driver+

Driving Innovation in Crisis Management for European Resilience

D913.41 – A GUIDE ON ASSESSING UNINTENDED SOCIETAL IMPACTS OF DIFFERENT CM FUNCTIONS- VERSION 2

SP91 - PROJECT MANAGEMENT

JULY 2019 (M63)

This project has received funding from the European Union's 7th Framework Programme for Research, Technological Development and Demonstration under Grant Agreement (GA) N° #607798

Project information

Project Acronym:	DRIVER+
Project Full Title:	Driving Innovation in Crisis Management for European Resilience
Grant Agreement:	607798
Project Duration:	72 months (May 2014 - April 2020)
Project Technical Coordinator:	TNO
Contact:	coordination@projectdriver.eu

Deliverable information

Deliverable Status:	Final
Deliverable Title:	D913.41 – A guide on assessing unintended societal impacts of different CM functions- version 2
Deliverable Nature:	Report (R)
Dissemination Level:	Public (PU)
Due Date:	July 2019 (M63)
Submission Date:	17/07/2019
Subproject (SP):	SP91 - Project Management
Work Package (WP):	WP913 – Research ethics & Societal impact assessments
Deliverable Leader:	PRIO
Reviewers:	Tim Stelkens-Kobsch, DLR Marcel van Berlo, TNO Nicola Rupp, WWU
File Name:	DRIVER+_D913.41_A guide on assessing unintended societal impacts of different CM functions - Version 2.docx
Version of template used:	V2.2 – February 2019

Revision Table

Issue	Date	Comment	Author
V0.01	03/05/2019	Draft ToC	Stine Bergersen, PRIO, WP leader
V0.02	10/06/2019	Initial draft	Stine Bergersen, PRIO, WP leader
V0.03	19/06/2019	Contribution to section 8	Camilo Palacio, ARC, WP partner
V0.04	28/06/2019	Contribution to Sections 3, 4 and 9	Elodie Reuge & James Philpot, EOS, WP partner
V0.05	28/06/2019	Contribution to all Sections	Stine Bergersen, Bruno O. Martins & Emilie Hermansen, PRIO, WP leader
V0.06	03/07/2019	Second draft	Stine Bergersen, PRIO, WP leader
V0.07	12/07/2019	Peer review	Tim Stelkens-Kobsch, DLR
V0.08	15/07/2019	Peer review	Marcel van Berlo, TNO Nicola Rupp, WWU
V0.09	16-17/07/2019	Updated draft	Stine Bergersen, PRIO, WP leader
V0.10	17/07/2019	Final check and approval for submission	Tim Stelkens-Kobsch, DLR, Quality Manager
V0.11	17/07/2019	Final check and approval for submission	Marijn Rijken, TNO, Project Director
V1.0	17/07/2019	Final check and submission to the EC	Francisco Gala, ATOS

The DRIVER+ project

Current and future challenges, due to increasingly severe consequences of natural disasters and terrorist threats, require the development and uptake of innovative solutions that are addressing the operational needs of practitioners dealing with Crisis Management. DRIVER+ (Driving Innovation in Crisis Management for European Resilience) is a FP7 Crisis Management demonstration project aiming at improving the way capability development and innovation management is tackled. DRIVER+ has three main objectives:

1. Develop a pan-European Test-bed for Crisis Management capability development:
    a. Develop a common guidance methodology and tool, supporting Trials and the gathering of lessons learnt.
    b. Develop an infrastructure to create relevant environments, for enabling the trialling of new solutions and to explore and share Crisis Management capabilities.
    c. Run Trials in order to assess the value of solutions addressing specific needs using guidance and infrastructure.
    d. Ensure the sustainability of the pan-European Test-bed.
2. Develop a well-balanced comprehensive Portfolio of Crisis Management Solutions:
    a. Facilitate the usage of the Portfolio of Solutions.
    b. Ensure the sustainability of the Portfolio of Solutions.
3. Facilitate a shared understanding of Crisis Management across Europe:
    a. Establish a common background.
    b. Cooperate with external partners in joint Trials.
    c. Disseminate project results.

In order to achieve these objectives, five Subprojects (SPs) have been established. **SP91** ***Project Management*** is devoted to consortium level project management, and it is also in charge of the alignment of DRIVER+ with external initiatives on Crisis Management for the benefit of DRIVER+ and its stakeholders. In DRIVER+, all activities related to Societal Impact Assessment are part of **SP91** as well. **SP92** ***Test-bed*** will deliver a guidance methodology and guidance tool supporting the design, conduct and analysis of Trials and will develop a reference implementation of the Test-bed. It will also create the scenario simulation capability to support execution of the Trials. **SP93** ***Solutions*** will deliver the Portfolio of Solutions which is a database driven web site that documents all the available DRIVER+ solutions, as well as solutions from external organisations. Adapting solutions to fit the needs addressed in Trials will be done in **SP93**. **SP94** ***Trials*** will organize four series of Trials as well as the Final Demo (FD). **SP95** ***Impact, Engagement and Sustainability***, is in charge of communication and dissemination, and also addresses issues related to improving sustainability, market aspects of solutions, and standardisation.

