH	VULNERABILITY	LOW
HIGH	Geographic isolation of the community from others	LOW
HIGH	Extent to which community members are isolated from each other	LOW
LOW	Degree of self-sufficiency	HIGH
LOW	Level of community spirit (Social Capital)	HIGH
HIGH	Degree to which families are dispersed geographically	LOW
LOW	Mobility of community members	HIGH
LOW	Equality of distribution of authority	HIGH
HIGH	Level of inherent conflict within community	LOW
LOW	Risk awareness	HIGH
HIGH	Susceptibility to source of risk	LOW
LOW	Resilience with respect to a realised source of risk	HIGH
LOW	Level of preparedness, both response and recovery	HIGH
LOW	Pre-emergency economic viability	HIGH

[12] Food Security Information Network, 2015. *Qualitative Data and Subjective Indicators for Resilience Measurement.* Technical Series No. 4: Report of Resilience Measurement Technical Working Group.

[13] Sullivan, Mark, 2003. Communities and their experience of emergencies. *The Australian Journal of Emergency Management,* 18(1), pp.19-26.

In this context, the formula for estimating resilience can be defined. Outrage Theory highlights that risk has two elements: hazard, defined as the experts' understanding of risk based on estimations of de facto losses in lives or in financial terms, and outrage, i.e. the public's perception of risk based on various aspects (see table 1). Domain Theory presents the concept of barriers in relation to specific domains, and how the optimization of both the systemic and supplementary barriers offers the best foundation for resilience. Resilience is both these components put together, i.e. risk and barriers, which means that a model estimating resilience can be formulated as follows:

Res. = f(R,BT),

Res. – resilience, f – function, R – risk, BT – systemic and supplementary barriers influencing each other.

Resilience = (risk = hazard + outrage) + (total barriers = systemic and supplementary barriers)

Prerequisites for a Common Culture: Common Risk Perception and Communication and Diversified Actions

Risk perception is important in relation to the notion of a common security culture in the Baltic Sea Region. Since there is a multitude of historical experiences in the region, the populations in each of the countries perceive forthcoming threats differently. It is, therefore, important to establish a common ground for understanding issues of risk and threat to enable more widespread cooperation in the field of disaster risk reduction. The current diversity of experiences causing differences in perception could create challenges and obstacles for a common understanding, but by raising awareness of the differences and what they are caused by, and by efforts to build a common understanding founded on the analysis of contemporary data and facts, the challenges can be overcome. This common understanding then lays the foundation for a common security culture fostering a safer and more resilient region.

Another potential challenge related to establishing a common understanding as a basis for a common security culture in the Baltic Sea Region is the increasing migration rate in the Baltic Sea Region, followed by different perceptions of risks due to different socio-cultural backgrounds. This inflow of experiences causing different kinds of outrage (i.e. public perception of risk), could then weaken the foundations of a common culture in regards to security, making it more difficult to cooperate and to make efforts coherent. This is not an issue that can be solved by ignoring it. Rather the quality of leadership and communication becomes increasingly important. They have to be based on awareness of the perceptions on the ground, and they have to relate to and reflect outrage, in order to be fully efficient and relevant. The issue of diffusion of the common understanding can possibly be overcome by clear communication, gathering the experiences from the public in the region, making the common security culture a coherent concept, and reflecting the actual experiences of the whole regional community and its different parts.

The cultural diversity within countries is one aspect to take into consideration, as in the case with the influx of migrants. Another aspect is the diversity between countries and the arrangement of the division between the public and the private sphere. As Domain Theory highlights, the external security measures for the individual security domain (ISD) shape and influence individuals' decision-making processes. These external security measures can be planned at the policy level, based on solid evidence and coherent strategies for disaster risk reduction. However, the size and scope of the ISD differ between the countries in the Baltic Sea Region, which could possibly present challenges to cooperation between the stakeholders in the region. This is an institutional matter that has to be taken into consideration in the planning process of common efforts. The objective should not be to streamline the institutions of the respective countries; rather the differences have to be brought into the light which could mean that an effort with a common aim for all the countries in the region could potentially have different implementation plans for each country, adapted to the specific country's institutional arrangement.

