*Driv*ing Innovation in Crisis Management for *E*uropean *R*esilience

D92.11 – Report on the Creations of Secondary Insecurities

Restricted to the consortium

Grant agreement number:	607798	Due date of deliverable: 31 December 2014
Start date of the project:	2014-05-01	Actual submission date: 19 December 2014
Duration:	54 months	

Lead Beneficiary: PRIO

Contributing beneficiaries: ARC, FHG

Keywords:
Secondary insecurities: Unease and Fear, Secondary Insecurities and Challenges in Deploying Technologies, Secondary Insecurities and Challenges in Terms of Legalities, Socio-Economic Secondary Insecurities and Challenges; Assessment Framework, Criteria Definitions, Assessments, Recommendations for tool development;

Dissemination level:	
PU	x
PP	☐
RE	☐
CO	☐

Release Number	Release date	Released by
0.1	31 October 2014	Mareile Kaufmann, Stine Bergersen, Covadonga Morales Bertrand
1.0	12 December 2014	Mareile Kaufmann, Stine Bergersen

Executive Summary

The purpose of the deliverable is to signal the secondary insecurities that crisis management (CM) measures and tools may cause for society, for example unease, suspicion, misuse, the creation of new vulnerabilities, economic instability and much more. In order to provide this information in the most accessible and structured manner, the deliverable is based on a framework that assesses different *categories of CM measures and tools* and their relation to *key criteria*. This deliverable is closely related to D92.21, the assessments of which focuses on the various societal costs and challenges that CM measures and tools may cause. Assessments and recommendations can be used as guidelines for the specific development of measures and tools in DRIVER, but also for CM in general.

The deliverable first introduces the assessment framework in detail. It summarizes this framework in a table (also giving reference to the relevant DRIVER tasks). The deliverable then introduces the key societal criteria through short definitions and examples. The core of the deliverable provides the assessments for each category. This part introduces each category and gives a short assessment of how measures and tools belonging to this category may impact on the most relevant criteria. Furthermore, it gives a short example that is DRIVER-relevant and concludes with concrete recommendations for the developers and users of CM tools and measures and provides an outlook for the follow-up deliverables.

The contents of this deliverable are closely related to the contents to be taught to key stakeholders in WP94.

Table of content

Table of figures

List of Acronyms

Abbreviation / acronym	Description
CM	Crisis management
Cf	See
D	Deliverable
EU	European Union
DoW	Description of Work
Ibid.	As above
ICT	Information Communication Technology
NSA	National Security Authority
PoT	Portfolio of Tools
PSS	Psychosocial Support
SP	Sub-project
SotA	State of the Art
T	Task
UAV	Unmanned Aerial Vehicles
USA	United States of America
WP	Workpackage

Table 1 List of Acronyms

1 Introduction

Crisis management (CM) and societal resilience, the key aspects of DRIVER, are often defined via measures and tools that allow individuals, communities, public and private sector to adapt their behaviour, help oneself and help each other in times of crises.[1] **However, the success of crisis management and societal resilience is not only about having tools and measures in place. The resilience of a society is also dependent on the values and identities a society shares as well as on the level of societal acceptance of CM measures.** In the aftermath of the 9/11 attacks[2] or the attacks on Norway[3], for example, these values were drawn upon by the country leaders at the time to strengthen and re-build and understanding of society.

Fostering these core values and principles, which are often seated at the core of societal identities, is important to strengthen societal resilience. At the same time are these societal principles often strained and negatively impacted – not only during crises and emergency situations that often disproportionately hit the most vulnerable in society, but also by tools and measures that are implemented in the name of crisis management. CM measures and tools can unintendedly perpetuate vulnerability, for example, by not taking the specific needs of different cultural groups or age- and gender-related needs into account. The overarching aim of workpackages 92 and 93 is thus to identify opportunities to foster societal values and ensure that DRIVER measures and tools produce as little as possible unforeseen negative side-effects on society. This contributes to the sustainability of the CM portfolio of tools, one of DRIVER's core objectives, from a societal perspective.

This deliverable in particular provides assessments of the **insecurities and secondary risks** that can be caused or produced by CM measures and tools that are developed and proposed by the DRIVER project. The deliverable is related to D92.21, which uses the same framework to assess the **societal costs** caused by crisis management measures, and the potential negative impacts they cause for society. The complete WP92 thus seeks to create a common understanding for avoiding unintended and disproportionate negative effects of CM measures and tools.

It could be helpful to briefly define the similarities and differences of insecurities, secondary risks and societal costs. Insecurity is defined in WP92 as an emotional state that includes fear and a general feeling of unease, whether on an individual or at societal level. As well-known from the context of critical security studies, security measures do not always cause a feeling of security, but can produce a *climate of fear* to achieve specific political goals, which, at the same time, impact negatively on society.[4] Secondary risks are here explored in terms of three main areas: Risks that may be caused when deploying CM technologies, such as new vulnerabilities and misuse, risks that CM measures and tools cause in terms of legality (however, a dedicated deliverable will be produced by FHG in WP 83) and in terms of economy. Besides that, there are a range of other key societal principles and values, which can be infringed upon, such as trust, solidarity and non-discrimination. These values

[1] IFRC 2012, "The road to resilience. Bridging relief and development for a more sustainable future." ; Longstaff, P.H., Armstrong, N.J., Perrin, K., Parker, W.M., and M.A. Hidek (2010): Building Resilient Communities: A Preliminary Framework for Assessment. Homeland Security Affairs VI (3). Cf. DRIVER DoW, Part B p. 9

[2] Colucci L (2008) Crusading Realism. The Bush Doctrine and American Core Values After 9/11. Lanham: University Press of America.

[3] http://www.telegraph.co.uk/news/worldnews/europe/norway/8659028/Norway-shooting-July-24-as-it-happened.html

[4] Furedi, Frank (2006) The Culture of Fear Revisited. London: Continuum. Jaeger, C; Renn, O, Rosa Eugene A, Webler, Thomas (2006): Risk, Uncertainty and Rational Action. London: Earthscan. Baker, Tom and Simon, Jonathan (2002) Embracing Risk. The Changing Culture of Insurance and Responsibility. Chicago: The University of Chicago Press.

and principles are explored in deliverable 92.21, the assessment of societal costs and negative impacts to society. Even though there is a distinction between insecurities, secondary risks and societal costs/negative societal impacts, these three overlap heavily – in fact, all of them fundamentally relate to insecurity. Additionally, all criteria that indicate insecurities, secondary risks and societal costs will finally feed into one overarching criteria system that is used to assess different sets of measures and tools in terms of their societal impact. They are here presented as separate to structure the deliverables accordingly.

Since SP9 follows an understanding of societies as centred around values and identities, the chosen criteria that are used to assess insecurities, secondary costs and negative societal impacts are selected on the basis of the core values that characterize European cross-border societies. The criteria represent values and principles which recur throughout European Union, United Nations and International Federation of the Red Cross Red Crescent CM policies (cf. 93.1). An in-depth introduction to the criteria is given in Chapter 4.

Since CM and resilience tools generally address society at large and the citizen directly, it is important to understand how the DRIVER measures and tools may impact the citizens and the values that are at the core of their identity. It is important to understand the crucial role that society at large and different actors in society play in dealing with crises (this is captured in the concept of societal governance, which will be further developed in 94.1). The fact that the societal acceptance of measures is central to the success of CM, and societal actors play increasingly important roles in CM necessitates what the DoW describes as a "societal cost-benefit analysis". Such an analysis would test in what way CM tools and measures can create negative impacts on key societal values and principles on the one hand. On the other hand, the same criteria can be used to assess the opportunities to foster societal resilience through these values, as well as the acceptance and legitimacy of CM measures and tools altogether. This is the role of the criteria system developed in WPs 92 and 93, which is adapted iteratively throughout the whole project. The criteria system shall function as a set of indicators and help guiding societal impact assessments or "societal cost-benefit analyses".

1.1 What does this deliverable do – and what will happen in the follow-up deliverables?

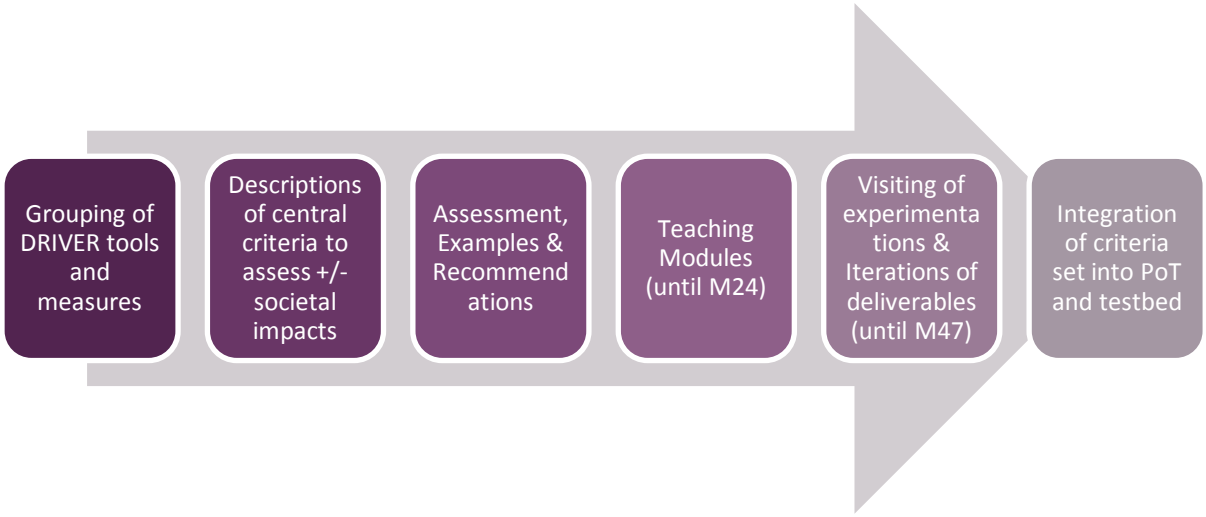
The deliverable will first introduce the framework that has been designed to conduct societal impact assessments in WPs 92 and 93. This includes an introduction to the way in which CM methods and tools were categorized. Since DRIVER develops a large portfolio of tools and not each tool can be assessed by itself, WP92 developed a set of tool categories and subcategories, which organize the various DRIVER CM measures and tools into meaningful units for societal impact assessments. The framework furthermore introduces the selection of key criteria, as well as a short discussion of the limitations and added value of this framework (Chapter 2). Chapter 3 will introduce the methodology that is used to conduct the assessments. Chapter 4 will introduce the criteria that are relevant for this deliverable in detail and give definitions for each of them to create a common understanding and terminology throughout the project. Chapter 5 is the core of this deliverable as it runs a first set of assessments of the different categories of measures and tools vis-à-vis the set of criteria. Every sub-chapter in Chapter 5:

- Introduces the category of measures and tools that are being assessed,

- Presents potential impacts on the most relevant criteria,
- Gives examples that are DRIVER-specific and
- Provides general recommendations that should be taken into account when developing CM measures and tools.

Assessments and recommendations can also be taken as guidelines and advice for the development of CM measures and tools in general. The assessments were conducted by PRIO and ARC. In conclusion, an overview table will summarize the discussed criteria, giving orientation to the DRIVER task leaders, in order to display which assessments are of particular relevance to them. The conclusion also points to the way in which this criteria system will be iterated and developed further in follow-up deliverables.

On an overarching level, SP9 implements the steps below. An initial version of the first three steps is presented in this deliverable (as well as D92.21). The idea of societal impact assessments and societal governance will be taught to the consortium in WP 94 to sensitize the partners to develop societally sustainable measures and tools. The WP 92 and 93 deliverables will be iterated throughout the project and made increasingly operational. A final version of the criteria system will be merged with those criteria of 93.1 and integrated into the DRIVER portfolio of tools (PoT) and the DRIVER testbed.



Deliverable 92.11 is thus a **first version** of a set of deliverables that will address key societal criteria, their assessments vis-à-vis tools, examples and recommendations. Since the tool development phase in DRIVER has only started, assessments in this deliverable naturally focus on theoretical discussions and literature that already exists about secondary impacts. They will address overarching challenges vis-à-vis the foreseen development of measures and tools for crisis management. After being present at various experiments in the different SPs, criteria, assessments and recommendations can be refined and the overall deliverable can be made more operational. As the different measures and tools are being developed further throughout DRIVER, the categorization of measures and tools will also be refined. This deliverable will have one follow-up deliverable in year 2. By producing these follow-up deliverables, SP9 “accompanies” the tools and measures (that are tested in experiments) and conducts re-assessments of societal impacts based on their experience from the experiments. It adapts criteria and recommendations where necessary in order to support a key objective of DRIVER, namely to facilitate change by accompanying the campaigns of experiments.

2 Framework for Conducting Societal Impact Assessments in DRIVER

2.1 Categorization of DRIVER Methods and Tools

Throughout WPs 92 and 93 SP9 conducts assessments of both crisis management activities *in general* and DRIVER measures and tools *in particular,* with regards to the creation of secondary insecurities (92.1), other societal costs (92.2), and positive societal impacts (93.1), all of which feed into suggestions for the refinement of measures. The idea was to develop an assessment framework that can be re-used in all deliverables that conduct societal impact assessments within WPs 92 and 93 to create a systematic overview and streamline the process. Tasks 92.1 and 92.2 are supposed to make statements and give assessment about CM activities in general and DRIVER tools and measures in particular.

In order to conduct these assessments in a meaningful way, SP9 followed an inductive approach. First, all DRIVER measures and tools were listed. From that, general categories and subcategories of crisis management activities were deducted. In a following step it was determined whether these activities are directed at the general population, crisis management professionals, volunteers or any others. Since each of the planned DRIVER measures and tools can incorporate several (sub-) categories, all planned DRIVER measures and tools were assigned to those categories that they fit into. The subcategories are the basis for the following assessments. DRIVER members can check in the overview table which kinds of assessments are relevant for their specific task. The value added by this framework is that it allows SP9 to make assessments about general CM activities at the same time. Through this approach the categorization also avoids repetition and is more effective than an assessment of each the 40 DRIVER measures and tools on a singular basis, since every DRIVER measure and tool combines several activities. Some DRIVER tasks are listed under several different categories, as these tasks combine many different CM aspects in one task.

This categorization was sent to SP leaders for their approval. Feedback was provided by SP2, arguing that any SP2 activity addresses methodological aspects. As such, their tasks should either be deleted from the framework or be assigned to a category that evaluates methodological aspects that are relevant also during tools design. Since the fostering of positive societal impacts and the avoidance of negative societal impacts already starts with tool design and specific methodologies can produce unforeseen side-effects, the authors of D 92.11 and D 92.21 decided to include SP2 and any tasks directed at the development of measures and tools. However, they are presented separate from the assessments of the operational measures and tools. They are summarized in the categories “Strategy Design” and “Methodologies for selecting measures & assessing impacts of experiments”. These categories and assessments may not appear in the final version of criteria, assessments and recommendations implemented in the PoT, but they serve as a guideline to develop tools and measures in DRIVER. SP3 has agreed with the framework with a few changes of tasks, but pointed to the necessity of a re-iteration once the DRIVER measures and tools have developed further.

Because the assessments of 92.11 are conducted at the very beginning of the project, they speak to a more general context and include general recommendations for the development of measures and tools. There is also a possibility that new tasks could emerge, that tasks might be joined (where for example the use of simulations is so diverse and fundamental that it is no longer constructive to keep it as a separate category of tools) or that task operations may change during DRIVER, so that the

assignment will look different in the end. Assessments conducted in the follow-up deliverables will take developments within the different DRIVER measures and tools as well as potential effects of combining tools or measures or of combining DRIVER tools with legacy (higher complexity experimentation in SE2 and JEs) into account.

2.1.1 Definition of Framework Categories

Operational tools and measures:

The category **Data & Information** refers to any activity, measure or tool that collects, stores, processes, or exchanges, and analyses data, for example for the sake of situational assessments, or tools that facilitate interoperability.

Risk, Damage and Needs Assessment describes any technology, system, measure or tool that does situational analysis and impact assessment, conducts early warning, risk analysis and forecasting, improves communication systems. Some of these tools are being developed specifically for DRIVER (such as the competence framework developed in 52.1), and some seek to improve concepts that already exist (such as in 34.1). Some, but not all technologies and tools mentioned in this category are closely related to the category Data and Information.

Cross-border and Cross-Sectoral Interaction includes measures and tools that facilitate national and international networking activities of CM partners, volunteers, professionals and institutions; this may include physical meetings or the organization of databases, tools and web-services. On a broader level this category includes tools and measures facilitating interaction across borders and sectors.

Communication between crisis managers and to the public refers to the category of tools as well as training measures that target on the one side the communication between CM professionals, and on the other side the communication between CM professionals and the population and/or volunteers. It includes both, public warning, the organization of stakeholder maps, but also the structured information exchange between different first responders.

Other Forms of Training refers to psychosocial training of the population, professionals and volunteers, but it also includes media training, as well as preparedness and management training of volunteers.

The category **Resilience Logistics & Contingency Plans** includes contingency plans and logistics planning that target resources, supply chains and core functions, for example in a city, in order to make them more resilient.

Decision Support Systems & Simulations. This category describes all activities that prepare and implement scenarios and simulations for exercises (computer-based and real). These are standard components of Crisis Management, most of which will also be made available in the PoT.

The category **Harmonization** refers to the collaborative efforts during all sorts of crisis management activities, but mainly during the response phase.

Methodology and Development of Tools:

The two final categories are placed outside the main table, as they refer to tasks that are not operational. They include preparatory and research-oriented work and are of a more methodological

nature. The recommendations of these categories will most likely not feed into the PoT. They are, however, important categories at this point in time, when tools are being developed and tested.

Strategy Design is a key part of many activities in crisis management and in DRIVER in particular. It supports the design of measures and tools, as well as their measurability and evaluation. It includes methodology and criteria development for community resilience, early warning and risk analysis, learning activities and lessons learned, competence building, and decision-making.

The category of **Methodologies for selecting Measures & Assessing Impacts of Experiments** refers to the DRIVER- experimentation activities, such as research- oriented, preparatory and methodological work from SP2.