The DRIVER+ Trials and the Final Demonstration will benefit from the DRIVER+ Test-bed, providing the technological infrastructure, the necessary supporting methodology and adequate support tools to prepare, conduct and evaluate the Trials. All results from the Trials will be stored and made available in the Portfolio of Solutions, being a central platform to present innovative solutions from consortium partners and third parties, and to share experiences and best practices with respect to their application. In order to enhance the current European cooperation framework within the Crisis Management domain and to facilitate a shared understanding of Crisis Management across Europe, DRIVER+ will carry out a wide range of activities. Most important will be to build and structure a dedicated Community of Practice in Crisis Management, thereby connecting and fostering the exchange of lessons learnt and best practices between Crisis Management practitioners as well as technological solution providers.

Executive summary

This deliverable uses the SIA Framework delivered in **D913.31** ***Societal Impact Assessment Framework-version 2*** (1), to carry out a set of exemplary societal impact assessments. The deliverable builds entirely on **D913.31** (1), where the framework that structures and guides the assessments was developed and presented. **D913.31** (1) is the foundation on which this deliverable is built and should be read in preparation of it. All information and documentation relating to how the SIA Framework and the methodology was developed, how the assessment criteria were selected, how feedback was gathered to revise the SIA Framework, etc. can be found in **D913.31**. However, a short recap of what the SIA framework looks like is given in this deliverable.

The ten exemplary assessments included in this deliverable are written based on the ten functional areas of the taxonomy of CM solutions that the DRIVER+ PoS is based upon (as presented in **D934.10** ***Taxonomy of CM functions for classification of solutions***) (2). One "function" is drawn from each of the "functional areas", and the assessments are made of those functions. The functions were chosen based on two selection criteria: *relevance* to that functional area and to CM more broadly, and *generalizability* within that same functional area. The selection was made by the lead authors of this deliverable, and the purpose of the example assessments is to demonstrate how the SIA Framework has been applied. Some of the assessments are of solutions selected from the Portfolio of Solutions (PoS), while others are selected for their importance in CM more generally and are not (currently) in the PoS. Some assessments are based on fictional solutions for illustrative reasons. With this approach the relevance of the SIA Framework to a broader CM community is increased, as well as the usability of the SIA Framework after the end of DRIVER+.

While the assessments all follow the five-step approach as described in **D913.31** (1), they vary to some extent in length and depth. This is a natural consequence of the qualitative approach to SIA which the DRIVER+ SIA framework has been based on from the beginning.

The set of assessments demonstrate that the SIA Framework can be applied to solutions also beyond the project. This is because all CM solutions can be categorized based on the functions of the DRIVER+ taxonomy of CM functions. Furthermore, some assessments are based on real-life technical solutions, and some are based on non-technical solutions such as methodologies and procedures. All in all, as with the DRIVER+ project as a whole, the deliverable takes on a rather broad concept of "CM solutions", meaning that a solution can be any means that contributes to a crisis management function; a solution is either one or more processes or one or more tools with related procedures.

The assessments are written by individuals with different professional backgrounds and different roles in CM, and the variation in the assessments is a testament to the fact that there is not one correct way of writing a societal impact assessment. However, the main goal was the same for all the authors when starting the work on their assessment: to identify potential and unintended societal impacts of the CM solutions that they are working with (or imagining working with).

TABLE OF CONTENT

List of Tables

List of Acronyms

Acronym	Definition
CM	Crisis Management
CTA	Constructive Technology Assessment
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
LEA	Law Enforcement Agency
PIA	Privacy Impact Assessment
PoS	Portfolio of Solutions
SIA	Societal Impact Assessments
SuIA	Surveillance Impact Assessment

1. Introduction

This deliverable contains ten societal impact assessments, conducted by using the DRIVER+ SIA Framework, which is delivered in **D913.31** ***Societal Impact Assessment Framework- version 2*** (1). The SIA Framework has been revised and updated throughout the DRIVER+ project, via SIA training sessions and the development during the Trials, and a description of all these developments and updates can be found in section 3 of **D913.31**.

All information relating to the background and development of the SIA Framework can be found in D913.31. The purpose of this current deliverable is only to collect and present the ten assessments.

The starting point for the assessments collected in this deliverable is that societal impact does not occur simply because a CM solution exists, but impact occurs as a solution is deployed or integrated into a certain societal context. As the assessments illustrate, in the same way that development of CM solutions is a dynamic process, so are the efforts to assess its societal dimensions.