The regional security domain (RSD) is significant for the discussion about a common security culture in the Baltic Sea Region. However, there is an important distinction between the regional security domain and the state security domain (SSD) in terms of the influence on the ISD. In the SSD decisions can be made and then implemented without any obstacles, directly influencing the ISD. The SSD is external to all levels below; however, the RSD is not external to the SSD in the same sense. In the RSD, decisions cannot be directly implemented in each state in the region due to national sovereignty; elaboration and consensus have to be components shaping the basis for any effort. This means that the SSD and RSD are integral parts of one another, rather than the RSD being external to the SSD. In the planning processes, this calls for special attention and consideration; planning in the RSD cannot be shaped the same way as in the SSD.

Activities and Tools

This section will present a number of activities and tools that can support efforts in the different phases of the security cycle, and they will be divided in accordance with those phases, i.e. prevention, preparedness, response and recovery. Attached to each activity is a list of possible tools. The proposed activities and tools make no pretense to being an exhaustive, complete list of possible options for action. They reflect priorities related to the issues that have been discussed in the theory and methodology sections of this paper. From this perspective, proposals presented here can be supplemented by other recommended actions and instruments, whenever it turns out that some issues are relevant but are not included here.

First is a table with an overview of the activity areas presented, showing which phase(s) each activity addresses, and which security domains are involved in the respective activity.

Table 4: The phases and domains different fields of activities address, and the domain responsible

ACTIVITY AREA	PHASE	DOMAIN RESPONSIBLE	DOMAIN TARGETED
Education and information	Prevention Preparedness Response Recovery	GSD RSD SSD	ISD MSD DLS
Safety technology	Prevention Preparedness	SSD	DLS
Identification hazards	Preparedness	GSD RSD SSD	ISD MSD DLS
Critical infrastructure	Prevention Preparedness Response	SSD DLS	SSD DLS
Leadership	Prevention Preparedness Response Recovery	GSD RSD SSD DLS	ISD MSD
Coherence and cooperation	Preparedness Response	SSD DLS	ISD MSD DLS
Cultural awareness	Prevention Preparedness Response	SSD DLS	ISD MSD DLS
Media	Prevention Preparedness Response		ISD
Lessons learnt – best practice	Recovery	SSD DLS	ISD MSD DLS
Reconstruction	Recovery	SSD DLS	ISD MSD DLS

ISD – Individual Security Domain
MSD – Micro-societal Security Domain
DLS – Domain of Local Security
SSD – State Security Domain
RSD – Regional Security Domain
GSD – Global Security Domain

11. PREVENTION

11.1 EDUCATION

The role of education is of utmost importance in the prevention phase. Education and/or information spreading can target the ISD, MSD, and DLS. This is the most effective form of preventing dangers, both in terms of cost-efficiency and societal effects. Education constitutes a solid strategy for building a population's safety and offers the possibility to influence attitudes, values, knowledge and skills required for preventing dangers in society. Through shaping the citizens' consciousness it is possible to raise awareness and influence behavior.

Education and information campaigns can influence prevention – in the ISD, MSD, and DLS – both through shaping "safe" behaviors and attitudes and through developing a sense of responsibility for undertaking particular preventive actions. In the planning of educational efforts or information campaigns it is important to consider which groups are targeted and how communication about risks is conveyed. Especially in regard to outrage, the public usually understands dangers and risks differently than experts. However, several aspects have to be taken into consideration in target group analysis: geographic location (including urban neighborhoods, villages, remote areas, slums, and suburbs), gender, age, and education level, knowledge of the dangers, language, ethnicity, culture, and type of workplace. It is important to emphasize that marginalized groups need special attention.

List 1 - Specific educational tools:

- One-way broadcast (from one single source to a wide audience);
- Two-way face-to-face interactions;
- 'Many-to-many' interactions (as in social networking using telephone and web tools);
- Publications: posters, guidelines, flyers, brochures, booklets, activity books, paper models, comic books, story books, tales, coloring books or electronic coloring books;
- E-learning – self-study curricula;
- Performing arts: plays, dance performances, poems, songs, street theater;
- Games: online safety games, card games, board games, plays, drawing competitions, writing competitions or tournaments;
- Audio and video materials: short videos, radio programs or television;
- Web pages and activities: websites, online games or online quizzes;
- Social media and telecommunications.