Each measure or tool may target or mainly involve the **population** as whole, CM **professionals**, **volunteers** or those researchers and scientists who develop the actual CM tools (**tool developers**). In some cases the addressee is **unknown** at this point in time. Attention needs to be paid to these different addressees as the measures may evoke different side effects on each level. The evaluations within WPs 92 and 93 will mainly target any measure or tool that has the population, professionals or volunteers as a target. Should a measure or tool address the society at large, potential disproportionate effects on particular societal groups, for example specific religious, cultural or age-groups, will be indicated in the assessments.

This categorization is not final. It may be refined over time, and when the tools are further developed, it is possible to identify if there are some tools that are more central and critical to CM than others. Such a prioritization could feed into the final criteria and recommendation system.

Category	Subcategory	Addressees	Measures as of WP/Tasks
Data & Information	Collection & Storage	Population	36.3, 43.1, 43.2, 43.4, 55.3
		Professionals	43.1, 43.2, 45.2, 45.3, 45.4, 52.4, 53.2, 55.3, 55.4
		Volunteers	36.3, 53.2, 55.3
		Unknown	
	Facilitating Data Processing	Population	
		Professionals	43.5,
		Volunteers	
		Unknown	
	Analysis & Evaluation	Population	36.3, 43.2, 43.3, 43.4
		Professionals	43.1, 43.2, 43.3, 43.5, 52.4, 55.4
		Volunteers	36.3
		Unknown	43.1, 53.2
	Exchange	Population	36.3, 43.2, 43.3, 43.4, 44.4
		Professionals	43.1, 43.2, 43.3, 44.4, 43.5, 45.2, 45.3, 45.4, 45.5, 52.4
		Volunteers	36.3
		Unknown	43.1
Risk, Dama	Operational	Population	

	needs assessment	Professionals	34.1, 52.2, 53.1
		Volunteers	52.2
		Unknown	
	Situational Analysis & Impact Assessment	Population	43.2, 43.4
		Professionals	43.2, 43.5, 44.2
		Volunteers	
		Unknown	43.1
	Early Warning, Risk Analysis & Forecasting	Population	
		Professionals	43.3, 44.1
		Volunteers	44.1
		Unknown	43.1
	Communication systems	Population	
		Professionals	45.3, 45.4
		Volunteers	
		Unknown	45.2, 45.3
Cross-border and Cross-Sectoral Interaction		Population	33.2, 36.3, WP55
		Professionals	44.2, 45.2, 45.3, 45.4, , 53.1, WP55
		Volunteers	36.3
		Unknown	52.2
Communication between crisis managers and to the public		Population	35.2, 35.3, 35.4, 36.2, 43.3
		Professionals	35.2, 43.3, 45.2, 45.3, 45.4
		Volunteers	35.2, 36.2, 44.3
		Unknown	
Other forms of Training	Psychosocial	Population	32.2, 32.3, 32.4, WP94
		Professionals	32.2, 32.3, 32.4
		Volunteers	32.2, 32.3, 32.4
		Unknown	
	Media & Policy	Population	
		Professionals	
		Volunteers	
		Unknown	35.2
Resilience Logistics & Contingency Plans	Resources, Supply Chains &	Population	
		Professionals	44.2, 44.5
		Volunteers	

	Contingency Plans	Unknown	44.1, 44.4, 46.1
	Core Functions in the City	Population	
		Professionals	
		Volunteers	
		Unknown	34.1
Decision support systems & simulations		Population	35.3
		Professionals	44.5, , 54.3
		Volunteers	
		Unknown	44.1, 44.4
Harmonization		Population	55.1, 55.3
		Professionals	52.4, 55.1, 55.3
		Volunteers	55.1
		Unknown	52.2, 53.2

Table 2 Categorization of DRIVER Measures and Tools (for operational purposes)

While the table above indicates how operational tools and measures in DRIVER are grouped and assessed, the table below lists methodological tasks. Although not operational, the indicated tasks in the table below indeed influences what a certain CM tool will look like once deployed. This refers to the point that the development of a tool or measure starts already at the idea-stage, and that societal impact can potentially already be influenced here.

Strategy Design	For Community Resilience	Population	WP 33
		Professionals	33.1
		Volunteers	55.1
		Unknown	
	For Early Warning & Risk Analysis	Population	43.3
		Professionals	43.3, 44.1
		Volunteers	44.1
		Unknown	43.1
	For Learning Activities & Lessons Learned	Population	55.1, 55.3
		Professionals	WP51, 52.4, 53.1, 55.1, 55.3
		Volunteers	55.1, 55.3
		Tool Developers	53.2
		Unknown	52.2, 53.2
	For Competence-Building	Population	
		Professionals	WP52

		Volunteers	
		Unknown	
	For Decision-Making	Population	
		Professionals	54.1, 43.1
		Volunteers	
		Unknown	54.3
	Costs & Effectiveness	Population	
		Professionals	44.5
		Volunteers	
		Unknown	44.1
Methodologies for selecting measures & assessing impacts of experiments		Tool Developers	SP2 & SP9

Table 3 Categorization of DRIVER Measures and Tools (for methodology & strategy design)

2.2 Selection of Key Criteria for DRIVER

The different categories and subcategories of measures and tools introduced above are assessed according to specific sets of criteria. In order to do so, SP9 developed different sets of criteria that correspond to the different tasks in WPs 92 and 93. Since some themes within the tasks overlap, close attention was paid in dividing and assigning the criteria *to one task only* in order to avoid double assessments at this point. Eventually, however, the complete criteria system will feed into the PoT and the testbed.

Task 92.1 focuses on **insecurities, such as unease and fear.** Here, it was decided to include, besides the dimension of fear (including criteria unease and suspicion as mentioned in the DoW), dimensions of secondary insecurities and risks vis-à-vis the deployment of technologies, as well as with regards to legality and socio-economic setups.

Since **task 92.2** focuses on **side-effects to societal values,** this task includes three dimensions: core societal values, political and administrative values, as well as rights and ethical principles. This also allows for assessments that describe whether existing values may be changed. For example, how privacy or freedom of movement is changed by the use of some measures and tools.

Task 92.3 focuses on **environmental aspects**. The related deliverable includes primary environmentally issues (potentially caused by DRIVER itself), and secondary environmental issues (to be confronted and/or resolved by DRIVER). The framework presented here and used throughout 92.1 and 92.2 is specifically developed for societal impact assessments. For 92.3, a specific framework is developed that allows for the assessment of impacts of DRIVER measures on the environment.

Together, the current two sets of criteria for 92.1 and 92.2 cover a large amount of different dimensions and criteria that are crucial for the assessment of impacts that crisis management measures may produce for societal life and crisis governance as a whole. For a narrative of the selection of criteria, please cf. Chapter 4. Both, ECORYS' and DWR's expertise on environmental impact assessment has also informed the inductive determination of criteria for 92.3. All dimensions and criteria are described in a few sentences in D92.11, D92.21 and D92.31 before they are put to use in the assessments.

92.1 Insecurities, such as unease and fear and secondary insecurities and challenges	
Dimension	**Criteria**
Fear	Unease Suspicion
Secondary insecurities and challenges in deploying technologies	Function creep vs. limitations Applicability Misuse New vulnerabilities for citizens Creating technology dependency
Secondary insecurities and challenges in terms of legality	Legality/ Legitimacy Truthfulness
Socio-economic secondary insecurities and challenges	Efficiency & effectiveness Impacts on market (production, consumption, innovation) Economic stability Employment
92.2 Side-effects to societal values	
Core societal values	Trust (in fellow citizens & Institutions) Social cohesion Solidarity Participation Diversity & value pluralism Open society vs. culture of control Cultural and gender sensitivity & sensitivity towards other minorities
Political and administrative values	Accountability Transparency/openness/visibility Integrity State-citizen-relationship International political reputation

	Negative standardization International cooperation & treaties
Rights and Ethical principles	Compliance to legal principles of suitability, necessity & proportionality Dignity & non-discrimination Privacy & Data-Protection Freedoms & does it allow for protest

Table 4 Dimensions and Criteria for D92.1 and D92.2

2.3 Value Added and Limitations of the Framework

The main value added by this framework is its effectiveness. Categories and subcategories of measures and tools speak to CM in general and DRIVER in specific (cf. tasks assigned to each more general category). One task can combine several subcategories of measures and tools and thus be relevant with regards to several criteria; the assessments will follow the development of the measures and tools throughout the project, but the assessment will not be based on task-level. The framework is designed to enable an efficient and effective monitoring of crisis management activities in general and DRIVER activities in particular and to provide recommendations to the development team, but also to developers in general, that enable a design respecting societal aspects.

What the framework cannot and shall not do is the *empirical* assessments of each different DRIVER measure or tool. This means that it is not foreseen to conduct experiments or participant observation in order to test how the 40 different DRIVER measures create effects and impacts in detail. SP9 will, however, be part of the experiments conducted in SP3-5 in 2015 to see how tools and measures develop and to get inputs for how to refine criteria, assessments and recommendations to make them more operational.

The next part of this deliverable will explain the methodology that SP9 used to conduct the assessments.

3 Overall Methodology for Societal Impact Assessments

CM and societal resilience can only be fostered if the planned measures and tools take account of those values and principles that sit at the core of those societies it is implemented in. A "societal cost-benefit analysis" tests in what way CM tools and measures can either create negative impacts on key societal values and principles or how the same values and principles can be used as an opportunity to foster societal resilience, as well as the acceptance and legitimacy of CM measures and tools altogether. Some key questions which the tool developer could reflect upon in terms of such an assessment could be:

- Who are the direct addressees of your measure/tool, and could its implementation be relevant to society as a whole?
- Think about the key societal values and principles that characterize European societies. Can you think of any that the planned measure/tool can either *foster* or *infringe* upon? How so?
- Can you think of any effects on society, positive or negative, that you may not have taken into account when planning the implementation of a measure/tool?
- How are you ensuring that your measure/tool will be accepted and considered as legitimate by the addressees and society as a whole?

There are several methodological entry points to assessing ethical and societal impacts of crisis management tools and measures, including theoretical discussions, quantitative or qualitative empirical analysis, methods of multi criteria decision analysis (cf. Belton and Stewart, 2002; Kunsch et al., 2009), scenario planning (cf. Lindgren and Bandhold, 2003) or the use of decision-making tools, as for example developed in the FP7-funded SIRA or ValueSec, DESSI or PACT.[5] As stated above, this workpackage does not follow a methodological approach of empirically testing all potential impacts of all planned measures, which is why the framework was developed in the first place and *key* criteria to be assessed were defined. However, every deliverable that involves assessments is structured in a way that they allow for follow-up deliverables. Workpackages 92 and 93 thus follow a two-step methodology to conduct the assessments.

3.1 Societal Impact Assessment Step 1 – First Version Deliverables

Workpackages 92 and 93 follow the approach of multi criteria decision analysis to structure complex problems by breaking them down in small problems and assessing multiple criteria. The different measures and tools that will be part of the DRIVER portfolio are being developed throughout the first few years of the project. A first assessment of the portfolio and crisis management measures in general is due 8 months after the project has started. Since the different measures and tools exist as a basic idea, but are not very concrete at this stage, deliverables 92.11 and 92.21, as well as 92.31 will formulate general recommendations and identify *likely challenges* that have to be paid special attention to when developing the measures further. **The categorization of measures is here the main reference point for the assessments.** They will serve as a starting point to compile and write assessments. Through that, DRIVER members can check in the overview table which categories of

[5] http://www.sira-security.de/index.html; http://www.valuesec.eu/; http://securitydecisions.org/about-dessi/

measures are most relevant for their task and read up on the potential impacts. These assessments will be written in an easy to understand way and point to potential impacts. By following this structure, the assessments give recommendations about crisis management in general, as well as DRIVER measures in particular. These general assessments and recommendations can then be taken into account in the further planning of the measures and tools. The fact that the assessments are a) conducted early in the project and b) are meant to give general directions to DRIVER partners to develop their tools means that they can, by default, only be general. These first assessments and recommendations are the basis for the teaching equipment (WP94) and serve for the DRIVER consortium as input now that they have just begun to design and develop the different measures.

Inputs for these assessments are based on each partner's expertise on a specific kind of measure, as well as on the SotA mapping-exercise of 91.2 and additional literature, as well as available project findings gained through desk research. This approach presupposes that those who conduct the assessments have extensive knowledge about the particular kind of measures and tools and have general knowledge about the different criteria to be assessed. This will be taken into account when assigning the different assessment tasks in the project. The team conducting the assessments reserves the ability to merge some of the categories for their assessments where necessary and where redundancies can be avoided. The final recommendations will, however, always indicate which subcategories are being covered.

3.2 Societal Impact Assessment Step 2 – Follow-up Deliverables

Now that general recommendations have been disseminated with this deliverable to all relevant partners and each task has advanced in the development of their respective tool or measure, the SP9 team will return to their assessments and conduct evaluations. Here SP9 will participate in SP3-5 experiments throughout 2015 (or if budget constraints are too high, Telcos) in which the will follow the development of the tools and may either organize focus groups for de-briefings (cf. Kamberelis and Dimitriadis, 2013) or the world-café method, a conversational procedure that encourages different groups to discuss a topic by rotating between different tables periodically. They are introduced to the previous findings by a table host (cf. Brown and Isaacs, 2010). The world-café method is only useful if partners working on similar topics rotate between different conversations. By following the focus group or the world-café method, partners working on tasks that belong to similar categories and subcategories will present how they took the general recommendations from the first range of deliverables into account in planning and devising their method/tool. Through that, the assessment team will a) learn more about the specific method or tool and b) learn what ethical challenges and difficulties in implementing the recommendations the partners encountered on their way. Based on these inputs, the assessment team will update the first deliverables by giving specific advice to each partner/task and making the recommendations more operational where necessary and prepare the integration of the criteria and recommendations into the DRIVER PoT.

This methodological approach reflects the overall plan of SP9, which is based on initial recommendations in the first round of deliverables and then follow-up recommendations in the consecutive deliverables and their integration into the DRIVER PoT.

4 Definition of Criteria

On an overarching level, insecurities and secondary risks are those kinds of negative impacts on society, which were not intended to occur and are not always reflected upon in the design or implementation of the measure or tool. DRIVER's aim is to include such reflections already at the stage of the design of the measure or tool. **Insecurity** is defined in WP92 as an emotional state that includes fear and a general feeling of unease, whether on an individual or societal level. As well-known from the context of critical security studies, security measures do not always cause a feeling of security, but can produce a climate of fear to achieve specific political goals, which, at the same time, impact negatively on society.[6] **Secondary risks** are here explored in terms of three main areas: risks that may be caused when deploying CM technologies, such as new vulnerabilities and misuse, risks that CM measures and tools cause in terms of legality and in terms of economy. It should also be noted that an overarching insight with regards to secondary insecurities and challenges, is that many of the criteria described and defined below can be both positive and negative. For example can both fear and suspicion be constructive and helpful instincts in the context of CM and resilience. And a certain degree of fear contributes to the individual being particularly alert in a crisis situation, something that could be useful as a self-protecting mechanism.

Even though the DoW's task descriptions distinguish between insecurities, secondary risks and other societal costs, these categories overlap heavily. They are here presented as separate to structure the deliverables accordingly, but this distinction is to a certain extent artificial, since, finally, all of the criteria from WPs 92 and 93 will feed into one overarching criteria system that is used to assess different sets of measures and tools in terms of their societal impact.

The selected criteria in this chapter function as a tool for societal impact assessments and as a glossary for DRIVER to ensure that a common and consistent understanding of the criteria exists. The aim of this terminology is not to deliver an exhaustive discussion of the concepts, but to deliver a functional definition of the criteria that helps assessing secondary impacts of CM measures and tools on societal values. In some cases, criteria exist to raise awareness, even though there is not always a concrete operational way of avoiding or counter-acting negative impacts (that is often the case with for example function creep, technology dependency and misuse).

SP9 ensures that DRIVER criteria, assessments and recommendations are based on the EU's perspectives on ethics and norms. This includes those values, principles and norms that have been advanced in the political and research landscape, for example in the Fundamental Charter for Human Rights, European policies or outputs from other European research projects that conducted societal impact assessments (cf. ValueSec, DESSI, PACT etc.). As such, SP9 seeks to build upon the existing CM legacy. An advanced analysis of these criteria and their relation to EU, UN, and Red Cross Red Crescent policies, frameworks, case studies and lessons learned can be accessed in D93.1. D93.1, which has been developed in parallel to D92.11 and D92.21, identifies opportunities for positive intervention, verifies the set of criteria used in D92.11 and D92.21 and includes specifically those policies in the review that address CM, Disaster Risk Reduction and Resilience Strategies.

[6] Furedi, Frank (2006) The Culture of Fear Revisited. London: Continuum. Jaeger, C; Renn, O, Rosa Eugene A, Webler, Thomas (2006): Risk, Uncertainty and Rational Action. London: Earthscan. Baker, Tom and Simon, Jonathan (2002) Embracing Risk. The Changing Culture of Insurance and Responsibility. Chicago: The University of Chicago Press.

A further selection had to be undertaken in order to produce a meaningful and manageable amount of assessments. The set of criteria needed to be applicable to DRIVER, so concepts that were too general, too specific or too similar to other concepts were excluded. Should the further development of the project indicate that the selected set of criteria is too expansive or lacking key criteria, it will be updated accordingly. The assessments and recommendations following in Chapter 5 and 6 are a direct consequence from this selection of criteria that is based on EU, UN and RCRC policies as well as additional definitions and thus not to be understood as a normative judgment.

4.1 Unease and Fear

Unease:

Crisis management activities may generate unease. This refers to a feeling of worry or discomfort, anxiety or discontent, and is often related to an uneasy state of mind over the possibility of anticipated trouble[7]. This could be both unease vis-à-vis developments in society that the affected individual feels uncomfortable with, and vis-à-vis other individuals. Unease can be more or less specific, for example a vague dissatisfaction, anxiety, disquiet or a lack of ease (as in social relations). Creating unease (and fear) can also be necessary and intentional, as it can prepare the population for crisis, or heighten their preparedness. A certain sense of unease can also be crucial to realize that a dangerous situation should be taken seriously. This criterion refers to a disproportionate amount of societal unease caused by CM measures and policies.