As highlighted also by the ASSERT-project[1], most of the various established methodologies for assessing some sort of impact on society, such as constructive technology assessment (CTA), privacy impact assessment (PIA) or recent developments in surveillance impact assessment (SuIA) draw on the key term *reflexivity*. This also goes for the SIA framework presented here and means that engaging in critical reflexivity towards societal issues is the basis for the assessments presented here. Reflexivity in this context also means appealing to the capability of crisis managers (practitioners, decision-makers, stakeholders etc.) to reflect on their role in the CM process and scrutinize their activities with regards to societal impact.

The assessments presented in this deliverable not only identify potential negative impacts, but also demonstrate that societal impact assessments can identify opportunities for positive impacts. Furthermore, to carry out societal impact assessments as part of CM research on innovation contributes to creating a shared understanding of the societal impact and the CM culture, but also of larger scale research funding frameworks and policies, and how they contribute to the objectives of policies.

To increase internal consistency within DRIVER+, the taxonomy of functions that the SIA Framework is based on reflects the DRIVER+ taxonomy of functions which the Portfolio of Solutions (PoS) is based on. The DRIVER+ taxonomy of functions was developed to categorise the contents within the PoS and the Trial Guidance Tool and encompasses ten "functional areas"[2] (2). These ten functional areas are then divided in 54 functions, each of which is then further subdivided in sub-functions. In this context, an assessment of all the functions would not be possible and it would reduce the practical usability of the SIA framework. Thus, it was decided that a SIA should be done in one example in each of these ten functional areas.

The taxonomy of the PoS is the product of detailed discussions within the DRIVER+ community and is representative of the CM field. As previously mentioned, it is organised in ten Functional Areas: Mitigation; Capability Development; Strategic Adaptiveness; Protection; Response; Recovery; Crisis Communication and Information Management; Command, Control and Coordination (C3); Logistics; Security Management. These ten Functional Areas are characterised as being Preparatory, Operational, or Common. Annex 3 to

[1] A report containing a Societal Impact Assessment manual and Toolkit was published as part of ASSERT, which refer to this point. The report can be accessed online here: http://assert-project.eu/wp-content/uploads/2013/04/D3-1-23-April-2014-Final.pdf

2 This taxonomy is presented as an Annex of **D934.10**, and can also be found on the following webpage: http://pos.driver-project.eu/en/knowledge/taxonomies

this deliverable provides a table summarizing the DRIVER+ taxonomy, compiling the functional areas, the functions, and the sub-functions.

In sum, in this deliverable one function has been chosen for each functional area, and a societal impact assessment has been made on each. This chosen function from each area was selected based on two criteria, by the authors of this deliverable: *relevance* to that functional area and to CM more broadly, and *generalizability* within that same functional area. Some of the assessments are of solutions selected from the PoS while others are selected for their importance in CM more generally and are not in the PoS. With this approach the relevance of the deliverable to the broader CM community is increased as well as the usability of the SIA Framework after the end of DRIVER+. The objective of this deliverable is therefore to illustrate how the SIA Framework should be used, and not to provide SIAs of all the solutions included in the PoS.

In section 2, a short recap of the SIA Framework is presented. This is only a brief summary of the basic steps to take to carry out an assessment, and the full description of the methodology (the SIA Framework) can be found in **D913.31**. The template which was used to implement the SIA Framework, i.e. carry out the assessments, are also presented. After that, section 3 contains all the ten social impact assessments, as they were written by the contributors to this deliverable. Section 4 includes a short conclusion and way forward.

There are four Annexes to this deliverable:

1. Annex 1- DRIVER+ Terminology.
2. Annex 2- Template- A Guide for Assessing the Societal Impact of Crisis Management Solutions.
3. Annex 3- DRIVER+ Taxonomy of Crisis Management Functions.
4. Annex 4- List of societal impact assessment criteria.

2. A guide for assessing the societal impact of Crisis Management solutions

The SIA Framework consists of the template "A guide to assessing the societal impact of crisis management solutions" (Annex 2), as well as two supporting documents: 1) a taxonomy of CM functions and 2) a set of societal impact criteria. All three components are presented in detail in section 4 of **D913.31** (1). The SIA Framework, which has been used to carry out the ten assessments for this current deliverable, takes as its starting point that all CM solutions can be organized according to the functions that they have, and that these functions can be assessed against a set of impact criteria. This is done by following a five-step approach.

By using the template, the two other main components of the Framework can be linked: the *CM functions,* which are the objects which will be assessed and a set of societal impact *criteria,* which are what these functions are assessed against. Thus, applying the Framework means following five basic steps, each containing a set of guiding questions:

1. Identify stakeholder groups/ communities.
2. Collect background information.
3. Get an overview of legislation and policies.
4. Identify and predict impacts.
5. Describe mitigating measures and follow up.

The result of following the five steps is a written assessment of what potential positive and negative societal impacts a certain CM solution has. The ten assessments collected in section 2 illustrate how this can look like in ten various cases and for ten various solutions.