11.2 TECHNOLOGY AND RISK ASSESSMENT

Research and development are important in the field of disaster risk reduction and new technologies and techniques for how to prevent risks are needed. It is important to "*provide guidance on methodologies and standards for risk assessments, disaster risk modelling and the use of data; identify research and technology gaps and set recommendations for research priority areas in disaster risk reduction; promote and support the availability and application of science and technology to decision- making*".[14]

List 2 – Technology and techniques for prevention measures:

- Scientific analysis;
- Devices to identify hazards;
- Risk assessment methodology;
- Resilience estimation methodology.

11.3 CRITICAL INFRASTRUCTURE

Related to prevention, the planning of the placement of critical infrastructure is an issue important to consider. However, first it is necessary to identify the critical infrastructure in a society. In order to be able to determine and identify "safe" locations for the planning of critical infrastructure, foresight analysis has to be performed, along with risk assessment. The term "location" does not necessarily mean geographical location here; it also includes virtual locations with reference to cyber security.

List 3 – Tools for identifying "best practices" for critical infrastructure:

- Risk assessment methodology: risk mapping, risk matrix, zoning plans or geoportals;
- Foresight analysis: scenario analysis;
- Identification (and definition) of critical infrastructure;
- Assessment of interdependence of critical infrastructure;
- Information technology tools and analysis;
- Assessment of likely environmental impacts enabling preventive efforts;
- International database of experts in the field of CI: meetings or conferences;
- Research for developing resilient infrastructure;
- Building critical infrastructure in "low" risk locations.

12. PREPAREDNESS

12.1 EDUCATION

Education and information campaigns are certainly equally important for the preparedness phase as for the prevention phase, but the scope and focus are slightly different in terms of message and information disseminated through

[14] UNISDR, 2015. Sendai Framework for Disaster Risk Reduction 2015 - 2030, p. 16.

educational channels. In the preparedness phase, focus is on preparing citizens for threats or dangers possibly waiting in the future. The education tools are the same as the ones used for addressing prevention, but the content differs (see list 1 in section 11.1 for educational tools). It is important to convey knowledge related to the occurrence of dangers, realizing the scale and types of needs in difficult situations and to shape proper behavior habits in hazardous situations. The most important threats to pay attention to are natural hazards: strong winds, frosts and blizzards, heavy rains, heat and drought, floods (snowmelt) and storms. When education programmes are being planned, it is important to take the target group into consideration.

12.2 CRITICAL INFRASTRUCTURE

To be prepared for potential hazardous events is important in relation to how to handle the critical infrastructure. A backup plan should be prepared that can be implemented if a disaster strikes, and a strategy for how to protect critical infrastructure should also be outlined and ready for use. The tools in list 3 in section 11.3 can be used for establishing preparedness, but there are some additional tools as well, presented below.

List 4 – Tools for establishing preparedness in relation to critical infrastructure:

- Back-up plans;
- Plans for protection of critical infrastructure if a disaster strikes with a particular focus on:

transportation, transport of dangerous industrial plants, pipelines (gas, water, fuel, etc.), landslides, oil wells, gas stations, power stations airports, storage of hazardous substances, dams, other hydraulic structures and other facilities specific for a given area and internet storage servers;

- Aiming for independence in relation to critical infrastructure;
- Contingency planning: guides, programs or information technology programs;
- Threat monitoring for critical infrastructure;
- Information sharing about critical infrastructure protection: books, conferences, meetings, websites, social media and regular media.

12.3 LEADERSHIP

Leadership is one of the most important issues to focus on in the effort to build a security culture, although it can pose a great challenge as well. The leadership should have the skills to build and lead a team, to raise individuals' self-awareness and to develop individuals' potential, but also to build authority and develop capacity for knowledge sharing. All these skills are necessary for managing effective communication, support and cooperation between all parties if a disaster strikes.

List 5 – Tools establishing preparedness in relation to leadership:

- Establishing clear leadership structures;
- Proper identification and definition of leadership, command and control at different levels of security management;
- Encouraging and developing team work skills among groups;
- Encouraging cooperation and collaboration;
- Building authority needed in case of emergency – development of emotional intelligence;
- Meetings with various groups in society establishing contact between citizens and leadership;
- Developing effective communication skills: study meeting and exchanges of expertise and experiences;
- Developing relationship management: meetings, integration or education.

12.4 CULTURAL AWARENESS

Culture is highly influential in formulating people's behavior and experience during disasters, which means that cultural diversity is also highly influential at the community level. In consequence, the level of cultural awareness in a community makes the citizens more prepared for handling a disastrous event. Therefore activities taking the cultural aspect into account should be organized. It is also highly important to raise cultural awareness among the rescue services.