> *Example: One risk that emergency measures face is, for example, to make the affected groups feel threatened or controlled by specific measures that were originally intended to safeguard them. Since UAVs are mainly known from the military and police context, the use of airborne sensors (43.2), for example, may give individuals the feeling of being under surveillance – even though UAVs may help to create a better overview of the emergency situation. This form of unease is more likely to happen if the reason for the use of the technology is not communicated to and contextualized for society at large.*

Suspicion:

Suspicion refers to the feeling of suspecting something or being suspected of something[8]. The term often has a negative connotation, but can also be a constructive feeling when it refers to being alert. It refers to the way in which populations may have the feeling of being suspected of something, thus being victimized, or they begin suspecting each other. Suspicion can occur in relation to specific groups of the population, the general public, or between affected individuals (whether they are part of DRIVER or not).

> *Example: If CM measures deal, for example, with personal data and the use of this data is not well explained to the population, a long-term consequence may be that the population starts questioning the legitimacy of government's measures. This creates a climate of suspicion, which eventually may impact the resilience of a society.*

[7] Unease. (2014). In *Merriam Webster.* Available at: http://www.merriam-webster.com/thesaurus/unease
[8] Suspicion (2014). In *Dictionary.* Available at: http://dictionary.reference.com/browse/suspicion?s=t

4.2 Secondary Insecurities and Challenges in Deploying Technologies

Function creep vs. limitations:

When developing, implementing and refining technological solutions for crisis management, the risk of function creep can be defined as the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to the potential invasion of privacy[9]. Limiting regulations, which foresee a restriction, are often implemented to counteract or minimize the risks of function creep.

> *Example: A solution that is introduced to do one thing, for example a camera for damage assessment, which is later used for other kinds of surveillance without it being legal or originally planned. Developers and crisis managers can limit or avoid function creep if they provide for a plan for the limitation of access to and use of the technology into its design.*

Applicability:

Applicability means developing crisis management tools that are relevant, useful or appropriate for the defined cause or a particular task. They must be suited to address a given situation[10]. One could say that applicability is the combination of usefulness and timeliness, and for crisis management solutions this could include both the (need for) the concrete solution and the point in time where the solution is introduced. Some tools will also need to consider their applicability in terms of law, i.e. whether legal regulation for the use of such tools already exists.

> *Example: When developing training programs for societal resilience, it is important to understand in which context this training will take place. The training will have to be applicable to societal and local contexts including, for example, the occupational and educational background, the specific composition of age, gender and culture in the targeted group.*

Misuse:

All tools and measures stand the chance of being misused and it cannot always be avoided. In the context of CM solutions this could refer to using a tool or a measure in the wrong way or for the wrong purpose[11]. The use does not have to be illegal in order for it to be defined as misuse, but, it could also refer to incorrect, unlawful or improper use, such as not complying with the data protection legislation, or with regards to function creep (cf. function creep).

> *Example: Collected data for the purpose of risk analysis can, for example, be misused for commercial purposes. This can be prevented by clarifying the purpose and the scope of the data collection and the access policies.*

New vulnerabilities:

[9] Function creep. (2014). In *Dictionary*. Available at : http://dictionary.reference.com/browse/function%20creep?s=t

[10] Applicability. (2014). In *Dictionary*. Available at. http://dictionary.reference.com/browse/applicability?s=t

[11] Misuse. (2014). In *Oxford Dictionaries*. Available at: http://www.oxforddictionaries.com/definition/english/misuse

When crisis management tools are developed and implemented, they can create new vulnerabilities for the affected individuals or groups. Vulnerability refers to the risk of being exposed to the possibility of being attacked or harmed, either physically or mentally[12].

Example: In the context of crisis management the creation of new vulnerabilities for citizens can typically include the collection of data, which creates a new asset for people who use this information for purposes other than crisis management. Another example is the creation of technology dependency (cf. Technology Dependency), which always also creates new vulnerabilities.

Technology Dependency:

Advances in technology development in various fields, including crisis management, can result in technological solutions that individuals become highly dependent on and thus they can create insecurities when these solutions are unavailable, or simply by knowing that these could become unavailable. Technology dependency relates to the diminished capacity of an individual or group to anticipate, cope with, resist and recover from the impact of a natural or man-made hazard[13] without a given technology.

Example: Creating technology dependency in terms of crisis management solutions can have both positive and negative effects. On the one hand, the dependency can in fact improve the quality of life for individuals, by providing new and effective solutions to their challenges. On the other hand, the increased reliance on technologies can create vulnerabilities as crisis management becomes dependent on solutions which create new vulnerabilities. One example is the increasing reliance on internet-based technologies for CM, while connectivity may be disrupted during crises. To counteract this risk, it is important to plan for backup-solutions, such as alternative analogue communication tools.

4.3 Secondary Insecurities and Challenges in Terms of Legality

Legality/ Legitimacy:

A central rule that forms a baseline for all activity within DRIVER is the principle of legality. This refers to an attachment to, or an observance of law, and the quality or state of being in accordance with the law[14]. This includes that the development of crisis management solutions and tools can only happen according to the relevant legal regulations in the given conditions and the context. Legitimacy refers to the acceptance of law and measures and various levels of legitimacy influences whether the law serves the intended purpose or not.

Example: As research has shown, an increasing amount of UAVs are currently being used for CM even though the regulative basis for the deployment of UAVs has not been fully developed

[12] Vulnerable. (2014). In *Oxford Dictionaries.* Available at : http://www.oxforddictionaries.com/definition/english/vulnerable?q=vulnerabilities+#vulnerable__7

[13] International Federation of Red Cross and Red Crescent Societies (2014). *What is vulnerability?* Available at : https://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/what-is-a-disaster/what-is-vulnerability/

[14] Legality (2014). In *Oxford Dictionaries*. Available at: http://www.oxforddictionaries.com/definition/english/legality

yet and varies in different countries and legislations. Infringements upon this regulation have become known, for example when the Federal Emergency Management Agency in the US (FEMA) grounded drones deployed by the company Falcon for damage assessments after the Colorado Floods[15]. Even though the society and Falcon could have considered this use as legitimate - given the crisis situation - the use was not legal.

Truthfulness:

Closely related to other issues that could pose secondary challenges for crisis management solutions, such as accountability, legality and legitimacy, truthfulness refers to the fact of consistently being honest and telling the truth, by containing or expressing the truth, which also includes acting truthfully[16].

Example: Truthfulness can, for example, be of particular importance when communicating a threat level or a certain crisis management solution to the affected population. Truthfulness also includes a decision about what should be in- or excluded from a communication of threats. Even though the communication of threats does not always require complete openness (a lot of information is confidential), any given information to the public should be truthful in the sense that it should be balanced and not allow society to draw potentially false conclusions.

4.4 Socio-Economic Secondary Insecurities and Challenges

Efficiency & Effectiveness:

Crisis management tools and measures will function differently in different conditions and contexts. The state or quality of being efficient[17] refers to both economic and practical efficiency of crisis management tools. In this context, effectiveness would be the degree to which something is successful in producing a desired result / success. Efficiency refers to how fast and how thorough it produces these results. Given the urgency of the crisis management context, effectiveness and efficiency should be a given of each CM solution, something that DRIVER wants to achieve.

Example: The achieved efficiency of a certain crisis management tool or procedure is affected by several issues, such as administrative applicability (cf. applicability) and the context to which it is being introduced or implemented.

Impacts on Market (production, consumption, innovation):

Crisis management activities can include secondary insecurities and challenges related to the market. When a crisis management tool or measure is developed and implemented it can have implications for the market in which it is being integrated. This can happen either as a result of presenting a new solution and thus by filling a gap in the market, or because it outperforms other available solutions.

[15] http://www.falconunmanned.com/falcon-uav-news/2013/9/14/-falcon-uav-supports-colorado-flooding-until-grounded-by-fem.html

[16] Truthfulness. In *Dictionary* (2014).

[17] Efficiency. (2014). In *Oxford Dictionaries*. Available at: http://www.oxforddictionaries.com/definition/english/efficiency?q=Efficiency+

Example: If a crisis management solution is a technological product targeted at the broader population, it can on the one hand create market opportunities by stimulating consumption among a certain population, but it can also exclude other groups which are not able to take advantage of it.

Economic Stability:

The economic stability both within European states and in Europe as a whole influences the introduction and implementation of (new) crisis management solutions. Economic stability refers to the absence of excessive fluctuations in the macro economy[18]. An economy with fairly constant output growth and low and stable inflation would be considered economically stable. Economic stability is usually seen as a desirable state for a developed country that is often encouraged by the policies and actions of its central bank[19], but which could also, in a smaller scale, be influenced by minor changes in the market, such as influential new products.

Example: When developing sustainable crisis management solutions, a sound economic model is of relevance, which could include information on the current economic situation in Europe and expected economic developments, as well as potential side-effects such a solution may produce on the economic stability of the diverse countries.

Employment:

Employment refers to the state of having paid work, but could also refer to the action of giving work to someone or to a person's trade or profession. Developing and deploying crisis management solutions, tools or measures, may on the one hand require labour forces or on the other hand replace existing labour forces. These changes can affect the market as a whole, a certain industry, or an individual company.

Example: It is to be taken into account whether specific technological solutions for CM replace existing work forces and their employment situation, producing side-effects for individual people, for companies and organizations or even the market as a whole.

[18] International Monetary Fund. (2014). *How the IMF Promotes Global Economic Stability*. Available at: http://www.imf.org/External/np/exr/facts/globstab.htm

[19] Economic stability. (2014). In *Business Dictionary*. Available at: http://www.businessdictionary.com/definition/economic-stability.html

5 Assessments and Recommendations

All assessments are formulated for the *subcategories of measures and tools* described above. The introduction of each assessment consists of a short description of the category's relevance for CM in general, and then points to the specific relevance for DRIVER tools and measures by giving some example tasks. This introduction generally also points out if there is a group that is specifically addressed by this measure or tool in order to specify the context of the assessments. The introduction is followed by the assessments of the relevant criteria. The impact on each criterion is described in one or two sentences and – if available - borrows examples from relevant fields of CM. They describe potential negative impacts that could either be expected direct consequences of a measure or effects that have been discussed in relevant news, academic papers, research projects or operational reports. References, where available, can be found in the footnotes. Each chapter gives an additional example that speaks to the specific DRIVER context to illustrate why the criteria need to be taken account of during the development of DRIVER measures and tools. The assessment ends with a set of recommendations, which are formulated as concrete suggestions that should be followed when developing and implementing tools and methods within DRIVER. They can also serve as inspiration for the development of CM tools and measures in general.

Overall, it is important to note two points: Since the criteria assessments could be boundless, this deliverable does not claim to be complete. In order to be useful and practical, it is limited to the assessments of those key criteria which are relevant for each DRIVER subcategory.

The authors are fully aware that *each measure and tool may have both a positive and a negative effect* on its addressees. This means that the measures and tools under discussion can have at the same time a positive impact on the same criterion. Positive impacts, however, are discussed in 93.1 and 93.2. It is also important to note that some aspects discussed here as negative effects can also be politically desired. Unease, for example, can also be intentionally utilized to create a positive state of alertness. Or, the usage of one technology for several purposes can in some cases be a *function creep*, a negative side-effect, and in some cases a desired effect. Since this deliverable focuses on negative effects of CM, it points to those side-effects that are *disproportionate* and those developments that are not openly reflected upon. It should also help developers to reflect on their work and to be aware of potential negative effects in order to be enabled to make an informed decision on its desirability.

The recommendations in this deliverable are thus to be read as advice against potential pitfalls, as general guidelines and principles to avoid disproportionate effects of secondary insecurities. The deliverable provides examples and guidelines for each responsible task leader to conduct societal cost-benefit-analyses about the potential impacts of the measure or tool that he or she is developing.

An overview of all relevant criteria per subcategory can be found in annex 1.

5.1 Data & Information

5.1.1 Collection & Storage

Related WP and Tasks: 36.3, 43.1, 43.2, 43.4, 45.2, 45.3, 45.4, 52.4, 53.2, 55.3, 55.4.

Data collection is unavoidable for the development and deployment of many CM solutions, since, for example, identifying gaps and discussing lessons learned requires data records. The tools and measures developed and deployed in DRIVER collect and store data from different actors and in different ways, for example through airborne sensors (43.2) and through smart-phone applications (55.1). The collection and storage of data in DRIVER varies from tools collecting data from professionals and the population in the field (43.1) to solutions that use citizens as sensors (36.3). Collection and storage needs to fulfil certain requirements to avoid creating secondary insecurities and challenges. Data protection laws differ also within the EU, but the common aim is to protect the values and interests of the data subject, such as privacy.[20] Data can be stored on paper, electronically or computer-based e.g. through cloud computing solutions, hard drives or memory sticks.

Function Creep, Misuse, New Vulnerabilities, and Legality: Not setting up limitations for the access and use of data (via encryption or password protection) increases the risk of function creep and also misuse of the collected data. The (large scale) storage of digital data can also create new vulnerabilities, as the data risks being hacked or illegally accessed. This vulnerability can happen by a breach of legality[21] such as local data protection law, which can lead to misuse of data or illegal access to data.

Unease and suspicion: The risk for data misuse needs to be actively counteracted. Otherwise, it can create unease or suspicion regarding the integrity of the data collector, should the population find out that their personal data is being illegally accessed or unrightfully reused through a CM tool or measure. Not informing the affected individuals about the predefined purpose for the collection and storage of personal data can lead to suspicion or unease which can even lead to a distrustful relationship with the population as they could feel unnecessarily controlled without clear reason (e.g. a risk in 43.2). One example of unlawful collection and storage of data is the NSA bulk collection of phone data in the USA.[22]

Applicability, Technology Dependency and Efficiency: There is also a risk that the data that is being collected is not applicable to the case at stake, meaning that the data collection can derive from imprecise or wrong variables or criteria, or that other methods for data collection would be better fitted to the cause. This can produce skewed results or data that is not appropriate for the task, which could make the CM tool or measure inefficient. This can also be caused by developing technology dependency, in the way that the technology we choose for a certain task in reality determines what kind of data is collected.

> *Example: 43.2 will use airborne sensors during CM activities, which necessarily imply the collection and storage of data. If the data collection and storage does not set limitations for the access to the gathered data, there is a risk that the data can be misused through a*

[20] Bygrave, L. (2002): Data protection law. Approaching its rationale, logic and limits. Great Britain. Anthony Rowe Limited.

[22] Ackerman, s. & Dan Roberts (2014) : «US government board says NSA bulk collection of phone data is illegal» in The Guardian. Available at: http://www.theguardian.com/world/2014/jan/23/nsa-barack-obama-phone-data-collection-illegal-privacy-board

[22] Ackerman, s. & Dan Roberts (2014) : «US government board says NSA bulk collection of phone data is illegal» in The Guardian. Available at: http://www.theguardian.com/world/2014/jan/23/nsa-barack-obama-phone-data-collection-illegal-privacy-board

potential function creep. Data collection also risks being an inefficient tool, as the variables for the selection can be chosen on the wrong assumptions.

Recommendations:

- The collection, storing and processing of data and information facilitated by developed DRIVER tools needs to uphold the data protection regulations to protect the data subject's privacy. This can be potentially challenging, especially regarding new technology and unexplored legal fields. Local Data Protection Authorities should be consulted when necessary.
- Make sure to only collect the data you need for the predefined purpose and do not reuse collected data uncritically.
- Do not store data for longer than necessary, and ensure safeguards when it comes to the technical and physical access to the data.
- Account for the applicability of the data collection methodologies and reflect upon the fact that some technologies and processes can be limiting, as they influence what data can be collected. Consider the necessity of the collection itself and evaluate other options to data collection, especially to intrusive data collection.

See also (sub)categories: Communication Systems;

5.1.2 Facilitating Data Processing

Related WP and Tasks: 43.5

The facilitation of data processing is different from the collection and storage of data, since the aim is to create, bridge or join systems of data processing. Working together and exchanging data is often crucial in CM. Here, the question is what practical impacts can cause the processing? Technology itself can be seen as a facilitator for data processing. Within DRIVER, the facilitation of data processing refers to, for example, tools or methods facilitating interoperability, such as methods for improving the situational awareness by integrating information from different agencies and professionals (43.5).

Technology Dependency: Data processing can be hindered by traits of the data processing tools, for example, if they are not designed to cope with the amount of data that are fed into them. Facilitating the expansion of databases can create a technology dependency, as, for example, merged databases require oversight and other forms of control that can be hard to manage manually.

New Vulnerabilities, Misuse, and Legality: New vulnerabilities can be caused by expanding databases in the population,[23] thus, increasing the risk of hacking. For example, facilitating the

[23] See for example Rosenblatt, A., & Attkinsson, C. C. (1992). Integrating systems of care in California for youth with severe emotional disturbance. I. A descriptive overview of the California AB377 evaluation project. Journal of Child and Family Studies, 1(1), 93-113. This article illustrates how the administration of databases and in particular the variables chosen to process the data in them, potentially can create vulnerabilities through facilitating e.g. discriminatory practises.

conjoining of data can influence the possibility for misuse or illegal use of data, simply because the quantity and quality of data changes once merged.

Function Creep: This increased complexity of the databases can also increase the risk for function creep, as the data could be seen as useful in new/ additional areas. The general development of new technology is inhabited with risks, and this also goes for CM tools. For example, although the modern society increasingly relies on digitalized solutions, this increase in the amount of data being collected is not in itself negative, but on a general level this development can make societies depend on new forms of technology inhabited by new (and also unknown) dangers and risks.

Legality, Effectiveness and Efficiency: If the legal requirements for facilitating data processing are not upheld, it can influence the applicability and effectiveness of the measure, for example, by complicating deployment. Efficiency can also be hindered, for example, by lack of harmonization when merging databases.