In the template in Annex 2, the guide that facilitates the assessment of the social impact of Crisis Management solutions, via the five steps, is presented. The template and its instructions were used to carry out all the ten assessments which are collected in the remainder of this deliverable. As described in section 1, the ten assessments were selected, one from each functional area of the taxonomy of CM functions, by the authors of this deliverable, who also wrote the assessments. The suggested length of an assessment is very hard to define as part of such a template, since the complexity and extent of the content will vary significantly depending on the solution at stake or the context in which it is being deployed. The template was also included in section 4 of **D913.31** ***Societal Impact Assessment Framework- version 2*** (1).

Based on the application of the SIA Framework during the project, especially at the SIA training during the I4CM conference in June 2019 and during the production of this deliverable, the application of the Framework has proved to be rather uncomplicated. Instructions were sent to the contributors of this deliverable, and the assessments were carried out with very little explanation or need for clarification. What has been the most recurring challenge is that the SIA Framework, and its three components (template, taxonomy of CM functions and list of impact criteria), makes up a substantial number of pages, and that the full set of documents might seem a bit overwhelming. The SIA training modules (**D913.52**, due in M66), which will provide training for individuals who want to make use of the SIA Framework aims to lessen this potential risk. The assessments have been carried out by individuals, and by teams of individuals from the different partner organizations contributing to this deliverable. Based on this experience, it seems that there is an added value of carrying out the assessment as a team effort, or at least to make an initial draft in cooperation with the other stakeholders working with the solution, which can then be further developed by one or more individuals. In this way, a broader set of experiences, backgrounds and knowledge can form the basis for the assessment. Eventual disagreements are likely to happen, but these should be documented and interpreted also as an additional value to the process, as they might help the

stakeholders in deepening their understanding in how societal impact can be complex and dynamic. More details on the assessment process, and how it can take place, can be found in **D913.31** (1).

2.1 Assessment from functional area "Mitigation"

0 General description of solution

Solution to be assessed: Drones.

Drones (Unmanned Aerial Vehicles) can be used by Crisis Management practitioners to gather a large variety of data in multiple environments. They can be loaded with sensors and flown over hazardous areas that would normally present danger to manned assessment. They require a trained operator to use and can be limited in speed and range but can also access areas that would otherwise be impossible to assess.

1 Stakeholder groups / communities

There are three main stakeholders involved in scenarios that require a risk assessment.
Firstly, there are the communities that are present in the area that requires assessment. These communities could either be directly affected by a crisis, such as residents of a building that has a gas leak, or they could simply be present in the area at the time of the assessment.

The second group are the operators of the surveillance system. These are likely to be either emergency services or belong to a private company. This group can include those that operate the drones, as well as those that are receiving and analysing the data. An important part of this group are also the decision makers, who are responsible for not only deciding which areas or risks need to be assessed, but also how the results or conclusions of the data are used and shared.

The final group that may be affected by this function are other members of a society. Unless it is undertaken in a very remote location, it is likely that the tools for undertaking the assessment – in this case, drones – will be quite visible and therefore the civil population can be considered a stakeholder for this function.

2 Background information

For the groups identified above, generic demographic information for a particular society or country is likely to have already been gathered. For example, it is likely that a lot of socio-economic indicators, such as those listed below, will already have data available.

Examples of information that may already be collected are:

- Unemployment.
- Family related data-Demographics.
- Community leaders.
- Infrastructure.
- Population.
- Housing availability.
- Education.
- Risk awareness.
- Environmental.
- Access to adequate health services.
- Community culture.
- Existing groups and institutions.
- Social structure.

Table 2.1: Community Characteristics (3)

Demography	*Culture*	*Economy*	*Infrastructure*	*Environment*
Population and age distribution	Traditions	Trade	Communication networks	Landforms
Mobility	Ethnicity	Agriculture/livestock	Transportation networks	Geology
Useful skills	Social values	Investments	Essential services	Waterways
Hazard awareness	Religion	Industries	Community assets	Climate
Vulnerable groups	Attitudes to hazards	Wealth	Government structures	Flora and fauna
Health level	Normal food types		Resource base	
Education level	Eating habits			
Sex distribution	Power structures			

Some specific issues that need to be considered are the social connotations connected with drones, or any type of aerial surveillance to perform a risk assessment. In Western societies, they are mostly considered as vehicles that are used for benevolent purposes, either business or leisure. Other societies, or communities, may have negative experiences with UAV's, particularly if they have experienced conflict, and this may lead to specific issues with the implementation of this function amongst certain communities or diasporas.

3 Relevant legislation and policies

There would be two areas of relevant legislation to consider for this function: The use of private data and any regulations regarding the means of data collection. Firstly, legislation regarding private or personal data is a consideration if certain types of data are being collected. Legislation such as GDPR will govern how data in the EU can be used and distributed.