List 6 – Tools furthering cultural awareness:

- Educational and informational campaigns promoting cultural awareness;
- Activities focusing on the cultural aspects;
- Identifying cultural differences in terms of disaster risk management;
- Online training programs – e-learning systems;
- Cultural exchange activities;
- Activities aiming for cultural integration in communities.

12.5 TECHNICAL EVALUATION AND CAPABILITIES

Preparedness entails being prepared in terms of materials and capabilities, and it has to be aimed at the actual threats and risks to be effective. It is also highly important that people can access the resources they need.

List 7 – Preparedness through materials and capabilities:

- Assets (redistribution of assets);
- Risk analysis aiming to define the needs;
- Creating a database mapping the resources needed in case of a disaster;
- Creating a database with tools for safety;
- Training, information and exercises in how to use certain materials;
- Guidelines and technical standards regarding support in risk management.

13. RESPONSE

13.1 INFORMATION

To be able to disseminate information to all affected people in case of a disaster is highly important. The relevant information might concern handling specific situations, who to contact, potential back-up plans if critical infrastructure has been destroyed or more generally, electricity for instance.

List 8 – Information channels in the response phase:

- SMS-services;
- Radio;
- People responsible for spreading information verbally;
- Internet;
- Social media.

It is important to remember that while planning the dissemination of information, target group analysis has to be performed, and the aspect of marginalization has to be taken into consideration as well.

13.2 LEADERSHIP (AND COOPERATION)

Leadership during an emergency situation is highly important, especially when people are frightened and might act irrationally due to their emotional state. The leadership has to be prepared for any disastrous situation and guide groups and individuals in a constructive manner, especially since the leadership should have a strategical perspective and an overview of what needs to be done. Several of the tools in list 5, in section 12.3 are important for building the structures of leadership necessary for operational functionality in the response phase.

List 9 – Leadership during the response phase:

- Clear guidance of the public on the priorities through available communication channels;
- Clear communication of the scope and consequences of any disaster – transparency;
- Transparency regarding accountability;
- Responsibility for making the efforts coherent;
- Coordinating the efforts of different individuals and groups and make them work together – foster cooperation.

14. RECOVERY

14.1 INFORMATION AND EDUCATIONAL CAMPAIGNS

In the process of recovery, it is important to engage the whole society, and this is done through the dissemination of information about what can be done, and how it can be done. In the recovery phase it is also important to learn from previous events, and in relation to this, information spreading and educational campaigns are of utmost importance.

14.2 RECONSTRUCTION

To rebuild and reconstruct infrastructure that has been destroyed is an integral part of the aftermath of a disaster; however, this can be done in different ways. The aim could just be to restore infrastructure to its former state, or reconstruction could be undertaken with the aim to facilitate resilience to forthcoming threats. When the vulnerability is known due to a recent disaster, it is easier to choose one's priorities.

List 10 – Reconstruction during recovery:

- Taking advantage of the knowledge gained from a disastrous event
- Reconstruction with the aim to build resilience for the future

14.3 LESSONS LEARNED

In the recovery phase, emphasis should not only be put on reconstruction and moving on. On the contrary, the event that took place has revealed important information that needs to be used for future planning. Lesson learning needs to be an integral part of the reconstruction efforts, and of future consideration of disaster risk reduction. It is also important to take into account the changes in perception that might have occurred as a consequence of an event.

List 11 – Taking advantage of lessons learned during the recovery phase:

- Institutional learning – what was done that was good, and what needs to be revised?
- Analysis of how the event affected different domains;
- Analysis of how risk perception on the part of the public (i.e. outrage) is affected by the event;
- Using the information revealed by an event for future planning – how have the different domains been affected? What were people's perceptions and actions during the event? How has the infrastructure been affected?
- Rehabilitation and reconstruction need to start ahead of a disaster. The recovery phase presents a critical opportunity to "build back better".

14.4 RECONSTRUCTION OF CRITICAL INFRASTRUCTURE

In the recovery phase, if critical infrastructure has been destroyed, the reconstruction has to be undertaken with the intention to prevent future destruction and to build preparedness. This could mean that critical infrastructure that has been destroyed has to be relocated, or rebuilt in a different and more resilient manner. It is of utter importance that critical infrastructure is kept intact even in case of a disaster; this means that information revealed from an event can be used to build resilience for the future.