> *Example: In 43.5, the aim is to improve situation awareness by integrating and facilitating the processing of information from different sources (such as the use of mobile devices in the field) and on different levels. This requires attention to the regulation of the new database. As the case is in 43.5, the merging of data from different sources can challenge the legality of the CM tools for example, if the regulative landscape is not up to speed with new data collection methods used (which, for example, is the case for the use of drones in Norway), if the CM tools are challenged by the amount of data that is being processed, or if the facilitating mechanisms are not those best suited for the job.*

Recommendations:

- When designing the measures that lead to the processing of data, and to ensure the efficiency of the procedure, a risk or impact assessment can minimize secondary insecurities and challenges like function creep and the creation of new vulnerabilities by setting limits for the use of the data.
- When planning CM measures prepare and test the efficiency and applicability of the mechanisms, the need for processing data in that scale, and reflect upon whether the action is leaving you more vulnerable by creating more technology dependency. Minimize data processing wherever possible.
- Planning- and impact assessments can verify whether the facilitating mechanisms introduced are timely and useful or whether they could hamper its applicability and effectiveness.
- The facilitation of data processing largely falls under the general rules for data protection and should adhere to the basic principle of legality.

See also (sub)categories: no related subcategories

5.1.3 Analysis & Evaluation

Related WP and Tasks: 36.3, 43.1, 43.2, 43.3, 43.5, 52.4, 53.2, 55.4.

Data analysis and evaluation is crucial for CM, as it provides the very basis for learning and developing new solutions for CM. To process data can mean to handle, alter, treat or refine data. Various kinds of data and information are being processed throughout DRIVER tools. This happens, for example, in relation to data collection through an airborne sensor suite that includes an on-board processing system and a direct data link from airborne platform to ground (43.2).

Legality and Unease: If the data processing and analysis tools do not uphold principles of legality, they can seriously jeopardize the project and create unease particularly to the data subjects, because their data risks being misused or not treated according to the agreement.

Suspicion: If the data controller does not fulfil its legal responsibility to ensure that the data and information is treated according to the relevant data protection legislation,[24] the data subjects (whether they are the population, professionals, tool developers or volunteers) can feel suspicion or unease about their privacy rights being hindered (such as the right to access your data).

Misuse: If limitations for data access are not set, the data risks being misused by someone obtaining illegal access to it, which can also create further unease among the affected individuals if they were made aware of unlawful or unrightful data processing.

Function Creep: The data analyst has an individual responsibility for maintaining information security with regard to confidentiality, integrity and accessibility. However, should the data processor not process the personal data according to a predefined agreement and purpose, it can include a risk of function creep, since the data could be reused for purposes that it was not intended to fulfil, without the consent of the data subject. This can cause unease and suspicion that can potentially influence the integrity of the data controller.

> *Example: In 43.2, the aim is to improve airborne sensor capabilities, for example through testing the usage of mobile sensors within a flood scenario. The use of such technology will include the processing of data, such as information from geo-referencing. A challenge here can be that legislation of this kind of data is not well developed in many European countries because this technology or method does not have a long tradition within civil sector use.*

Recommendations:

- Analysis of data and information needs to have a predefined purpose and happen according to data protection legislation in the country where the data collection is happening.
- Make sure that the data analysis is necessary and proportional to the case and ensure that the data subjects are informed in advance, if possible.
- Personal data shall not be further processed or reused in any way incompatible with the predefined purpose.
- The data analysis needs to adhere to processing standards that make the output legally usable. Task 85.3 will act as a legal and regulatory advisor to the DRIVER project, and the ethical procedures, risks and safeguards for responsible research (including, but not limited to SC15), can be found in D91.3.

[24] In Norway e.g., the relevant legislation is the Personal Data Act of 2000, but the most local legislation and the one closest to the data collection itself should be consulted.

See also (sub)categories: - no related subcategories

5.1.4 Exchange

Related WP and Tasks: 36.3, 43.1, 43.2, 43.3, 43.5, 52.4, 53.2, 55.4, 36.3.

The exchange of data is important to increase efficiency and effectiveness as well as to strengthen collaboration in the area of CM between different stakeholders. It implies mutual trust and can be beneficial to all partners. Data exchange between different actors happens on multiple occasions within a CM scenario, and is a necessary and common activity in many areas of technology development and deployment. This is, for example, the case in WP45 where the aim is to tear down the barriers of information exchange within the responders' community at all levels. This necessarily requires data or information exchange. Exchange of data and information can be informal (45.2) and a valuable method for knowledge production, development of tools or measures, sharing of experiences, or finding new solutions for old challenges. However the process can be said to be dual-edged, as it can create both positive and negative side effects. This duality is explicitly referred to within DRIVER in 45.4, where the interconnection of communication systems (the first responders "system of the systems") is being analysed in order to clarify threats and opportunities connected to the use of such systems.

Function Creep: Data exchange can increase the risk of function creep, especially if the data being exchanged consists of (partly) unnecessary data. New or other uses could be found for the data, which were not initially intended.

Misuse: Misuse can happen as exchanging data diffuses the information and makes it less easy to control and regulate. Exchange can potentially challenge the legal regulations when it comes to cross-border exchange.

Suspicion: Suspicion as to why individual's personal data needs to be shared can rise if the exchange of information does not seem like the best or most obvious solution for the task at hand.

Truthfulness and Unease: If the process of data exchange does not adhere to the principles of transparency and truthfulness, it can create feelings of suspicion or unease, for example, among individuals being made aware that their data is being shared without a good reason or as per predefined agreements. This is especially important in a social and political climate that is increasingly concerned with issues of privacy.

Legality and Misuse: When data and information is exchanged between one partner, system or database, to another, the risk of misuse arises if the exchange is not well regulated, for example by legally and practically regulating access to the databases. A breach in information security in the data exchange could open up access to potentially sensitive data (such as geo-locations from UAVs), which is illegal according to data protection legislation. As the technical infrastructure and the complexity of the database increases once exchanged or merged, handling it correctly and properly becomes increasingly important. A breach of some kind could potentially have more substantial impact as the consequences would reach out to more people (e.g. the data subjects whose data is contained in the databases).

Efficiency: If the data exchange does not happen securely (secured interoperability is addressed for example in WP45), including regulating the retention of data, the risk for misuse increases because the data is not well enough protected, and the risk for inefficiency increases because the governing of the database becomes more difficult.

> *Example: In 36.3, the aim is to use existing software to organize volunteers by using citizens as sensors by means of a crowd tasking solution. As this will necessitate an exchange of data in order for a crowd tasking solution to be possible, there is a potential that legal challenges caused by uncompliant legal frameworks can arise if the exchange happens cross-border. Also, there is a risk that the data gathered and exchanged through such a tool will be seen as useful, e.g. for developing other tools, which would risk reusing and thereby misusing the data.*

Recommendations:

- Do not exchange data unless it is deemed the best solution.
- Minimizing data exchange can also automatically minimize the risk of misuse of the data, simply as less people will be able to access it. Unnecessary data exchange should be avoided to minimize the risk of function creep**.**
- Data exchange should happen only after a critical evaluation of the receiver and after ensuring that the receiver upholds standard routines and regulations for processing the exchanged data. This is particularly important when exchanging data with third countries.
- Data and information exchange needs to happen within the legal frames and adhere to the principles of proportionality, necessity, applicability and transparency.
- The rules for data protection need to be carefully upheld in order to limit or prevent potential misuse of the information and to ensure an effective process.
- When connecting or conjoining systems, the risks and threats need to be evaluated to minimize misuse and function creep.
- Solutions for encryption should be considered.
- Access to the databases must be limited both practically and legally. This means that the very process and principle of exchanging information and data needs to be deemed the best solution for the issues at stake, a reflection which would include evaluating the applicability and effectiveness of the data exchange.

See also (sub)categories: Situational Analysis & Impact Assessments, Mapping; Communication Systems;

5.2 Risk, Damage and Needs Assessment

5.2.1 Gap Analysis

Related WP and Tasks: 34.1, 52.2, 53.1

In general, gap analysis is a method for deciding where the effort should be spent, and in CM this can include analysing where mistakes have been made in the past and where more attention is needed. The analysis of gaps is one aspect of different tasks within DRIVER. They include self-assessments

conducted by organizations to understand gaps in crisis management (34.1), identification of gaps in competence (52.2), as well as in systems to enhance lessons learned (53.1). These tasks mainly address professionals and volunteers, which is why societal impacts are likely to appear only indirectly.

Unease and Efficiency: While the identification of gaps is generally useful to reduce vulnerabilities and enhance the effectiveness of CM, the difficulty is to determine at what point the most crucial gaps are identified. Since the amount of gaps in need of management can be boundless, it is important not to over-engineer crisis-management, regulating any possible aspect of it, since that may cause inefficiency or even unease as a side effect. [25]

Applicability: The particular strategy used to identify gaps needs to be tested with regards to its goals. The identification of gaps is highly dependent on the focus and the variables chosen to conduct the analysis, meaning that they are prone to 'produce the results that you are looking for', which may easily result in a skewed analysis.

Misuse: Even though gap analysis may follow strict strategies, they may also be misused for political or commercial agenda setting, meaning that key actors may push analyses to cover specific gaps that mainly serve a particular political or commercial purpose.

New Vulnerabilities: Although gap analyses are generally aimed at reducing vulnerabilities, labelling a gap as such also defines it at the same time as something vulnerable. It is thus important to compare and contrast identified gaps with vulnerability analyses to avoid creating pseudo-vulnerabilities only by labelling them as a gap. The communication of gaps also draws attention to potential vulnerabilities that can become targets for individuals with malevolent intentions.

Legality: The identification of gaps is based on a vast variety of information and information sources. In particular knowledge connected to infrastructures and private companies may be confidential and private. The collection of data to identify gaps has to be in accordance with the law.

Efficiency, Impacts on the Market: A focus on gaps that are not necessarily crucial to be covered may produce unnecessary costs for specific companies and infrastructure providers, both in terms of providing the additional technologies or solutions. As such, some gap analyses risk being inefficient, producing detrimental impacts on the market.

> *Example: If organizations conduct self-assessments to identify general gaps in CM, these self-assessments are informed by the views on CM and the products and services that exist within that organization. As such, they may risk identifying only the gaps they are looking for or to misuse the gap analysis to place a specific agenda that may serve a political or commercial purpose rather than CM as a whole.*

Recommendations:

- In order to confine the analysis, the current and the end state of the field to be analysed have to be described clearly and before the gap assessment is conducted.
- When conducting the analysis, use a broad variety of data sources to avoid producing skewed results.
- Comply with data protection regulations.

[25] Aradau C and van R Munster (2011) The Politics of Catastrophe. London> Routledge

- From the various gaps you will reveal, identify only the *key gaps* to be covered to avoid over-engineering CM.
- Communicate about gaps carefully as they also point to a vulnerability that can be exploited.
- All measures to fill newly identified gaps have to be reflected upon with regards to their potential for political and commercial misuse.

See also (sub)categories: Data & Information;

5.2.2 Situational Analysis & Impact Assessment

Related WP and Tasks: 43.2, 43.4, 43.5, 44.2

Situational analysis and impact assessments are important tools to prepare CM decision-making and plan effective response. Within DRIVER, such assessments are conducted to identify damages and needs through mobile applications (43.1), airborne sensors (43.2), via social media and crowd-tasking (43.4) and by integrating information from different agencies and dimensions (43.5). This category also includes the assessments and mapping of actions undertaken by responders (44.2). Most measures and tools are directed at both professionals and the population as such, which emphasizes the necessity for careful evaluation of secondary effects.

Unease, Suspicion: Since the use of unmanned aerial vehicles (UAV) is not yet the norm and mainly known from a military context, the deployment of airborne sensors mounted on UAVs may cause unease within the population, if the population does not know what the vehicles are being used for. The population may furthermore feel disproportionate unease by being watched, which creates a climate of suspicion between the population and those who deploy airborne sensors.[26] A similar climate of unease and suspicion may occur if the usage of data from social media is not explained well enough by those who collect it.[27] If people feel looked at while accessing their social media, they may stop using them.

Function Creep: Any novel technology, such as airborne sensors, or any novel method to collect data from social media or via apps, which are originally developed for the context of crisis management, easily opens up for function creep. They can be used for purposes other than crisis management, for example, commercial, but also – especially in the context of UAVs – military or other political usage.[28]

[26] The Peace Research Institute Oslo and the Norwegian Board of Technology hosted a workshop on the 7th of March 2013, discussing whether drones could and should be used in search and rescue operations in Norway. This workshop, developed in cooperation with the Norwegian Red Cross, involved over 25 experts from fields such as military and defense, law, ethics and fundamental rights, technology and emergency management. It was part of the FP7-funded DESSI project (Decision Support on Security Investment). Gogarty and Hagger write that although UAVs "have begun to transition to the civilian sector they still retain many of their military characteristics." (2008: 144). The same problem is touched upon by the OCHA report, pointing out that humanitarian organizations wish not be associated with military technology https://docs.unocha.org/sites/dms/Documents/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf, p. 9

[27] Kaufmann M (forthcoming 2015). Resilience 2.0. Media Culture and Society.

[28] Kaufmann M (forthcoming 2015) Drone/Body. In: Sandvik and Jumbert (eds) The Good Drone. Ashgate.

Applicability and truthfulness: Especially when gathering data from social media, there may be more methods, devices or ways to get this information. It is thus important to check whether the method chosen is really applicable in the given context and whether the method may not open up the circulation of invalid information, meaning that it may also cause results that do not reflect the truth – or do not reflect the truth in a meaningful way vis-à-vis its purpose.[29]

Misuse and Efficiency: Using social media and apps to collect data for situational awareness is prone to misuse by both those who collect and those who provide data. Efforts need to be spent to distinguish deceptive from correct information that is circulated via apps or social media after crises, which impacts on efficiency. If those who collect data use the collected data or even the technology itself for purposes other than originally indicated, this information is also being misused.[30]

New Vulnerabilities and Misuse: Data collected via airborne sensors, social media or apps may not only create new vulnerabilities vis-a-vis the privacy[31] of the data owners, but also the aggregated data that is used to identify vulnerabilities, needs and requirements can be hacked and misused by malevolent parties.[32] As such, the creation of datasets always implies its own vulnerabilities. **Technology Dependency**: In case data collected from airborne sensors or apps become the norm, such measures and methods do create technology dependencies, meaning that when they fail, little alternative options for doing situational assessments are available, which again impacts on efficiency and effectiveness. A broad variety of situational analysis tools and methods is thus necessary. **Legality:** In particular the use of airborne sensors is not consistently regulated throughout Europe. It is important to verify how the use of airborne sensors is regulated in the country of application and whether the use conforms to this legislation before the actual application during CM will take place.[33]

Efficiency & Effectiveness: The tasks 43.1-5 mainly suggest methods for data collection. In order for those methods and tools to be efficient and effective, they also need to include meaningful methods for data analysis. Big data, however is not always better data[34] and in some cases a considerable amount of work force is needed to analyse this data, which may infringe upon the efficiency of the measure.

[29] Cf. research on social media research methods and the selection of variables by Steve Pickering, Kobe University; Boyd D and K Crawford (2012) Critical Questions for Big Data. Information, Communication and Society 15(5) : 662-679 ; Kaufmann M (forthcoming 2015). Resilience 2.0. Media Culture and Society.

[30] Andrejevic M and K Gates(2014) Big Data Surveillance : Introduction. Surveillance and Society 12(2) : 185-196. Boyd D and K Crawford (2012) Critical Questions for Big Data. Information, Communication and Society 15(5) : 662-679. Kaufmann M (forthcoming 2015). Resilience 2.0. Media Culture and Society.

[31] http://www.theguardian.com/technology/2014/jun/20/little-privacy-in-the-age-of-big-data; Gonzalez Fuster Gloria, Bellanova Rocco (2013) European Data Protection and the Haunting Presence of Privacy. NovATIca, from 2012/2013 Annual Selection of Articles, issue Privacy and New Technologies, pp.17 - 22.

[32] http://www2.warwick.ac.uk/fac/cross_fac/cim/research/socialising-big-data/

[33] Gogarty, Brendan and Meredith Hagger (2008) The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air. Journal of Law, Information and Science 19 (1): 73-145. ; Rutkin, Aviva (2014) Drone law: Flying into a legal twilight zone. http://www.newscientist.com/article/mg22229694.400-drone-law-flying-into-a-legal-twilight-zone.html#.VACCfDKSx8F

[34] Boyd D and K Crawford (2012) Critical Questions for Big Data. Information, Communication and Society 15(5) : 662-679

Example: Collecting information via airborne sensors, apps or social media may lead to unease for those who are directly targeted by the measures, mostly because they may feel watched. The selected methods to collect and analyse data may furthermore allow for misuse, function creep and may produce skewed results, since especially crowd-tasked information is prone to misuse or the circulation of deceptive information. Datasets created via these methods may be useful, but they also create new vulnerabilities, because they can be hacked.

Recommendations:

- Make sure to clearly define the scope of the data that is supposed to be collected via airborne sensors, social media or apps. Clearly mark these methods and tools as something that belongs to the crisis management context, for example by marking UAVs with the logo of the organization that uses them.
- Adhere to data protection legislation and communicate clearly that you will not misuse personal data. This can be done by issuing information pages and informed consent forms for those who share data online - even if that happens voluntarily.
- Ensure that effective ways for analysing big data are in place, which do not infringe upon the data provider's privacy or produce skewed results.
- Establish mechanisms that help verifying the truthfulness of information without increasing the amount of overall surveillance.
- Make sure that alternative methods for situational assessment are in place to avoid technology dependency.

See also (sub)categories: Data & Information;

5.2.3 Early Warning, Risk Analysis & Forecasting

Related WP and Tasks: 43.1, 43.3, 44.1

Within CM, risk assessments play an important part in the situational analysis to enhance preparedness and reaction and to ensure the effective use of resources. Within DRIVER, this is reflected in both 43.1 and 44.1 for example. Risk and early warning are integral aspects for assessing crisis dynamics and approaching hazards (43.3). Because risk and early warning systems have always been important technologies within crisis management, their secondary impacts are also well-explored, especially when it comes to their implementation.[35] This section focuses on the way in which risk assessments and public warnings may cause *general* negative effects on society when they are being *implemented*. For advice on strategy design and methodological aspects of risk assessments check section 6.1.2.

[35] Furedi, Frank (2006) The Culture of Fear Revisited. London: Continuum. Jaeger, C; Renn, O, Rosa Eugene A, Webler, Thomas (2006): Risk, Uncertainty and Rational Action. London: Earthscan. Baker, Tom and Simon, Jonathan (2002) Embracing Risk. The Changing Culture of Insurance and Responsibility. Chicago: The University of Chicago Press.