Secondly, legislation regarding the operation of certain vehicles may have a restricting effect on the ability to use certain tools. Regarding the solution of sensors operated by drones, it is likely that there are local airspace regulations concerning the use of drones in urban areas, restricting their use as a tool in certain scenarios.

4 Identify and predict impacts

Unease - Calmness	**Suspicion - Trust**	Misuse - Protection	New Vulnerabilities - Progress
Technology dependency – Flexible solutions	Function Creep – Specialized and controlled use	Sustainability	Accountability
Transparency	Integrity	**Negative – Positive Standardization**	International relations
State-Citizen-Relationship	Political Reputation	Social Cohesion and Solidarity	Participation
Diversity	**Open – Control Society**	Cultural and Gender Sensitivity	Suitability, Necessity and Proportionality

In/justice & In/equality	Dignity/Autonomy	Non-discrimination	**Privacy & Data Protection**
Freedoms and Protest			

Open-Control Society. The use of airborne surveillance to gather data in response to a crisis may begin to normalise the idea of aerial surveillance, operated either by the intelligence services or Law Enforcement Agencies (LEA). If the sensors are transported by UAV's, this could contribute to developing a more controlled society, where the population can be monitored through the use of this function. This has an overlap with the criteria of negative standardisation. A further issue that arises regarding this criterion is how the data that has been gathered is stored and potentially used after the crisis. If it is available for LEA's, it may be that gathering data to assess risks can result in information about a community or region being used for security reasons.

Privacy and Data Protection. As mentioned above, aerial surveillance with gather a range of data that is necessary to perform the risk assessment. It is likely that in the course of gathering this data there will be information gathered on individuals that would not normally be available publicly, especially if the gathering takes place in an urban setting. The gathering of private data may be a concern for citizens. Further to this, even though private data may not be gathered via the sensors, there may be a *perception* that it will be collected, which may impact citizen's trust in the practitioners. This will overlap with the transparency criteria.

Freedoms and Protest. If individuals have the opportunity to register problems or seek reassurances regarding the process of accessing risks, using drones may not be a solution that facilitates this, as identifying who the drone is operated by and its purpose will not be easy, therefore meaning that citizens do not know who to seek answers from. This again overlaps with transparency.

Suspicion and Trust. As mentioned previously, it may not be easy for citizens to identify certain tools that are being used to gather the data that will be used to undertake the risk assessment. Therefore, without the proper information they cannot be certain that the tools are being used benevolently and that the data gathered is being used benevolently. As mentioned in the background information, given different communities experiences with drones, they could be viewed with suspicion. This again overlaps with transparency.

Technology Dependency. If the function 'assess the risk' is served through analysing data collected by drones, this runs the risk of the technology (UAV's) being unavailable. This may happen if there is inclement weather, if the terrain is unsuitable for the collection of data via aerial surveillance or if the type of data that is required cannot be gathered using UAV's to transport the sensors. If there is no other way to gather the data required, then the function 'to assess the risk' will be compromised.

Transparency. As already mentioned with several other criteria, transparency regarding the gathering and analysis of data can increase the public's trust in a solution and acceptance. Ensuring the information is available about the reasons for using UAV's, the types of data that is being gathered and why it is needed, and the results of the assessment will help improve the transparency of the solution.

Negative standardisation. The use of the drones to perform the function 'assess the risk' can create a negative standardisation, whereby it becomes commonplace for UAV's to be used by emergency services or LEA's for surveillance. This can also cause issues of function creep, as surveillance and sensor data is gathered and used for more purposes than simply risk assessment.

5 Mitigating measures

There are several measures that can be implemented to ensure that the negative consequences identified

in the previous step are mitigated as much as possible.

Firstly, it is clear that communication with the affected communities will be vitally important. Informing them of the likely presence of UAV's, the intentions behind the surveillance and the results of the data analysis will help prevent them from forming their own, possibly negative, ideas about the purpose of the drones, and will help prevent many of the negative impacts resulting from questions of trust and suspicious activity. Likewise, openly telling the public about the use of drones to assess risks will provide them with an opportunity to register feedback, thereby minimising the impact of citizens not having freedom to register disapproval of a solution. Explaining the type of data that is being gathered and why it is gathered will help disperse privacy concerns.

The second mitigating step that needs to be taken is to have a clear overview of the type of data gathered and whether this data is likely to impact on the privacy of individuals. An important part of this will be to have a plan for the storage or disposal of the gathered data after the assessments have been made, depending on whether the data needs to be retained or not. This will show that sensitivities towards private data are being respected, and that individual's privacy will not be impacted without due consideration. This will also allow for individuals to understand how and why their data may be used.

Thirdly, a key factor is to ensure that the sensors are only gathering the specific data required for the risk assessment this will help to reduce function creep and negative standardisation, by restricting opportunities for the application of drones and sensors to be used to gather data for other purposes than risk assessment.