List 12 – Recovery and reconstruction of critical infrastructure:

- Use the information revealed by an event to build resilience in the reconstruction;
- Build preparedness in the recovery phase.

Concluding Remarks

This report aimed to contribute to the enhancement of the understanding of the concepts of security, risk, and resilience, particularly in relation to the construction of a common security culture in the Baltic Sea Region. The theoretical foundation of this report is two-fold. The first theoretical perspective has emphasized the importance of understanding the distinction between risk perception of the public and by experts. The second theoretical perspective has highlighted the relevance of understanding the different levels – or domains – of security, and how these influence the security systems, through supplementary and systemic barriers potentially in play between the domains. The objective to present these theories in relation to the concepts of security, risk, and resilience, was necessary for the modeling of resilience estimation. All these aspects are tied together in the sense that they can build a common understanding of the different components of a security culture, thus contributing to the building of a common security culture potentially functioning as a platform for cooperation around security issues in the Baltic Sea Region.

The issue of vulnerability has received special attention in this report since it is too often neglected in the planning and implementation processes of security systems. Vulnerability can take several different shapes, and it contributes to the complexity of the structure of needs in society. However, overlooking this issue means that the security systems that are created will be flawed. Hence, addressing vulnerability is not just an effort beneficial to the vulnerable individuals themselves, but rather it strengthens the security system overall and allows for a more resilient society.

Another objective of this report has been to outline the importance of planning the security measures and systems with respect to the different phases of the security cycle: prevention, preparedness, response and recovery. Even though some tools can be used to address a number of phases, the intentions and aims of the actions depend on which phase they are targeting, and when specific tools are activated. In the last section of this report potential activities and tools have been presented, some of them more detailed than others. However, the idea has not been to outline specific recommendations for actions, but rather to give an overview of the types of activities that can possibly be activated in relation to the specific phases.

In conclusion, an outline of the five most prominent potential benefits of this report is presented below:

1. The content and the theoretical approach in the report contribute to the understanding of the concepts of risk, security and resilience overall.
2. The report contributes to the understanding of how a common security

culture can be constructed, and the potentials and challenges attached.
3. The report outlines the potential in establishing a common security culture as a basis for cooperation around security issues in the Baltic Sea Region.
4. The model of resilience estimation can be used as a tool for understanding which aspects should be considered in the planning processes of security systems.
5. The activities section of this report can be used as a tool for the conceptualization of different actions and their relationship to the different phases of the security cycle.

References

Alexander David E., 2016. The game changes: *Disaster Prevention and Management after a Quarter of a Century. International Journal of Disaster Prevention and Management*, 25(1).

Council of the Baltic Sea States (CBSS) Secretariat, 2014. *Being Secure in the Baltic Sea Region. A Handbook of a Priority Area Secure*. Vilnius: KOPA.

European Commission, 2014. *Macro-regional strategies. Retrieved 2016-11-10*, from http://ec.europa.eu/regional_policy/en/policy/cooperation/macro-regional-strategies/