Unease and Effectiveness: Issuing early warnings may easily cause unease, especially when they are medially over-represented and come without concrete advice for the population. The 2014 terror-warnings in Norway caused a broad societal discussion about the way in which the warnings caused feelings of insecurity in the population.[36] Risk assessments may, if deployed in any field of crisis management, also contribute to a constant feeling of possible insecurity.[37] Even if early warnings are efficiently implemented, they may have detrimental impacts on effectiveness if the warnings result in panic within the population.[38]

Suspicion: Not all risk assessments target a specific group or population, but if they do, as is often the case with Muslim extremists, they risk creating a feeling of suspicion towards a broader societal group entailing various other negative consequences.[39]

Misuse: Early warnings, especially if they are made public, can also bear the potential for misuse, since they can serve as instruments, for example, to place a specific political agenda within the public and/or facilitating the implementation of specific political measures.

New Vulnerabilities: The public communication of risk assessments through early warnings can cause new vulnerabilities if weaknesses are identified by individuals with malicious intentions.[40]

Impacts on Market: As a result of public warnings consumption of specific goods and services, for example the avoidance of public transport or other public services during an emergency alert, may be impacted in unintended ways since they are often profiled as potential hot spots or targets.[41]

Economic Stability: In particular cases, it can happen that public risk assessments and early warnings impact the stock exchange and thus market behaviour, which creates economic instability within specific domains, especially those domains that are expected to be hit by potential disasters.

> *Example: A warning that is not well-planned and that over-emphasizes risk within the public domain may not only cause unease, but may change the consumption of specific services or cause instabilities in the market, e.g. of/for companies in the potentially affected region.*

Recommendations:

---

[36] http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-terrortrussel-7650037.html; http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-terrortrussel-7650037.html; http://klassekampen.no/article/20140728/ARTICLE/140729963; http://morgenbladet.no/samfunn/2014/et_glimt_av_usa#.VCLQI_mSx8E; http://www.jstor.org/discover/10.2307/30000168?uid=32605&uid=3738744&uid=32604&uid=2&uid=3&uid=5909240&uid=67&uid=62&sid=21104745263583http://www.dagsavisen.no/samfunn/krisepsykolog-advarer-mot-overdreven-frykt/

[37] Hagmann J and M Dunn Cavelty (2012) National risk registers: Security scientism and the propagation of permanent insecurity. Security Dialogue 43(1) 79–96.

[38] http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-terrortrussel-7650037.html; http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-terrortrussel-7650037.html; http://klassekampen.no/article/20140728/ARTICLE/140729963; http://morgenbladet.no/samfunn/2014/et_glimt_av_usa#.VCLQI_mSx8E;

[39] Kaufmann (2010) Ethic Profiling and Counter-Terrorism.

[40] http://www.jstor.org/discover/10.2307/30000168?uid=32605&uid=3738744&uid=32604&uid=2&uid=3&uid=5909240&uid=67&uid=62&sid=21104745263583

[41] http://metro.co.uk/2014/09/01/text-that-warned-of-terror-attack-on-london-underground-branded-a-hoax-by-police-4852485/

- Contemplate the secondary effects that a public warning may generate, be as clear as you can in formulating the message.
- Include concrete advice for professionals, volunteers and citizens to avoid confusion or panic.
- Avoid generalizations vis-à-vis specific societal groups to lower the general level of suspicion such assessments can cause.

See also (sub)categories: Situational Analysis & Impact Assessments, Mapping; Communication between crisis managers and to the public;

5.2.4 Communication Systems

Related WP and Tasks: 45.2, 45.3, 45.4.

Communication technologies play a crucial role during crisis. Professionals and especially first responders need to be in constant communication and exchange data and information through secured and interoperable systems to ensure an appropriate response. The field of communication technologies develops rapidly. Systems are continually being introduced and the new mass-market devices enable the participation of the general public in crisis response with different results. Within DRIVER WP45 will focus on secured interoperability tools aimed at improving information exchange within the responder's community. Specifically Task 45.4 will assess the risks and opportunities of the use of existing and planned communication systems (i.e. GSM, TETRA, TETRA3); the interconnection with other systems; and the use of mass-market devices (i.e. smart-phones, tablets). Professionals and tool developers involved in these tasks need to take into consideration that the analysis of existing communication tools, as well as the design and implementation of the guidelines to use them, can indirectly create secondary insecurities and challenges.

Legality: As explained in the section devoted to Data and Information, the exchange of data and information through communication tools can infringe upon legal requirements for data collection, storage and protection. Especially if the communication is meant to happen across countries, there might be legal vacuums or a lack of harmonized European legislation in regards of data exchange.

Function Creep and Misuse: The use of mass-market devices is especially prone to the misuse of data for purposes other than CM (economic, political, or security related).

New vulnerabilities and Technology Dependency: Especially in the absence of legal frameworks, new vulnerabilities can be created by relying on communication tools that can be hacked for information about, vulnerable infrastructure, distribution or resources in a supply chain, etc. A dependency on a technology that might fail during a crisis creates vulnerabilities, especially if alternatives to these tools do not exist. For example, to rely only on smartphones makes a communication system vulnerable if the GSM technology fails during a crisis.

Applicability: If high standards for interoperability of new technologies are not met, the system may not be applicable across borders.

Efficiency: The introduction of latest software will require constant investments in upgrading exercises (i.e. from 3G to 4G, TETRA to TETRA3) which can compromise the efficiency of the whole system.

Example: If all communication is gathered through the TETRA system, it may create a high degree of technology dependency, which may result, in cases of failure, in new vulnerabilities. Should the development of the system not involve all related countries, it may compromise cross-border applicability.

Recommendation:

- Always have alternative plans and redundancies for communication systems available to avoid complete dependency.
- Clearly set out what the communication technology will be used for to avoid function creep and misuse.

See also (sub)categories: Exchange;

5.3 Cross-border and Cross-Sectoral Interaction

Related WP and Tasks: 33.2, 36.3, 44.2, 45.2, 45.3, 45.4, 52.2, 53.1, WP55.

In an increasingly intertwined European society, cross-border communication, interaction, networking and international collaboration is of utmost importance for CM. Networking and international collaboration are important to allow intra- and cross-border cooperation before, during and after a crisis. DRIVER includes the development of measures and tools that facilitate national and international interaction of CM partners, volunteers, professionals, institutions and the general public. Engaging and facilitating formal and informal social networks of citizens will also play an important role to ensure the participation of the general public and civil society in crisis management and thus enhance community resilience (33.2). International cross-border collaboration and networking happens through the organization of databases, tools and web-services aimed at creating collaborative tools for formal and informal exchange of information and data among professionals (45.2, 45.3), identifying competences (52.2, 52.4) and lessons learned (53.1), etc. Given the complexity of international collaboration and networking, the potential for creating secondary insecurities and challenges is high.

Unease and Suspicion: If a networking and communication systems for early warning works across borders, there is, dependent on the involved addressees, a risk of over-alerting about a (potential) crisis to wider audiences than originally intended. This may create unease or suspicion among the network partners or trigger social alarm in populations that did not need to be addressed.

Efficiency & Effectiveness: Oversight and control over the networks/collaborations are on the one hand necessary but can, on the other hand, add even more complexity and lead to concerns about efficiency and effectiveness**.** Oversight and control mechanisms are both costly and can slow down the whole collaboration process.

New Vulnerabilities, Misuse and Function Creep: Big networks and collaborations can compromise transparency, which can create secondary vulnerabilities, for example when the origins of specific

messages are not traceable. The more data is exchanged within the network, the more vulnerable is this information to misuse and function creep and non-compliance with data protection legislation.

Misuse: The organization or institution facilitating collaboration, including the distribution of responsibilities, will be in a position of power. This creates potential for political misuse, especially with regards to economic or political agenda-setting.

New Vulnerabilities: Single countries, especially low-income countries, might find it difficult to adjust to new frameworks, which could create new vulnerabilities for these countries if they cannot comply with the newly established standards for CM.

Legality and Applicability: If the collaboration or networking includes data exchange, especially personal data, the principle of legality should always be upheld. The exchange should be proportional, transparent, of limited access and compliant with legislation on data protection. Cross-border data exchange might not be possible due to a potential lack of harmonized legal frameworks. Authorizations for data exchange by respective authorities should be granted before initiating any exchange of data within or across countries (cf. 95.22 ethical approvals). In addition, the more data is exchanged internationally, the more vulnerable is this information –or the software that facilitates the exchange- to misuse, function creep, and non-compliance with data protection legislation.

> *Example: The organization of international databases may cause new vulnerabilities because data protection regulations are not internationally aligned, which opens up opportunities for misuse, function creep and hackability. This requires thorough planning and mechanisms for oversight, which may not be efficient.*

Recommendations:

- Establish guidelines about which kind of messages are distributed internationally and which are confined to national or even sub-national borders to avoid the spreading of unease.
- Take into consideration that every international collaboration system has to pay attention to each country's legal regulation mechanisms for data exchange, especially to ensure interoperability and reduce local vulnerabilities.
- Take into consideration that every international collaboration system may necessitate a potentially inefficient but effective oversight-system.
- Ensure that the size does not obscure the transparency of the network. Find design-solutions that allow for transparency.

See also (sub)categories: Data and Information; Early Warning, Risks and Forecasting; Communication Systems;

5.4 Communication between crisis managers and to the public

Related WP and Tasks: 35.2., 35.3, 35.4, 36.2, 43.3, 44.3, 45.3, 45.4

Communication tools are essential, if not the most essential part in CM, for informing the public about upcoming hazards and taking appropriate measures. They are not only important for alerting the population (35.3) in the early warning phase but also in the preparation phase (35.4). Knowledge on how to address particular stakeholder groups via media can help channel the willingness of the public to help in a way that assists and does not obstruct the response. In the last years responders had to learn that spontaneous volunteers (36.2, 43.3) are not only individually converging to disaster sites but organizing themselves using social media. Thus it is important to have in place and use communication tools to organize spontaneous volunteers and direct them in the most suitable way for CM (36.3, 44.3). The impact of modern collaboration tools (45.2) on CM is noticeable on a daily basis. So any improvement in a structured information exchange (45.3) is a welcome development for CM. Furthermore in order to overcome the impacts on telecommunication infrastructure the communication in a CM scenario mostly relies on radios (45.4).

Suspicion, Misuse, and Legality: Almost everybody in the EU has at least a mobile phone. According to the experience of some DRIVER end users people often do not fear the misuse of their private data and share them rather easily. Nevertheless, to avoid suspicion, which can lead to a bad reputation and lose of trust to an organization managing the volunteers - when using web or app based solutions for informing the public and organizing and mobilizing their willingness to help - responders shall take measures to guarantee the legality and conformity of the communication tools with national and European data protection regulations.

Function Creep, Misuse: When it comes to using communication tools for coordinating spontaneous volunteers not only the issue of misuse of data but also of their manpower could arise. This can be the case when spontaneous volunteers are used for purposes other than assisting the response and the beneficiaries (e.g. refurbishing a fire station). To avoid that, a four-eye principle[42] should be put into place, ideally separating the level that a) requests b) alerts and deploys the volunteers and c) the level which gives clearance to the deployment.

Applicability: To assure the applicability – in the sense of appropriate use of volunteers - people should be able to state and freely select for which purpose they want to be contacted (e.g. preparedness information, blood donation campaign, immediate response only) and used.

Employment: Response organizations that rely on manpower may be threatened by ICT-based approaches to managing spontaneous volunteers and fear that their work force is being replaced by volunteers. In internal communication and trainings with these stakeholders it must be assured that they understand that these spontaneous volunteers will a) do either menial work in cases where lots of manpower is needed - thus freeing professional resources for more important tasks or b) provide expert knowledge that was previously uncovered.

New vulnerabilities and Technology Dependency: In particular solutions based on technology and new media may exclude whole groups of people from communication (e.g. older people, people with disabilities, people with less language proficiency). These groups may not keep up with the development of technology, lose an information channel and may therefore be more vulnerable than before. Also organizations relying only on new technologies will develop a technology dependency

[42] This principle is described as following by United Nations Industrial Development Organization : « The four-eyes principle means that a certain activity, i.e. a decision, transaction, etc., must be approved by at least two people. This controlling mechanism is used to facilitate delegation of authority and increase transparency ». Available at: http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html

that may turn them more vulnerable during crisis especially in case the crisis impacts on the communications infrastructure.

Example: Local crisis staff normally organizes itself with paper and pencil. When starting to use a collaborative tool there is no need for the paper and pencil solution and the training of analogue procedures anymore. In case of long lasting power outage – a blackout - the infrastructure for the collaborative technology might not work anymore.

Recommendations:

- Organizations should consider keeping backup procedures in the case of a failure of new technologies.
- When introducing new collaborative tools through workshops and trainings, professionals should be reassured of the benefits of these tools for their daily work and minimize a potential perception about professional workforce being replaced by volunteers or new technologies, if possible.
- Ensure conformity with European data protection regulations when organizing volunteers through any kind of tools (ICT – and non-electronic based).

See also (sub)categories: Data and Information; Communication Systems; Early Warning, Risks, Forecasting;

5.5 Other Forms of Training

5.5.1 Psychosocial

Related WP and Tasks: 32.2, 32.3, 32.4

In the past years Psychosocial Support (PSS) has come to be regarded as a necessity in CM interventions, both regarding the psychological well-being of responders as well as the affected population. Thus, the more people are trained in PSS the better the quality support the others receives (32.2). A new approach towards PSS is based on physical activity (32.2). While on a CM mission, volunteers need some kind of PSS, which starts with self-preparation (32.4).

Unease: An unbalanced application of confrontation methods or an overemphasizing on the possible psychological effects the occurrence of an incident may have such like dreams or flashbacks could lead to the appearance of these effects – purely triggered by the participation in the PSS training and not a traumatic event itself. Also if attendants of PSS-training, which have unprocessed experiences, are not properly accompanied through self-awareness parts, the occurrence of a re-traumatisation cannot be ruled out.

Function creep, applicability: Trainers in PSS may overestimate their skills and exceed their competences failing at directing participants to a qualified psychologist or psychotherapist.

Legality, employment: PSS trainings must be set up in accordance to applicable national ethical and legal regulations which may govern the provision of psychological services, such as obligation to confidentiality, obligation of documentation or labour-laws.

When a proper confinement to existing qualified offers (psychologists and psychotherapist) is missing professionals could fear that they are being replaced. Thus in the conceptualisation of PSS-programmes this must be avoided. In addition, when collecting and processing private data at PSS trainings, the informed consent of participants is needed.

Example: When adapting a training in PSS developed in and for a specific national context for a European-wide application within the Driver portfolio of tools, other national contexts substantially deferring from the original one may apply (e.g. the confinement between PSS and qualified professionals and ethical and legal regulations governing the provision of PSS are different and require special adaptation efforts).

Recommendations:

- Careful selection of PSS-Trainers to guarantee that confrontation techniques and methods of self-awareness are applied rightly and trainers do not overestimate their skills and recognise when trainees must be directed to qualified psychologist and psychotherapists, is needed.
- Proper conceptual confinement for not interfering with existing qualified professional services is essential.
- Training content and the added value of the training should be communicated with the trainees in a timely and truthful manner. Accurate information about the scope, goals, methodology of the training should be explained in advance (preferably in the invitation letter to the training).
- Having a qualified psychologist in the host organisation overseeing the development of PSS training programmes and monitoring their application can assure the proper application of the former points.
- Legal and ethical national background governing psychological support must be respected when transferring existing PSS trainings to other national contexts.
- Ensure conformity with European data protection legislation and rights and cultural customs related to privacy.

See also (sub)categories: Community Resilience**;** Data & Information;

5.5.2 Media & Policy

Related WP and Tasks: 35.2

Media contact during a crisis is highly probable. Therefore crisis communication training courses for CM professionals, public policy makers and media stakeholders (35.2) enables more effective use of media channels and the appropriate framing of messages to reach the various groups within population. When people conclude that they are at risk (by perceiving a risk or being told by authorities or the media) they are more likely to take proactive action. Empiric evidence suggests

that people take action when they think they are at risk implementing the most appropriate actions they know.[43]

Unease, Suspicion, Truthfulness: Poor communication practices, such as sending mixed or conflicting messages from multiple sources, late release of critical information or the exclusive use of communication channels that are perceived as less trustworthy, can lead to unease or can raise mistrust on the side of the population. Panic is less likely to arise when being honest instead of sending mixed messages. Mistrust can express itself, for example, by avoiding public health recommendations. Leaving myths and arising rumours uncorrected in crisis communication may reinforce existing perceptions that certain social groups are responsible for the disaster or may even get preferential treatment.

Unease: It is important that official warning messages include recommended protective actions when the disaster strikes and raise the awareness and preparedness of the population before the occurrence of disasters. Media trainings should therefore prepare the sender of the message to frame the messages in an appropriate way to reach various target groups within the population, triggering the most appropriate proactive actions while avoiding panic and unease on the side of the population. Furthermore alerted but not affected population will strive to get additional information on the hazard, especially when they were emotionalised by mass media coverage, and some will even act and try to help. Experiences from the 2013 floods in Austria and Germany support this thesis as social media groups formed rapidly gathering several thousand followers grasping to know more about the flood situation, posting pictures of the floods. And, when communicators give no guidance on how to most effectively help the affected, unaffected people may even try to organize citizen-to-citizen help largely independently and often uncoordinated with the response.

> *Example: Untrained communicators sending no or mixed messages and giving no guidance on protective measures and how to best help the affected may cause unease on side of affected and non- affected population.*

Recommendations:

- The least effective communication strategy is withholding information – the best strategy for disaster managers is communicating and acting truthfully avoiding mixed messages
- The communicator training foreseen in WP35 on how to talk to stakeholders shall provide guidance for political leaders and media stakeholders: communicators should be able to 1) send clear messages to the various target groups, 2) include the most effective protective measures in their communications and 3) effectively make use of the various existing media channels.
- In a cross-sectoral or cross-border crisis a coordinated media communication strategy is key to avoiding mixed messages, confusion and erosion of trust.

See also (sub)categories: no related subcategories

[43] Lindell et al (2006) Fundamentals of Emergency Management

5.6 Resilience Logistics & Contingency Plans

5.6.1 Resources, Supply Chains & Contingency Plans

Related WP and Tasks: 44.1, 44.2, 44.4, 44.5, 46.1.