2.2 Assessment from functional area "Capability Development"

0 General description of solution

Solution to be assessed: PROTECT.

PROTECT application is a web-based alert and notification system for emergency (and early warnings) situations concerning civil protection. The main concept behind is to monitor and control emergencies and to manage a pool of resources to support the assistance provided during emergencies. PROTECT uses a map oriented user approach powered by the know-how and skills from Alert4All[3], featuring the monitoring and reporting on the development of each scenario, management of all documents related to the scenario, management and dissemination of messages and notifications, collection and retrieval of lessons learnt.

1 Stakeholder groups / communities

- The first group are the communities affected by the crisis.
- The second group are the emergency responders.
- The third group are the CM practitioners using the PROTECT system.
- The fourth group are the public that receive the alerts from the system.

[3] Alert4All is a research project funded under FP7- SECURITY. Alert4All focuses on improving the effectiveness of one element of the People-Centred Early Warning Systems paradigm, namely alert and communication towards the population in crises management. More info on the project can be found here: https://cordis.europa.eu/project/rcn/98427/factsheet/en

- The fifth group are the decision makers who will control the use of the system and how resources are allocated, based on other factors than just CM (politicians).

2 Background information

If the system is sending public alerts, it is important to understand the audience for these alerts. Such factors to consider would be: language skills, access to the technology required to receive the message, are they from a community that is likely to have trust in emergency services/authorities. CM practitioners and decision makers need to understand their background to avoid any biases when allocating resources. Previous experience in the tool is positive or negative. Whether the system is vulnerable to manipulation. Where are the resources and different entities involved from – are they all local or are there national or international groups involved.

3 Relevant legislation and policies

- **Sendai Framework for Disaster Risk Reduction**
- The Sendai Framework for Disaster Risk Reduction 2015–2030 was adopted at the Third UN World Conference in Sendai, Japan, on March 18, 2015. The Framework ensures continuity with the work done by states and other stakeholders under the Hyogo Framework for Action (HFA) 2005–2015: Building the Resilience of Nations and Communities to Disasters.
- **General Data Protection Regulation – GDPR**
- The GDPR is a regulation in EU law on data protection and privacy for all citizens of the European Union and the European Economic Area. It aims to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
- **Charter of fundamental rights of the European Union (2016/c 202/02)**
- The Charter of Fundamental Rights of the European Union (the Charter) brings together the fundamental rights of everyone living in the European Union (EU). It was introduced to bring consistency and clarity to the rights established at different times and in different ways in individual EU Member States. The Charter sets out the full range of civil, political, economic and social rights based on:
    - The fundamental rights and freedoms recognised by the European Convention on Human Rights.
    - The constitutional traditions of the EU Member States, for example, longstanding protections of rights which exist in the common law and constitutional law of the UK and other EU Member States.
    - The Council of Europe's Social Charter.
    - The Community Charter of Fundamental Social Rights of Workers.
    - Other international conventions to which the EU or its Member States are parties.

4 Identify and predict impacts

Unease - Calmness	**Suspicion - Trust**	**Misuse - Protection**	**New Vulnerabilities - Progress**
Technology dependency – Flexible solutions	Function Creep – Specialized and controlled use	Sustainability	**Accountability**
Transparency	**Integrity**	Negative – Positive Standardization	**International relations**
State-Citizen-Relationship	Political Reputation	**Social Cohesion and Solidarity**	**Participation**
Diversity	Open – Control Society	**Cultural and Gender**	Suitability, Necessity and

		Sensitivity	Proportionality
In/justice & In/equality	Dignity/Autonomy	**Non-discrimination**	**Privacy & Data Protection**
Freedoms and Protest			

Social cohesion and solidarity. Alerts may only be received by certain groups or communities, undermining social cohesion. If resources are not allocated fairly among different groups affected by a crisis, it may undermine solidarity within a society.

Participation. If society or communities are involved in the creating of the principles that drive CM decision making and the allocation of resources through the system, they are more likely to accept the decisions that are made, as they had the opportunity to contribute and register their opinion. If decisions are made that are opaque, it may undermine the effectiveness of the tool as the public does not accept them and therefore seeks redress.

Diversity. Different groups may need representation in the system, to ensure that the requirements of each group are clearly articulated and understood by the team making the decisions. Resource management may otherwise reflect the internal biases of the system or decision makers.

Cultural and Gender Sensitivity. Being aware of any resource requirements or extra care that may be needed due to cultural or gender factors will help decision makers better allocate resources, and will lead to a better crisis response as the emergency services are able to deliver more effective and specialised aid.

In/justice and In/equality. If resources are unfairly allocated then there will be a negative societal impact as the groups that do not receive a fair share will suffer a greater effect from the crisis, and will feel unfairly treated.