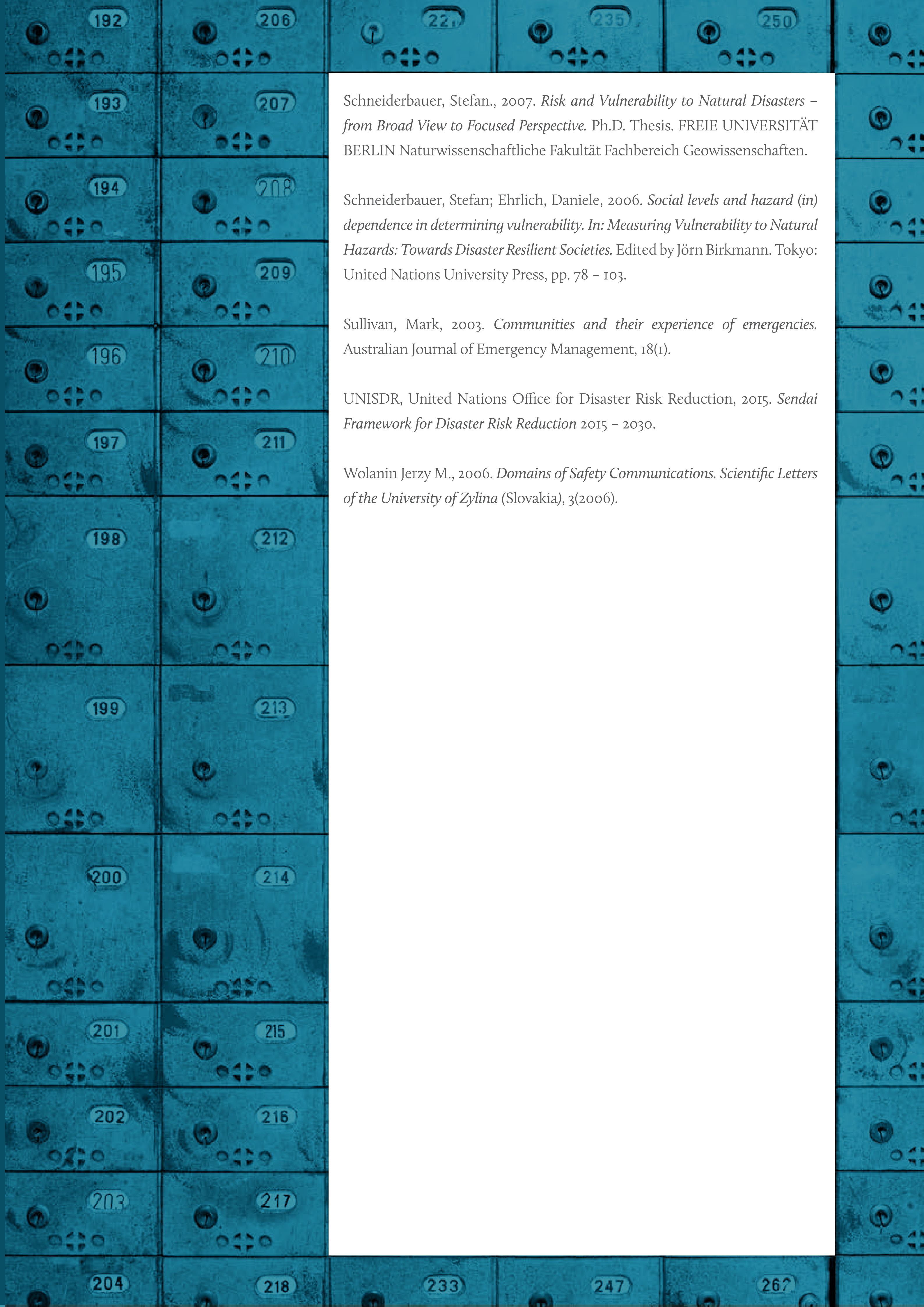
Food Security Information Network, 2015. *Qualitative Data and Subjective Indicators for Resilience Measurement.* Technical Series No. 4: Report of Resilience Measurement Technical Working Group, September 2015.

Klein R. A., 1997. *Monograph on Risk Assessment for Emergency Services.* Leicester: Institution for Fire Engineers (Publications) Ltd.

Sandman, Peter M., 1987. Risk Communication: Facing Public Outrage. *EPA Journal* (U.S. Environmental Protection Agency), November 1987.

Sandman, Peter M., 1988. *Risk Communication: Facing PublicOutrage.* Management Communication Quarterly, 2(2).

Sandman, Peter M., 1993. *Responding to Community Outrage: Strategies for effective Risk Communication.* Falls Church: American Industrial Hygiene Association (AIHA) Press.



Schneiderbauer, Stefan., 2007. *Risk and Vulnerability to Natural Disasters – from Broad View to Focused Perspective.* Ph.D. Thesis. FREIE UNIVERSITÄT BERLIN Naturwissenschaftliche Fakultät Fachbereich Geowissenschaften.

Schneiderbauer, Stefan; Ehrlich, Daniele, 2006. *Social levels and hazard (in) dependence in determining vulnerability. In: Measuring Vulnerability to Natural Hazards: Towards Disaster Resilient Societies.* Edited by Jörn Birkmann. Tokyo: United Nations University Press, pp. 78 – 103.

Sullivan, Mark, 2003. *Communities and their experience of emergencies.* Australian Journal of Emergency Management, 18(1).

UNISDR, United Nations Office for Disaster Risk Reduction, 2015. *Sendai Framework for Disaster Risk Reduction* 2015 – 2030.

Wolanin Jerzy M., 2006. *Domains of Safety Communications. Scientific Letters of the University of Zylina* (Slovakia), 3(2006).