Distributing resources via well-functioning supply chains, and also ensuring that contingency plans are in place is crucial for CM. Within DRIVER, resources can be human and material- in terms of knowledge, deriving from cross-border cooperation (44.2), financial resources, or material resources (such as a disaster relief supply chain in 44.4).

Unease and Suspicion: Especially when dealing with low-income countries, the distribution of human and financial costs and resources should be adjusted accordingly to prevent excess burdens that can lead to unease or suspicion and affect economic stability in a negative way. If the distribution of resources and/or preparation of contingency plans involve (personal) data collection, these should be protected according to national legislation to avoid creating suspicion among the affected population.

Legality and Truthfulness: To avoid misuse, truthfulness as to how the resources are distributed and spent is required. It is very important to pay attention to both national and international legislations, especially in relation to data protection, when developing new tools, as grey areas and legal vacuums exist since the legislation are not always up to speed .

Technology Dependency: Novel methods for distribution of resources (especially if it fills a gap) can also risk increasing technology dependency if their innovation and performativity depends greatly on technology, making other alternative methods difficult.

> *Example: In 44.2, tasking and capacity monitoring aims at improving the effective assignment of resources during crisis resolution. If these resources include human resources then these should be treated fairly, and the collection of their personal data regulated.*

Recommendations:

- Tools and measures to improve the distribution of resources (whether human, material or financial) need to account for fair distribution of costs and benefits.
- The tools need to adhere to the principles of legality, truthfulness, and efficiency.
- Testing of the supply chain effectiveness should be as realistic as possible, and include as many relevant variables as necessary.

See also (sub)categories: For Costs & Effectiveness Assessments; Data & Information; Early Warning, Risk Analysis, Forecasting;

5.6.2 Core Functions in the City

Related WP and Tasks: 34.1

When it comes to crisis management, one crucial issue is to uphold (or restore) the core functions in the city to avoid additional damage and negative effects. Resilience logistics and contingency plans in DRIVER refer mainly to the resilience of local governments and related areas of mobility, energy, water, buildings, logistics and information technologies (34.1). This task includes the identification of core functions within government and the development of indicators and plans for strengthening their resilience. Since the identification of core functions and resilience indicators itself is unlikely to produce negative effects, potential secondary impacts are highly dependent on the methodologies that are chosen to conduct these identifications and which may influence the results.

Applicability: The selection of resilience indicators must be meaningful and applicable in the sense that they a) really apply to the given domain and that they b) really strengthen resilience within the particular domain without causing practical issues.[44] One practical issue is, for example, a domino-effect in governance, meaning that the realization of one resilience indicator may cause effects that require further measures (cf. example below).

Misuse and Impact on Market: The identification of key resilience indicators is always tied to the identification of measures that need to be implemented to address these indicators. The selection of indicators is on the one hand informed by specific strategies;[45] on the other hand the selection can be influenced by either political or commercial interests[46] that foresee the implementation of a specific measure. This is not negative per se, but the selection of indicators needs to reflect whether they are prone to political or commercial misuse that could, for example, impact negatively on the market.

New Vulnerabilities and Unease: Keeping track of key functions and resilience indicators is closely related to the identification of vulnerabilities. Documentation about this often collects and synthesizes this information and thus creates a new vulnerability, if these vulnerabilities become public or are exploited by individuals with malevolent intentions. It is also possible to over-analyse vulnerabilities and create more unease about them than necessary.

Technology Dependency: If the measures that are installed to enhance resilience are technological solutions, they may cause new dependencies which, if they fail, create negative impacts.

Legality: Information about the vulnerability and resilience of logistical domains and infrastructure can be confidential. Those who assess key functions, vulnerabilities and indicators need to ensure that they do not infringe upon legality and only obtain information about (potentially private) infrastructures and processes with consent.

Efficiency & Effectiveness: Measures resulting from resilience and contingency planning may not always have to be efficient. Contingency plans and resilience measures often foresee redundancies to enhance flexibilities, which results in backup solutions that may never be used (if there is no crisis). Especially measures that apply to commonly owned infrastructure often lead to a “tragedy of

[44] http://www.um.edu.mt/__data/assets/pdf_file/0007/215692/Briguglio_The_Vulnerability_Resilience_Framework,_23_Mar_2014.pdf p. 27
[45] http://www.degruyter.com/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1732/jhsem.2010.7.1.1732.xml
[46] Kaufmann, M (2013) Cyber-resiliens i EU. Internasjonal Politikk 71(2): 274-283.

the commons", whereby investors into solutions do not necessarily see results that concern them directly, but rather the common good.[47] These potential inefficiencies have to be taken into account when identifying indicators and developing contingency plans. Some measures and contingency plans even enhance complexity (e.g. redundancies), which may cause new security breaches.[48] In that case indicators and measures are even ineffective and it should be evaluated whether they are useful.

> *Example: Resilience indicators and contingency plans for information infrastructure are often based on principles of technical redundancies. These redundancies may foster resilience, but they also add complexity and make the governance of information infrastructure less transparent, especially if these newly added redundancies follow their own set of security policies. A diversity of policies again increases the risk of security breaches and creates a need for more universal standards (domino-effect of governing resilience/contingency planning).*

Recommendations:

- Avoid domino-effects in resilience governance by choosing resilience indicators and measures for contingency plans that strengthen resilience without causing too many follow-up measures.
- Reduce complexity of contingency plans wherever possible.
- Reflect on the influence that commercial or political actors may have on the selection of resilience indicators.
- Make sure that it is understood that enhancing resilience may not result in directly visible effects for those who invest.
- Cost-benefit logics will not apply to most resilience measures and contingency plans, since many contingency plans do not create sufficient incentives for actors to invest.
- Make sure that the identification of vulnerable or resilient infrastructures is not determined by their insurability.

See also (sub)categories: For Costs & Effectiveness Assessments

5.7 Decision Support Systems & Simulations

Related WP and Tasks: 35.3, 44.1, 44.4, 44.5, 54.3

Simulations are a common method for preparing for crisis[49] and can be useful to test out solutions or tools to enhance the management of a real crisis. A large part of DRIVER activities revolves around developing and testing CM solutions through scenarios and simulations. This category includes only

[47] http://www.enisa.europa.eu/media/press-releases/the-internet-interconnection-2018ecosystem2019-new-report-identifies-top-risks-for-resilient-interconnection-of-it-networks

[48] Kaufmann, M (2013) Cyber-resiliens i EU. Internasjonal Politikk 71(2): 274-283.

[49] See e.g. Falenski, A., Filter, M., Thöns, C., Weiser, A. A., Wigger, J. F., Davis, M., ... & Käsbohrer, A. (2013). A Generic Open-Source Software Framework Supporting Scenario Simulations in Bioterrorist Crises. Biosecurity and bioterrorism: biodefense strategy, practice, and science, 11(S1), S134-S145.

simulations and decision-support systems that are used as a operational CM tool.. Task 44.4 models and develops scenarios for the supply chain to enhance CM preparedness, which then feeds into 44.5 which stimulates the occurrence of unforeseen events and creates a decision-support tool (an application) for professional logistics crisis managers. The partly unknown accuracy of this method includes some risks.

Applicability: There is a risk that the variables and elements in the design of the scenario are incorrect, flawed or imprecise. This can produce skewed results undesirably influenced by the tool developers, and have an impact on the applicability of the experiments –among other negative effects. Whenever possible, it is advisable to introduce participatory approaches to scenario planning with potentially affected communities to ensure its applicability in a real crisis.[50]

Suspicion and Unease: Testing out CM solutions on volunteers through public experiments, as may happen in SP6, risks creating disproportionate suspicion and unease among the public if they are not informed in advance. If the applicability and effectiveness of the very design of scenarios are not useful or appropriate, it can create unease and influence the progress of the project. Even if the experiments happen within a controlled environment, if the participants are not informed of the nature and purpose of the activity in advance, it can cause unease and infringe upon the desired truthfulness of the project as individuals could feel misled. Providing this information in advance can be of more or less importance, depending on the nature of the experiment and the scenarios. The scenarios can appear distressing and cause unease also to participants, because they remind individuals of current threats and insecurities in society. These simulations happen "close to real conditions" and will include eventual distress and discomfort.

Legality: Noncompliance with legal frameworks can create risks and consequences that can seriously hamper the project, e.g. difficulties in implementing or distributing the scenario- based tool because local legal regulations are not complied with.

> *Example: The joint experiments in SP6 have different scenarios as their basis. Although these are internal DRIVER- activities, the use of scenario- based experimentation or workshops can also happen beyond the duration of the project, for example to update and test the portfolio of tools. If the accumulated knowledge from the scenarios proves incorrect or irrelevant, this will influence the applicability and effectiveness of the tool that is tried and tested through the scenarios. This can be caused by choosing imprecise or too precise scenarios which do not account for a highly unpredictable future.*

Recommendations:

- The public should be appropriately informed, to the furthest extent possible to avoid suspicion and unease.
- Make sure that the simulations reflect realistic conditions, for example by introducing participatory approaches to scenario planning with potentially affected communities.

[50] World Vision (2013), Participatory Scenario Planning for Community Resilience, Planning tool, UK. http://9bb63f6dda0f744fa444-9471a7fca5768cc513a2e3c4a260910b.r43.cf3.rackcdn.com/files/9813/7871/8703/Planning_For_Community_Resilience.pdf

- To ensure generalizability, choose scenarios for simulation that are not too narrow.

See also (sub)categories: - no related subcategories

5.8 Harmonization

Related WP and Tasks: 43.1, 54.1, 54.3

When collaborating during CM activities, a harmonization of practices (sometimes related to standardization, but here more policy-oriented) is a basic principle that emerges in different scales and has relevance on different occasions. When harmonizing standards or routines for CM, especially in the critical response phase, the in-advance planning and preparedness is crucial. Within DRIVER, many activities revolve around harmonization and cooperation. In 55.3, the outputs of training sessions on psychosocial support are harmonized with training and support tools. In 55.1, the focus is the collaboration between professionals and the general public focusing on how different professional organizations can align with each other their collaboration with the public.

Legality: When harmonizing regulations and procedures, some secondary insecurities and challenges may occur. Regulatory harmonization has to do with legal compliance and the role of regulatory governance within a sector, such as banking or industry.[51] For CM this means that there is a risk that harmonizing legal frameworks can be challenging, as, for example, new technology is lacking specific legislation in many countries.

Applicability: If different national legislations relevant for CM activities cannot be harmonized, the applicability of the developed CM tools will be affected as implementation could be difficult in the different countries. Despite its intent to simplify, harmonization can also require more and more complex legal regulations and rules. The applicability will be affected if two elements reject harmonization.

Unease: Harmonization of practices or regulations for CM can be a source of potential unease if the cost and benefits of the harmonization are not equally distributed between the partners. The process of harmonization is often affected by various power dynamics of the participating actors. As a result, unease or suspicion can arise due to a (perceived or real) imposition of certain interests.

Efficiency & Effectiveness: If the purpose of harmonization is not communicated to and respected by the involved individuals, this can affect the efficiency and effectiveness of the harmonization. Individuals involved in the harmonization process may feel overlooked despite having a sense of ownership of the process and accountability towards the organization.

Economic Stability: Lack of applicability can also create additional costs, and potentially influence the economic stability of the project. If harmonization is a basis for the project, but is in reality limited – because of a lack of legal compliance between two states or companies, for example – inefficiency or negative impacts on the market or employment can occur. That is the harmonization does not in

[51] One example is banking CM in the European Union, where harmonization is a central element. See e.g. Garcia, G., & Nieto, M. J. (2005). Banking crisis management in the European Union: Multiple regulators and resolution authorities. Journal of Banking Regulation, 6(3), 215-219.

fact contribute to resolving the issue at stake, whereby the joining of two services etc., instead reduces work places and competing companies risk going out of business.

New Vulnerabilities: Harmonization can also create new vulnerabilities because a harmonized set of systems is more vulnerable for failure than diverse and independent systems.

> *Example: When 45.4 aims at easing the information exchange across the CM community in Europe, harmonization of language and terminology, and technical and physical infrastructure is an important success criterion. If the development of a "system of systems" omits risk evaluations and legal and financial considerations, the harmonization infringes upon the applicability of the system because the implementation would be difficult.*

Recommendations:

- Harmonization of language and terminology can be a good foundation for furthering CM solutions, but requires, for example, financial and social impacts assessments in addition to the more fundamental legal requirements.
- Harmonization leading to fruitful preparatory CM planning can be crucial for the complex and critical crisis response phase as long as the harmonization is well-established and well-implemented, and does not complicate the CM process by adding unnecessary layers of organization etc.
- The output of the harmonization must ensure safeguards to minimize risk of misuse, for example, by limiting access to the data that forms part of the harmonization.
- How harmonization can create more vulnerability must be considered, for example, by ensuring routines and safeguards for limiting access to the databases of the harmonized systems.

See also (sub)categories: Cross-border and Cross-Sectoral Interaction; Communication Technologies; For Competence Building;

6 Methodology

These two final categories are placed outside the main assessment chapter, as they refer to tasks that are not operational CM. They include preparatory and research-oriented work and are of methodological nature. The recommendations of these categories will most likely not feed into the PoT. They are, however, important categories at this point in time when tools are being developed and tested.

6.1 Strategy Design

6.1.1 For Community Resilience

Related WP and Tasks: WP33

Enhancing and enforcing community resilience is a corner stone for crisis management in general. This is also reflected within DRIVER, for example WP33 aims at creating a community resilience model with indicators and measurement tools to assess resilience in urban and rural areas across Europe (33.1). Community resilience is reflected, among other things, in the quality of the psychosocial support provided (33.3) and the ways in which community support is organized through civil society and social networks during and after a crisis (33.2). The selection of indicators for the community resilience model and the design of an efficient and measurable approach itself can create undesired secondary effects that can have a detrimental impact on the future implementation of the community resilience model. These assessments and recommendations will focus on the way in which the *standardization and modelling* inherent in these tools can cause secondary effects.

Unease and Suspicion: Involving communities and individuals in crisis preparedness, response and recovery phases is an important step towards empowering populations to strengthen their resilience. But it does not come without important secondary insecurities and challenges that can affect the individual, social, economic and political dimensions of a community. Too much emphasis on the role of grassroots and civil society organizations (33.2) –whether composed of trained or untrained members- can create unease as communities can feel overburdened with the responsibility to take care of themselves. The community resilience model will set-up standards that communities may feel pressured to live up to, especially if their empowerment requires the active engagement of people before, during and after crisis occurrence. If resilience indicators include a bias towards a specific group, their implementation may cause suspicion towards that specific group.

Technology Dependency: Choosing resilience models and indicators is not a random exercise, but highly context-dependent. Professionals need to remember that there is always a risk for developing a methodology dependency that produces skewed or not accurate enough results.

Truthfulness and Applicability: The definition of resilience and the selection of indicators to measure it are directly linked to the political situations at the time of its conceptualization. Resilience indicators reflect a specific vision of how a society should look like and perform, and what kind of

responsibilities the state, the community, and the individual has towards its wellbeing, safety and security. Are local knowledge and traditional coping mechanisms taken into account when developing the resilience model and indicators? How to develop sufficient indicators to measure all possible dimensions of resilience? Can some indicators not be measured? The applicability and truthfulness of the model will depend on the concept of community resilience and the indicators chosen. To avoid these potential secondary effects, participatory processes should be included whenever possible to reach a common definition of resilience along with related indicators and strategies (e.g. gap analysis, scenario planning, etc.).[52]

Function Creep and Misuse: Resilience models can be politically misused to make the community members responsible to perform security activities that should in fact be guaranteed by the state.

New Vulnerabilities: The engagement of communities needs to be balanced to avoid the creation of new vulnerabilities and unease. Communities may feel (more) vulnerable because they have been made aware of previously unknown risks and also due to the perceived need to care for themselves.

Efficiency & Effectiveness: The model of WP33 might be quite effective in empowering communities in a financially efficient way (as it avoids the massive employment and deployment of professional staff and resources), but it may reduce overall efficiency, if it relies too much on average citizens to perform tasks that should be performed by professionals or trained volunteers. Also, an effective community resilience measure is likely to require complex oversight mechanisms and investments in capacity development that might question its efficiency.

Employment: The engagement of unlearned community members in crisis management may decrease the employment and payment of professionals and shifts the responsibility for its wellbeing to the communities and individuals.

> *Example: If local knowledge about resilience is not taken into account when developing resilience models and indicators, resilience indicators may a) not be applicable and thus produce skewed results, b) may miss out on local potential, c) overburden local community members with tasks that they may not be familiar with.*

Recommendations:

- Communities should be consulted about their willingness and readiness to perform according to given indicators.
- Always consider context for developing resilience indicators. When developing indicators take into account what and for whom you seek to measure resilience.[53]
- Participatory processes are good tools to ensure applicable, truthful, inclusive and sustainable approaches to community resilience.[54] When planning resilience strategies and identifying resilience indicators ensure that it does not overburden local communities. The burden on communities has to be carefully balanced with the duty of the state to protect its citizens, i.e. ensure that none of the tasks assigned to average citizens should ideally be

[52] World Vision (2013), Ibid.
[53] OECD Working Paper (2013) Risk and Resilience. From Good Idea to Good Practice. http://www.oecd.org/dac/governance-development/FINAL%20WP%2013%20Resilience%20and%20Risk.pdf
[54] World Vision (2013), Ibid.

fulfilled by professionals to avoid employment and effectiveness problems, as well as the creation of vulnerabilities and unease.

- Ensure oversight mechanisms for resilience programs, even if they may not seem efficient.

See also (sub)categories: For Costs & Effectiveness Assessments; Scenarios & Simulations; Psychosocial;

6.1.2 For Early Warning & Risk Analysis

Related WP and Tasks: 43.1, 43.3, 44.1.

For crisis management, risk assessments play an important role in the situational analysis to enhance preparedness and reaction, and to ensure the effective use of resources. Within DRIVER this is reflected in 43.1 and 44.1 for example. Risk and early warning are integral aspects for assessing crisis dynamics and approaching hazards (43.3). As opposed to 5.2.3, which focuses on the *implementation* of risk assessments and early warning systems, this section focuses on those effects that need to be taken into account when *developing and modelling* risk assessment and early warning strategies.