Non-discrimination. Those that aren't connected to the alert system may be discriminated against if there are no other means of communicating the danger or safety messages. Likewise, if the groups that are experiencing the crisis are not well represented in the system, allocating resources may lead to discrimination.

Privacy and Data Protection. If individuals have to subscribe to system using personal data, and perhaps allow location tracking to receive alerts then there maybe concerns over their privacy and who the data is shared with.

Unease-calmness. If the alerts are not well written and do not provide actionable, helpful information, it may create greater unease in the population as they know that something is amiss, but cannot take action to feel more secure. Furthermore, if it is seen that resources are being moved to certain areas, or emergency figures mobilised without an explanation, it may create panic.

Suspicion and Trust. If the decision makers are clearly identifiable and the source of the alerts is clear, the audience is more likely to have trust in the message and follow the instructions. As mentioned, if resources are moved without explanation, it may create suspicion.

Misuse/Protection. If the system incorrectly allocates resources, based upon a lack of information or wrong decision, it will undermine the protection of the affected groups.

New Vulnerabilities – Progress. Using an online system means that it is vulnerable to cyber-attacks or malicious actors.

Technology Dependency – Flexible Solutions. For effective resource management it requires that all CM practitioners are able to access the system. It may be the case that the crisis interrupts the ability to do so, meaning that the system is undermined. Likewise, the alerts can only be received by those connected to the internet, meaning that a secondary system is necessary.

State-Citizenship Relationship. Citizens trust the state to correctly allocate CM resources for their protection. This can be affected by participation, as explained earlier. Incorrect allocation or perceived unequal allocation may result in the relationship being damaged and reduced trust in the CM institutions.

Transparency. If the decisions made about allocating resources are recorded in the system and reasons why, it means that citizens will have better access, and therefore if necessary are able to hold decision makers to account. This means that they are likely to make fairer and non-biased decisions about allocating resources. This also affects accountability.

Accountability. The hierarchy of decision makers in the system should be clear, so that when instructions are given they are followed immediately.

Integrity. The principles guiding the allocation of resources are decided previously, possibly using participation, and during a crisis that are adhered to.

International Relations. If the crisis crosses borders, it may be required to communicate and involve emergency responders from other countries. If they are integrated into the system, it is important that the principles of their engagement and their knowledge of the system and available resources are established quickly and effectively.

5 Mitigating measures

The key mitigating step will be to ensure that the principles and guidelines that govern how resources are allocated are clearly established prior to the crisis and possibly created using public participation; at the very least they should be publicly accessible so that the community is able to understand the principles and potentially register disapproval.

If this is done beforehand, it means that resource allocation will be managed fairly and equitably among those affected by a crisis, leading to greater social cohesion and solidarity, and more trust and acceptance of the system.

For those receiving the alerts, it should clear who the message has come from and what the recommended course of action is. This will increase their security and trust in the system, meaning that they are more likely to follow the safety instructions. It is also important to inform citizens of other means of communicating safety instructions, as not all will be able to receive alerts sent via Protect, so promoting other communications channels that use different technology or are available in different languages will be an important step for mitigating this potential discrimination.

2.3 Assessment from functional area "Strategic Adaptiveness"

0 General description of solution

Solution to be assessed: Algorithm-based predictive police system.

This solution creates an algorithm aiming at predicting likely crimes and its likely perpetrators. It aims at enhancing proactive policing and improve intervention strategies based on data about previous crimes. This data can lead to an identification of locations, people, and scenarios that are at a higher risk of crime. The algorithm is developed with data input from previous crimes, suspect profiling, geo-location of previous crimes, and other social factors that are understood to be potential crime triggers. Regarding the SIA Functional Area, this solution deals with Strategic Adaptiveness (a preventive function, as defined in the taxonomy of CM functions), more specifically the function "Conduct civil security foresight". The function includes solutions that identify key drivers and trends, that identify plausible futures, and that explore the implications of alternative futures.

1 Stakeholder groups / communities

This solution requires interventions from two main groups of people. Firstly, the main stakeholders are the technology developers that build the algorithm. Secondly, the main end-users are law enforcement agencies.

This solution will then affect the community at large, but in particular the members of the social groups identified as being at higher risk, as well as the inhabitants of the areas that are understood to be more likely to witness crime.

2 Background information

Predictive policing is rapidly becoming an instrument used by law enforcement agencies in different parts of the world, from the US to the EU and India. The use by the police of predictive methods is part of a larger dynamic by which algorithms take part in the judicial system.

Predictive policing methods are often understood as falling into four general categories: methods for predicting crimes, methods for predicting offenders, methods for predicting perpetrators' identities, and methods for predicting victims of crime. Their use has been subject of high contention. While its advocates argue that they can contribute to anticipating future crimes (and therefore to mitigate them) and to devise long-term strategies, its contesters argue that these methods stigmatize specific segments of the population, they target areas that are typically already challenged by other socio-economic factors, they are based on causal nexus that are often not fully established in criminological sciences, and they are not colour or race blind.