Applicability and Truthfulness: Because risk assessments are a largely accepted method within crisis management, their applicability and truthfulness is often unquestioned, even though risk assessments are highly dependent on the context and chosen variables, and may only have limited potential to make a meaningful assessment or to express the truth about a development. Despite their methodological shortcomings, the results of risk assessments often gain considerable trust and acceptance within diverse crisis management groups.[55]

Technology Dependency: If the method of risk assessments is overly trusted within crisis management it can produce a kind of technology- or methodology- dependency, as for example was the case in the L'Aquila earthquakes when the statement by risk authorities reassured people to stay within the city, which caused major negative impacts once the earthquake struck harder than expected.[56] This is also a risk that researchers face and need to take account of as the L'Aquila researchers, for example, were sentenced to prison for their wrongful analysis. This may not happen in every jurisdiction, but illustrates the amount of responsibility the risk assessment researcher has.

Legality: Is relevant for risk assessments to the extent that information that is collected to conduct risk assessments, especially if that information is of a private nature, comes into conflict with data protection laws.[57]

> *Example: If the variables that a risk assessment is based on are not well-tested and proven to reflect the situation that it is supposed to analyse the risk assessment may cause skewed results, which can have fatal consequences in the CM setting.*

[55] http://www.ramas.com/wttreprints/Myths.pdf; Amoore, Louise and Marieke de Goede (2008) Risk and the War on Terror. London : Routledge.
[56] http://www.radicalgeography.co.uk/laquilasum.pdf
[57] http://rt.com/news/data-protection-rules-eu-491/

Recommendations:

- When planning the risk assessments for a specific setting, carefully design the variables that feed into the assessments to avoid secondary impacts.
- Make sure that alternative assessments methods exist to avoid dependencies on just one method.
- Set clear boundaries as to which kind of data is being collected to conduct risk assessments to avoid the integration of private data.
- When communicating the risk to lay persons, make sure they are informed about the real significance of scientific accuracy.

See also (sub)categories: Data & Information; Early Warning, Risk Analysis, Forecasting;

6.1.3 For Learning Activities & Lessons Learned

Related WP and Tasks: WP51, 52.2, 52.4, 53.1, 53.2, 55.1, 55.3

Documenting and utilizing lessons learned is an important tool to enhance the effectiveness and efficiency of crisis management. Within DRIVER, many learning and training activities happen, but the concept of learning activities and lessons learned will also be relevant beyond the project. DRIVER includes variables related to learning with the basic aim to increase the effectiveness of CM management as a whole. These include, for example, the identification of the need for a standardized European model for learning activities (55.1, 55.3and WP51), lessons learned (WP53) and competence building (WP52).

Unease: The strategies for identifying lesson learned from crisis situations and learning activities can create unease if the approach over- engineers the crisis situation, aiming at controlling every single variable and aspect of it.[58] Focusing too much on the negative outcomes of the crisis and its management can also cause unease because the selection encompasses a too pessimistic take on CM solutions.

Misuse & Suspicion: If the identification of the lessons to be learned from contains a "hidden agenda", for example, in terms of a political or economic expression, which is not clearly communicated, it can be defined as a form of misuse of the tool.

Applicability & Technology Dependency: If the selection of the lessons that are chosen as the basis for the learning activity imply a predefined set of values (whether cultural, or economic, political, etc.), lessons learned activities may not be applicable cross- border or cross-agency, because every lesson learned is context-dependent. On the other hand, there is the risk of choosing variables that are *too* contextually dependent and narrow, and thus overlooking certain potential lessons to be learned. This can be caused, for example, by structuring an interface in a way in which it creates its own dynamic on the prioritization of the lessons to be learned (e.g. when searching or categorizing by keywords). The selection of lessons or variables can also influence or increase technology dependency if lessons learned exercises can only be conducted by computer programs.

[58] Aradau C and van R Munster (2011), Ibid.

New vulnerabilities: A wrongful or incorrect analysis and selection of lessons learned can create new vulnerabilities. If not communicated carefully, the analysis of lessons learned can point out vulnerabilities to individuals with malevolent intentions. Also, once identified such lessons can put a high burden at the first responders that are supposed to manage following crises; although they might themselves be in a situation of heightened stress, they are probably legally bound to avoid any mistake and might be additionally put under stress which increases the likelihood of wrong decisions or technical mistakes.

Legality: There is a risk that the cross- border and cross-agency approach to defining lessons learned could be hindered by national legal frameworks (e.g. data protection issues for example when dealing with covert or sensitive information or data).

Efficiency & Effectiveness: The use of a lessons learned approach may be very effective, although not efficient, as the requirements to be met and the resources to be spent (costs) can easily surpass the benefits.

> *Example: WP53 will create a Lessons Learned Framework for CM that is useable for professionals and tool developers in a cross-national context. It will follow a top-down approach defined by the needs of decision-makers. If these different needs (all) imply a predefined set of values, the lessons learned exercise may not be very structured or effective for the given context.*

Recommendations:

- When prioritizing which lessons should be learned, make sure to also include those which serve as empowering lessons, and not only the negative outcome of crisis.
- Try to get as much knowledge about the field as possible to ensure including the most relevant lessons learned as the basis of the learning activities. This includes setting clear limits to what kind of lessons you seek to learn about.
- Reflect upon the values the prioritized lessons are based upon and why they are seen as more relevant than others.
- Ensure that there are mechanisms in place to safeguard against misuse of the lessons learned methodology (e.g. misuse due to hidden political agendas)
- Pay attention to minimizing the exposure to new vulnerabilities.
- Carefully include new lessons into first responder's and crisis managers training curriculum.

See also (sub)categories: Other Forms of Training; Data & Information;

6.1.4 For Competence-Building

Related WP and Tasks: WP52

When implementing a CM tool or measure it is important to have a strategy in place for how the tool will build or enhance competence within a specific field. Such a strategy should account for variables such as demographics. Within DRIVER, WP52 will develop a harmonized competence framework for crisis management that is applicable across the EU through the integration of different learning and

competence approaches into a harmonized and systematic framework. Concretely, this involves the standardization of competence building across Europe (52.1) that will feed into the harmonized framework (52.2) and the web-based competence-check-tool for crisis management professionals (52.4). These assessments and recommendations will focus on the way in which the *standardization and modelling* inherent in these tools can cause secondary effects.

Applicability, Efficiency & Effectiveness: The need to constantly update a competence framework might affect its applicability, effectiveness and efficiency. If not planned in a transparent and inclusive manner with all international partners involved, procedures for harmonising cross-border and cross-organizational contexts may not be applicable. Competence is also hard to prove and therefore it can be hard to establish standardized procedures or effectiveness measuring models for it.

Suspicion, Unease, and Truthfulness: The identification process of competences and gaps (52.1) can be influenced by organizational agendas. Organizations from low-income countries might feel unease if they perceive that a culturally biased understanding of competence and competence gaps is imposed on them that, for example, benefit certain economic and employment interests of other countries or organizations.

New vulnerabilities and Misuse: If competence-building is defined by single actors only and not through a consensus-based process it may be opened up for misuse to enable specific (hidden) agendas.

Legality: Professionals might meet obstacles in terms of legal regulations for cross-border harmonization of competence frameworks, which may jeopardize the standardization process (i.e. some paramedical practices are not legal in certain countries and there might be a scarcity of some competences in some regions, thus creating an international unbalance in CM capacities).

> *Example: If the understanding of competences does not take local frameworks into account, it may not be applicable internationally, it may not conform to given legal regulations and it may cause unease among participating members.*

Recommendations:

- Make sure all relevant partners are involved in devising or at least in reviewing competence-building models. Base competence building models on international consensus.
- Take local contexts into account. Different backgrounds in terms of geography, ethnicity, socio-economic indicators, etc. need to be taken into consideration by developers to benefit from a broader definition of competence for crisis management ("traditional" competences based on cultural coping mechanisms developed throughout centuries versus "highly technical" competences derived from latest scientific and technological developments).
- Shared terminologies to define competence and competence needs, as well as strategies to achieve a standardized and harmonized framework are important aspects to take into consideration when planning competence building.
- Ensure that competence building in a specific domain does not infringe upon or require certain legal amendments in member countries.

See also (sub)categories: For Costs & Effectiveness Assessments; Data & Information;

6.1.5 For Decision-Making

Related WP and Tasks: 43.1, 54.1, 54.3

Because important decisions usually have to be taken under circumstances of urgency regulations and competences for an effective decision-making process in CM need to be in place. Supporting decision-making during crisis management is a key activity within DRIVER, for example when it comes to damage and need assessment (43.1), as well as decisions about CM in general (54.1). Within tasks 43.1, 54.1 and 54.3 models are being developed to enhance decision-making process and context training. These tasks refer to the impacts that can be caused by the developments of tools and methods that should support it. As a result, these recommendations will focus on the way in which the *standardization and modelling* inherent in these tools can cause secondary effects.

Unease: It is expectable that, due to the urgency of a real-life situation and dependent on the intensity of the training, decision-making training may create both competence, but potentially also unease within professionals. The training model may point to areas that are new to decision-makers and entail a high degree of responsibilities and commitment due to the enormous potential impact of a crisis on society. It is sensible to take this into account when designing and deploying decision-making models.

Applicability: Since most decision-making strategies translate different aspects of the decision into numeric values, it is important to check how this process may infringe negatively upon applicability**.** The outcome of the decision-making tool is thus highly dependent on the method chosen to convert real-world phenomena, dynamics or political priorities into numeric values.

Efficiency & Effectiveness: Any mistake or misrepresentation of a situation can lead to skewed results and potentially detrimental and inefficient decisions. It is therefore important to reflect upon which phenomena can be translated into numeric models at all and which cannot be represented sensibly by numbers. When designing decision-making tools it is important to reflect upon how the representation of results in specific graphs may be misleading, over-representing specific aspects of the results.[59]

Misuse: Decision-making models, even if they are based on numeric assessments, can be prone to misuse. In most decision-models numeric values can be assigned by decision-makers to indicate priorities. If these priorities are not well-reflected they can be misused for political agenda setting.[60]

> *Example: If models that support CM decision-making (such as in 54.1) translate variables into numeric values that do not represent reality, they produce skewed results. Decisions based on these models may turn out to be inefficient, ineffective or in the worst case have negative effects on society.*

Recommendations:

[59] Cf. ValueSec and DESSI projects.

[60] http://www.referenceforbusiness.com/management/De-Ele/Decision-Making.html

- Evaluate carefully which decision-making parameters can be translated into numeric values and how.
- Make sure that the graphical representation of decision-making results is easy to understand and does not over-represent certain aspects.
- Make sure that political agenda-setting is not covertly integrated into decision-making methodologies, either by avoiding loopholes or by integrating approaches overtly into decision-making that address political agenda setting (for example by making a function where policy makers can indicate their priorities overtly).

See also (sub)categories: no related subcategories.

6.1.6 For Costs & Effectiveness Assessments

Related WP and Tasks: 44.1, 44.5.

It can be difficult to estimate the costs vis-à-vis the benefits when it comes to creating and deploying CM solutions, most importantly because CM measures and tools may never come into use, or we will never know what particular crisis they might have prevented. DRIVER takes into consideration the limited availability of financial resources compared to the potentially unlimited costs for crisis management tools and measures. Cost-benefit analyses are needed to identify which tools and measures are most effective and efficient (44.5) – as an integral part of CM altogether. A too broad view on cost-benefit analysis can also suggest the belief that crisis preparedness is something that we can ultimately prepare ourselves for completely if enough resources are applied. It is debatable whether this cost-benefit analysis refers mainly to methodology, i.e. it is used at the stage of the development of tools, or whether it is in itself a fundamental tool in CM that will be re-used by other crisis managers for preparation and operational CM.

Efficiency & Effectiveness: Crisis management investments often face the problem of the ´tragedy of the commons´: The potential benefits of the CM tools and measures are not always likely to outweigh their costs because an investment may help another area more than the one in which was invested. Crisis management investments then do not necessarily pay off in case crisis hits elsewhere or does not hit at all. But calculations about potential risks in particular areas can influence partners to invest in common goods, such as a European wide system of measures. However the most effective CM solution is not always the most efficient one. Alternatively, a very efficient tool can be ineffective and create secondary insecurities and challenges among the crisis population.

Unease, Suspicion and Misuse: Carrying out cost-benefit analyses of CM solutions can create unease among professionals in relation to the effectiveness vs. efficiency dilemma described above. Making significant investments in specific `problems´ (i.e. terrorism, harbour security, storage of pharmaceutical products, etc.) can, on the one hand, create suspicions in the population about political or economic agendas hidden behind such investments. On the other hand, such a considerable investment can be perceived as a sign of danger, causing unease in the population. In low-income countries making cost estimations can create significant unease in relation to its economic capacity to make the necessary investments into the appropriate CM tools.

Function Creep: An investment into a (new or updated) particular technology always entails the risk of function creep. The investment can be done with the intent to address crisis management related issues but, at the same time, it is likely that such technologies are at some point to be used or misused for unintended purposes (e.g. surveillance, illegal data collection, etc.).

New Vulnerabilities and Applicability: Cost estimations or cost-benefit analysis based on wrong assumptions can cause serious new vulnerabilities. Wrong assumptions derived from inaccurate situation analysis, gap analysis or forecasting can lead to wrongful cost estimations and cost-benefit analyses, ultimately leading to unprofitable investments –whether financial, human, organizational or all of them.

Truthfulness: In respect to the above, the population may doubt the truthfulness of the leadership's communication about investments, as well the truthfulness of the analysis.[61]

> *Example: A cost- effectiveness analysis in DRIVER may always face the problem of the tragedy of the commons or the uncertainty of investments. If this is not clearly reflected about, potential investors may be lost. Should an investment not be clearly based on its effect on the population, it may cause either unease or suspicion about the "ulterior motive" for the investment. A cost-benefit analysis that does not take gap analyses, situational analyses and risk assessments into account may lead to unprofitable investments.*

Recommendations:

- Identify a balance between the "societal effectiveness" and its financial, logistical or organizational efficiency.
- All measures and tools addressing societal impacts need to be accompanied by sufficient financial, human and physical resources to be both effective and efficient.
- Make sure that decision-makers reflect upon the "tragedy of the commons" situation.
- Take low-income countries' investment capacities realistically into account.
- Devise a communication strategy for justifying the investment without creating unease in the population.
- Make clear statements on how these investments are to be used to avoid unintended misuse.
- Ensure close communication with those conducting gap, risk and situational analyses.

See also (sub)categories: Data Collection & Storage; Gap Analysis, Situational Analysis & Impact Assessments;

[61] El Pais: Ebola in Spain: Five days after Ebola case confirmed, Deputy PM takes control of crisis, http://elpais.com/elpais/2014/10/10/inenglish/1412949468_311967.html

6.2 Methodologies for Selecting Measures & Assessing Impacts of Experiments

Related WP and Tasks: SP2 & SP9

This section considers the internal DRIVER activities mainly in SP2 and SP9, which can be described as research strategies and methodology. Strategy design for dealing with data outputs from the DRIVER experiments refers to activities that exclusively take place within DRIVER, for example by means of performance and benefits metrics (23.2) and Impact and Effectiveness Assessments (23.4) or doing the ethical impact assessments in WPs 92 and 93. This does not mean, however, that the way in which data is being analysed or evaluated and measures are being selected within DRIVER does not infringe upon CM as a whole. This prompts a few research ethical and methodological considerations.

Applicability: Choosing criteria and variables to conduct assessments of DRIVER measures is not easy, since they may only be applicable for some measures, but not for others. It is thus important to evaluate the results of the assessments to ensure that the criteria chosen are not infringing upon the applicability of the measure.

Misuse: When assessing DRIVER measures it is possible that some measures are considered more important than others – that may be because they are easier to assess, because they "sell better" or because they are more central within the project. If some criteria prioritize specific measures over others without indicating or reflecting that, they offer the possibility of "methodological misuse".

New Vulnerabilities, Efficiency & Effectiveness: If the selection of criteria focuses too much on producing specific outputs, they may create new vulnerabilities for the project. This is because some potentially important measures are not properly assessed, or are neglected or changed with the effect that they may cause new vulnerabilities, inefficiency or ineffectiveness both for the project itself or the crisis situation once the measures are being put into action. Equally, if the selected criteria and variables are too complicated they rather enhance complexity and inefficiency within the project instead of reducing it.

> *Example: Performance and benefits metrics may be opened up for misuse or may be inapplicable if the scope of criteria and variables is too narrow, only focusing on particular forms of benefits. As such, they may cause inefficiencies and new vulnerabilities for the project.*

Recommendations:

- Test the criteria and variables on many heterogeneous measures in order to find out whether they are applicable and produce meaningful results for all measures.
- Should one set of criteria be either too generic or may not apply to all DRIVER measures, consider whether the assessment of different measures may need different sets of performance criteria.
- If some measures are more central than others in the project, reflect that in the selection of criteria to avoid misuse.

- Do not let the criteria that are easy to assess determine the overall set of assessment criteria.

See also (sub)categories: For Cost & Effectiveness Assessments; Strategy Design/decision-making;

7 Preliminary Conclusions

The table in the annex summarizes the assessments above and provides an overview of the criteria that have been discussed per category of tools. As such, it allows for the preliminary conclusion that all criteria have shown to be relevant in the context of crisis management in general and the DRIVER project in particular. This result, however, needs to be further contextualized.

Firstly, these assessments are not final. As mentioned in the introduction, SP9 will follow the DRIVER tool development, observe experimentation as well as scenario-based implementation and will furthermore pay attention to ongoing discourses on CM in order to update the categorization of tools, criteria, assessments, examples, and recommendations where necessary. The next steps are thus to participate in DRIVER experimentations throughout the next year and to update this deliverable accordingly in version 92.12, due in M19. The same follow-up procedure is foreseen for the other deliverables in WPs 92 and 93 so as to validate criteria, refine recommendations and make this deliverable more operational over time. 93.1 already provides a fist reality-check for the criteria set as the criteria are being verified in detail in relation to EU, UN and IFRC crisis management and resilience policies.

Secondly, even though this table displays frequencies of discussed criteria, it does not serve as a basis to argue that those criteria which have been mentioned most often are the most important. The importance of criteria is strictly context dependent. What this table does show, however, is which criteria are likely to be relevant for particular categories of tools. As such, this table serves as a first hint or an initial alert that should attract the attention of those who develop and implement CM tools and measures.

Finally, this idea of the alert is also the starting point for conceptualizing the integration of the criteria set into the DRIVER portfolio of tools (PoT) and the testbed (the DRIVER methodology). The integration of WP 92/93 findings into the PoT and testbed is the ultimate aim of these WPs and will be enabled through the final versions of all 92 and 93 deliverables, the last of which are due in M47. A concrete methodology for integration will thus be developed throughout the next three years alongside the further development of the PoT and the testbed. A first suggestion for the criteria integration, however, is to create a kind of “alert system” that at the same time enables decision-makers, end users and stakeholders to understand and asses the kind of impact that a tool or measure can have on society. This would include the following steps:

1. The selection of criteria, their definitions, the assessments, examples and recommendations are being refined and iterated through participation in DRIVER experimentations. A refined version of the full set is delivered in the final versions of deliverables, latest in M47.
2. The categorization of tools is equally being updated and refined throughout the DRIVER project.
3. Both, criteria, recommendations, examples and tool categories are being “tagged” with a tagging system that allows for different combinations of tools and with different scenarios.
4. When a specific category of tool or a combination of tools is being retrieved from the PoT, the relevant criteria will appear on a dedicated area on the PoT screen. The tagging system will ensure that these criteria match the researched tools/combinations and the particular

context. The user could then have several options: a) The user can click on each criterion to read a definition in order to learn more about this criterion, its relevance and the way it is being understood. b) To follow-up, the user can upon further clicks retrieve example assessments and recommendations in order to understand which next steps to take and what to pay particular attention to in the implementation.

5. A mechanism for ensuring that criteria and recommendations are actually being paid attention to in the implementation will have to be developed. A suggestion is that the user cannot proceed with the ongoing operation in the PoT unless s/he has given a short written reflection about how to avoid negative and foster positive societal impacts.

Please note that these are *preliminary* ideas and suggestions for the integration of criteria into the PoT. They will first have to be discussed in detail in SP9 and eventually planned and realized with those partners who develop the PoT and the testbed. This work will, as indicated, start once the concrete planning for the PoT's structure has actually begun. It will furthermore have to be discussed whether the tagging of criteria to different tools and contexts is a realistic plan and how to identify the underlying structures and logics for this tagging system.

8 Bibliography

Aftenposten (2014) Kritiserer mediene for å skape angst etter terrortrussel, http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-terrortrussel-7650037.html

Amoore, Louise and Marieke de Goede (2008) Risk and the War on Terror, London, Routledge.

Andrejevic M and K Gates(2014) Big Data Surveillance : Introduction. Surveillance and Society 12(2) : 185-196.

Aradau C and van R Munster (2011) The Politics of Catastrophe, London, Routledge

Baker, Tom and Simon, Jonathan (2002) Embracing Risk. The Changing Culture of Insurance and Responsibility. Chicago: The University of Chicago Press.

Berg B L & Lune H (2004) Qualitative research methods for the social sciences, Volume 5, Boston, Pearson, p. 86.

Belton, V and Stewart, T (2002) Multiple Criteria Decision Analysis: an integrated approach. Dordrecht, Kluwer Academic Publishers Group.

Black, Daniel (2014) Where Bodies End and Artefacts Begin: Tools, Machines and Interfaces. Body & Society 20(1), pp. 31-60.

Boyd D and K Crawford (2012) Critical Questions for Big Data. Information, Communication and Society 15(5), pp. 662-679.

Briguglio L (2014) The Vulnerability and Resilience Framework for Small States, Univeristy of Malta, p.27.
http://www.um.edu.mt/__data/assets/pdf_file/0007/215692/Briguglio_The_Vulnerability_Resilience_Framework,_23_Mar_2014.pdf

Brown, J and Isaacs, D (2010) The world café. Shaping our Futures Through Conversations that Matter, San Francisco, Berrett-Koehler publishers.

Bygrave, L. (2002) Data protection law. Approaching its rationale, logic and limits, Great Britain, Anthony Rowe Limited.

Centre for Interdisciplinary Methodologies, Socialising 'Big Data': Identifying the Risks and Vulnerabilities of Data-Objective, Warwick University, http://www2.warwick.ac.uk/fac/cross_fac/cim/research/socialising-big-data

Colucci L (2008) Crusading Realism. The Bush Doctrine and American Core Values After 9/11. Lanham: University Press of America.

Courtney Jr, R. H. (1977, June) Security Risk Assessment in Electronic Data Processing Systems, in Proceedings of the June 13-16, 1977, National Computer Conference, pp. 97-104.

Dagsavisen (2014) Advarer mot overdreven frykt, http://www.dagsavisen.no/samfunn/krisepsykolog-advarer-mot-overdreven-frykt/

Decision Support and Security Investment (DESSI) Project, http://securitydecisions.org/about-dessi/

Dictionary.com, http://dictionary.reference.com

El Pais (2014), Five days after Ebola case confirmed, Deputy PM takes control of crisis, Madrid. http://elpais.com/elpais/2014/10/10/inenglish/1412949468_311967.html

Emmitsburg MD (June 2014) Federal Emergency Management Agency Emergency Management Institute. www.training.fema.gov/EMIWeb/edu/fem.asp

European Union Agency for Network and Information Security (ENISA) (2011) The Internet Interconnection 'ecosystem' - new report identifies top risks for resilient interconnection of IT networks, Press Release, http://www.enisa.europa.eu/media/press-releases/the-internet-interconnection-2018ecosystem2019-new-report-identifies-top-risks-for-resilient-interconnection-of-it-networks

Falenski, A., Filter, M., Thöns, C., Weiser, A. A., Wigger, J. F., Davis, M., & Käsbohrer, A. (2013) A Generic Open-Source Software Framework Supporting Scenario Simulations in Bioterrorist Crises, In Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, 11(S1), S134-S145.

Fersen S, Nelson S, et. al. (?) Myths about Correlations and Dependencies and their Implications for Riks Analysis, submitted to Human and Ecological Risk Assessment, http://www.ramas.com/wttreprints/Myths.pdf

Forschungsverbund – Sicherheit im Öffentlichen Raum (SIRA),http://www.sira-security.de/index.html

Furedi, Frank (2006) The Culture of Fear Revisited. London: Continuum.

Garcia, G., & Nieto, M. J. (2005) Banking crisis management in the European Union: Multiple regulators and resolution authorities, Journal of Banking Regulation, 6(3), pp. 215-219.

Gogarty, Brendan and Meredith Hagger (2008) The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air. Journal of Law, Information and Science 19 (1), pp. 73-145.

Gonzalez Fuster Gloria, Bellanova Rocco (2013) European Data Protection and the Haunting Presence of Privacy. NovATIca, from 2012/2013 Annual Selection of Articles, issue Privacy and New Technologies, pp.17 - 22.

Hagmann J and M Dunn Cavelty (2012) National risk registers: Security scientism and the propagation of permanent insecurity, in Security Dialogue 43 (1), pp. 79–96.

International Federation of Red Cross and Red Crescent Societies (2014) What is vulnerability? https://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/what-is-a-disaster/what-is-vulnerability/

International Monetary Fund. (2014). *How the IMF Promotes Global Economic Stability*. Available at: http://www.imf.org/External/np/exr/facts/globstab.htm

Jaeger, C; Renn, O, Rosa Eugene A, Webler, Thomas (2006): Risk, Uncertainty and Rational Action. London: Earthscan.

Kamberelis, G and Dimitriadis, G (2013) Focus Groups. From Structured Interviews to collective conversations, Oxon, Routledge.

Kaufmann (2010) Ethic Profiling and Counter-Terrorism, Examples of European Practice and Possible Repercussions, LIT Verlag Münster.

Kaufmann, M (2013) Cyber-resiliens i EU, In Internasjonal Politikk 71(2), pp. 274-283.

Kaufmann M (forthcoming 2015) Resilience 2.0. Media Culture and Society.

Kaufmann M (forthcoming 2015): Drone/Body: the Drone's Power to Sense and Construct Emergencies. In Sandvik KB and Gabrielsen Jumbert M (eds.): The Rise of Good Drone. London: Ashgate.

Klassenkampen (2014) Advarer mot fryktkultur, http://klassekampen.no/article/20140728/ARTICLE/140729963

Kunsch, PL, Kavathatzopoulos, I and F Rauschmayer (2008) Modelling complex ethical decision problems with operations research, Omega 37, pp.1100 – 1108.

Lindell M.K., Prater C.S. & PerryR.W. (2006) Fundamentals of Emergency Management.

Lindgren, M and Bandhold, H (2003) Scenario Planning. The link between future and strategy, New York, Palgrave Macmillan.

Longstaff, P.H., Armstrong, N.J., Perrin, K., Parker, W.M., and M.A. Hidek (2010): Building Resilient Communities: A Preliminary Framework for Assessment. Homeland Security Affairs VI (3).
Marx, Karl (1989) Marx's Grundrisse, 2nd edition, D. McLellan (ed.), London, Macmillan.

Merriam Webster Dictionary, http://www.merriam-webster.com/thesaurus/

Metro (2014) Text that warned of terror attack on London Underground branded a hoax by police, http://metro.co.uk/2014/09/01/text-that-warned-of-terror-attack-on-london-underground-branded-a-hoax-by-police-4852485/

Morgenbladet (2014) Et glimt av USA, http://morgenbladet.no/samfunn/2014/et_glimt_av_usa#.VEgyYUstzg5

Norwegian Data Protection Authority, http://www.datatilsynet.no/Teknologi/Dronar--kva-er-lov/

OECD (2013), Risk and Resilience. From Good Idea to Good Practice, Working Paper.

http://www.oecd.org/dac/governance-development/FINAL%20WP%2013%20Resilience%20and%20Risk.pdf

Office for the Coordination of Humanitarian Affairs (OCHA) (June 2014), Unmanned Areal Vehicles in Humanitarian Response, OCHA Policies and Study Series, p.9. https://docs.unocha.org/sites/dms/Documents/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf

Oxford Dictionaries, http://www.oxforddictionaries.com/

Prettenhalter, F. E. (2012) Risk and Insurability of Storm Damages to Residential Buildings in Austria, in Geneva Papers on Risk and Insurance - Issues and Practice, 37(2), pp. 340-364. http://www.researchgate.net/publication/227469470_Risk_and_Insurability_of_Storm_Damages_to_Residential_Buildings_in_Austria

Porter, C. (2014) Little privacy in the age of big data, in The Guardian. http://www.theguardian.com/technology/2014/jun/20/little-privacy-in-the-age-of-big-data

Reference for Business, Encyclopaedia of Business, 2nd Ed. http://www.referenceforbusiness.com/management/De-Ele/Decision-Making.html

Reznek, M., Smith-Coggins, R., Howard, S., Kiran, K., Harter, P., Sowb, Y., ... & Krummel, T. (2003) Emergency Medicine Crisis Resource Management (EMCRM): Pilot study of a simulation-based crisis management course for emergency medicine, Academic Emergency Medicine, 10(4), pp. 386-389.

Rosenblatt, A., & Attkinsson, C. C. (1992) Integrating systems of care in California for youth with severe emotional disturbance. I. A descriptive overview of the California AB377 evaluation project, Journal of Child and Family Studies, 1(1), 93-113.

Irmak R-D (Ed.) (August 2010) Journal of Homeland Security and Emergency Management, Volume 7, Issue 1, http://www.degruyter.com/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1732/jhsem.2010.7.1.1732.xml

IFRC 2012, “The road to resilience. Bridging relief and development for a more sustainable future.”

Radical Geography (?) L'Aquila Earthquake, Italy 2009, A Case study of an Earthquake in an MEDC, http://www.radicalgeography.co.uk/laquilasum.pdf

Russia Today (2013) EU response to NSA leaks: MEPs approve data protections rules, http://rt.com/news/data-protection-rules-eu-491/

Rutkin, Aviva (2014) Drone law: Flying into a legal twilight zone, Magazine issue 2969 http://www.newscientist.com/article/mg22229694.400-drone-law-flying-into-a-legal-twilight-zone.html#.VACCfDKSx8F

Stewart, David W. & Martin, Ingrid. M. (1994) Intended and Unintended Consequences of Warning Messages: A Review and Synthesis of Empirical Research, in Journal of Public Policy & Marketing, Vol. 13 (1), Spring Issue, pp. 1-19. http://www.jstor.org/discover/10.2307/30000168?uid=32605&uid=3738744&uid=32604&uid=2&uid=3&uid=5909240&uid=67&uid=62&sid=21104745263583

Tardy, T (2013) Mainstreaming Human Security in Peace Operations and Crisis Management: Policies, Problems, Potential, in International Peacekeeping, 20 (1), pp. 121-123.

The Guardian (2014) US government board says NSA bulk collection of phone data is illegal, http://www.theguardian.com/world/2014/jan/23/nsa-barack-obama-phone-data-collection-illegal-privacy-board

The Washington Post (2014) When Drones Fall from the Sky, http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/

ValueSec Project, cost-benefit analysis of current and future security measures in Europe, http://www.valuesec.eu/

World Vision (2013) Participatory Scenario Planning for Community Resilience, Planning tool, UK. http://9bb63f6dda0f744fa444-9471a7fca5768cc513a2e3c4a260910b.r43.cf3.rackcdn.com/files/9813/7871/8703/Planning_For_Community_Resilience.pdf

Weblinks

http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-terrortrussel-7650037.html

http://www.dagsavisen.no/samfunn/krisepsykolog-advarer-mot-overdreven-frykt/

http://www.degruyter.com/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1732/jhsem.2010.7.1.1732.xml
http://www.enisa.europa.eu/media/press-releases/the-internet-interconnection-2018ecosystem2019-new-report-identifies-top-risks-for-resilient-interconnection-of-it-networks

http://www.falconunmanned.com/falcon-uav-news/2013/9/14/-falcon-uav-supports-colorado-flooding-until-grounded-by-fem.html

http://klassekampen.no/article/20140728/ARTICLE/140729963;

http://morgenbladet.no/samfunn/2014/et_glimt_av_usa#.VCLQI_mSx8E;

http://www.radicalgeography.co.uk/laquilasum.pdf
http://www.ramas.com/wttreprints/Myths.pdf;

http://rt.com/news/data-protection-rules-eu-491/

http://www.telegraph.co.uk/news/worldnews/europe/norway/8659028/Norway-shooting-July-24-as-it-happened.html

http://www.theguardian.com/technology/2014/jun/20/little-privacy-in-the-age-of-big-dat

http://www2.warwick.ac.uk/fac/cross_fac/cim/research/socialising-big-data/

Annex1: Overview of relevant Criteria per Category & Task

	Dimensions for task 92.1: Insecurities (Unease, Fear) and Secondary Risks													
	Emo. Insecurities		Secondary risks											
	1 Fear		2 Deploying technologies					3 Legality		4 Socio-economic				
Subcategory	**Unease**	**Suspicion**	**Function creep vs.Limitations**	**Applicability**	**Misuse**	**New Vulnerabilities**	**Technology Dependency**	**Legality**	**Truthfulness**	**Efficiency & Effectiveness**	**Impacts on market**	**Economic Stability**	**Employment**	**Measures as of WP/Tasks**
Category: Data & Information														
Collection & Storage	X	X	X	X	X	X	X	X		X				36.3, 43.1, 43.2, 43.4, 45.2, 45.3, 45.4, 52.4, 53.2, 55.3, 55.4
Facilitating Data Processing			X		X	X	X	X		X				43.5
Analysis & Evaluation	X	X	X		X			X						36.3, 43.1, 43.2, 43.3, 43.5, 52.4, 53.2, 55.4
Exchange	X	X	X		X			X	X	X				36.3, 43.1, 43.2, 43.3, 43.5, 52.4, 53.2, 55.4, 36.3
Category: Risk, Damage and Needs Assessment														
Gap analysis	X			X	X	X		X		X	X			34.1, 52.2, 53.1
Situational Analysis & Impact Assessment	X	X	X	X	X	X	X	X	X	X	X			43.2, 43.4, 43.5, 44.2
Early warning, Risk Analysis & Forecasting	X	X			X	X				X	X	X		43.1, 43.3, 44.1
Communication Systems			X	X	X	X	X	X		X				45.2, 45.3, 45.4
Category: Cross-border and Cross-Sectoral Interaction														

Cross-border and Cross-Sectoral Interaction	X	X	X	X	X	X		X		X				33.2, 36.3, 44.2, 45.2, 45.3, 45.4, 52.2, 53.1, WP55
Category: Communication between crisis managers and to the public														
Communication between crisis managers and to the public		X	X	X	X	X	X	X					X	35.2., 35.3, 35.4, 36.2, 43.3, 44.3, 45.3, 45.4
Category: Other Forms of Training														
Psychosocial	X		X	X				X					X	32.2, 32.3, 32.4
Media & Policy	X	X							X					35.2
Catetegory: Resilience Logistics & Contingency Plans														
Resources, Supply chains & Contingency Plans	X	X					X	X	X					44.1, 44.2, 44.4, 44.5, 46.1
Core functions in the city	X			X	X	X	X	X		X	X			34.1
Catetegory: Decision Support Systems & Simulations														
Decision Support Systems & Simulations	X	X		X				X						35.3, 44.1, 44.4, 44.5, 54.3
Category: Harmonization														
Harmonization	X			X		X		X		X		X		43.1, 54.1, 54.3

Category: Strategy Design														
For Community Resilience	X	X	X	X	X	X	X		X	X			X	WP33
For Early Warning & Risk Analysis				X			X	X	X					43.1, 43.3, 44.1
For Learning Activities & Lessons Learned	X	X		X	X	X	X	X		X				WP51, 52.2, 52.4, 53.1, 53.2, 55.1, 55.3
For Competence-Building	X	X		X	X	X		X	X	x				WP52
For Decision-Making	X			X	X					X				43.1, 54.1, 54.3
For Costs & Effectiveness Assessments	X	X	X	X	X	X			X	X				44.1, 44.5
Category: Methodologies for Selecting Measures & Assesing Impacts of Experiments														
Methodologies for Selecting Measures & Assessing Impacts of Experiments				X	X	X				X				SP2 & SP9