Recent reports have shown some of the problems associated with these methods. Research from the AI Now Institute, for example, has shown that police across the US are training crime-predicting AI´s on falsified data (4), highlighting how supposedly objective systems can perpetuate corrupt policing practices. Civil liberties organizations have demonstrated that law enforcement agencies increasingly let computers search for data patterns and sometimes draw far-reaching conclusions from the findings, which poses certain risks to human rights. Finally, these methods often pose transparency problems, given that the mathematical formulae of the algorithm are often developed by private companies that do not disclose them.

According to a recent study by Albert Meijer and Martijn Wessels, the existing "empirical evidence provides little support for the claimed benefits of predictive policing. Whereas some empirical studies conclude that predictive policing strategies lead to a decrease in crime, others find no effect. At the same time, there is no empirical evidence at all for the claimed drawbacks". The authors conclude that "the

current thrust of predictive policing initiatives is based on convincing arguments and anecdotal evidence rather than on systematic empirical research" (5).

3 Relevant legislation and policies

A key concern with predictive policing is that national and international legislations are often not fully equipped to deal with it. Whereas constitutional and procedural provisions about surveillance and due process apply, they are often either not observed or cannot be enforced, due to the lack of transparency surrounding the algorithms.

Data about people and neighbourhoods are inserted in the algorithm without information for the subjects, and therefore they cannot know that they are target of specific measures that impact their daily lives.

4 Identify and predict impacts

Unease - Calmness	**Suspicion - Trust**	**Misuse - Protection**	New Vulnerabilities - Progress
Technology dependency – Flexible solutions	**Function Creep – Specialized and controlled use**	Sustainability	**Accountability**
Transparency	Integrity	Negative – Positive Standardization	International relations
State-Citizen-Relationship	Political Reputation	**Social Cohesion and Solidarity**	Participation
Diversity	Open – Control Society	**Cultural and Gender Sensitivity**	Suitability, Necessity and Proportionality
In/justice & In/equality	Dignity/Autonomy	Non-discrimination	Privacy & Data Protection
Freedoms and Protest			

Suspicion- trust, state- citizenship relationship, social cohesion, solidarity. The use of algorithms for predictive policing has many potential societal impacts. These methods interfere with the equation suspicion vs. trust, as the suspect profiling operated by the solution erodes the trust in the criminal system. By this, it carries the potential to impact the state / citizen relationship, therefore affecting social cohesion and solidarity.

Technology dependency. Transparency. Accountability. As mentioned before, while the solution can provide support to decision-making and strategic planning, it raises new challenges that did not exist beforehand. From this perspective, they foster a technology dependency that is not sufficiently sustained by empirical studies. At the same time they raise questions of transparency and accountability, given that the criteria according to which people or areas are selected as being of high risk of crime are normally not provided.

An additional potential impact has to do with misuse of the solution and function creep, i.e. the use of the solution for a different purpose or function that the one that it was created for. Even though this is a risk associated with many technological innovations, it is particularly relevant in cases such as this, where issues of privacy, procedural and constitutional rights, and societal trust are at stake.

Finally, several studies have also pointed out that predictive policing disproportionately impact racial minorities and it often does not exhibit cultural and gender sensitivity. Specific communities and areas are often targeted by the algorithm and impacted more than the average. As technology is never neutral,

common values and prejudices found in the society at large are often reflected upon the technology, even if unwittingly.

5 Mitigating measures

To mitigate the anticipated potential impacts, the solution needs to attend the highest legal standards, including norms that deal with both procedural and constitutional rights.

Potential problems with transparency should be addressed by making available information about the functioning of the algorithm, the data that it is based on, and the impact the results have on judicial and policy decisions. Additionally, particularly affected population and neighbourhoods should be informed about their inclusion on high-risk lists. This mitigation action is crucial to ensure accountability in case problems arise and to allow judicial screening and contestations.

In order to pre-emptively face potential societal impacts, the development of the algorithm should be monitored by a national ethics committee, so that the highest standards of research ethics can be observed.

These mitigation measures are needed in order to ensure a healthy citizen / state relationship and high levels of societal trust.

2.4 Assessment from functional area "Protection"

0 General description of solution

Solution to be assessed: Privacy Impact Assessment (PIA).

A Privacy Impact Assessment, or PIA, is an analysis of how personally identifiable information is collected, used, shared, and maintained. In Crisis Management, a PIA can be an important tool especially during the development of technical solutions. Such technical solutions can be solutions devised to protect critical information infrastructure (CII), which, if damaged, would cause harm to people, the economy or the country, etc. The ability to connect different technologies in Crisis Management has enabled an increase in broad interagency collaboration. This development has occurred alongside a move to accumulate and analyse for example crowdsourced responses. Given the scale and the nature of the information accessed and collected, there is a pressing need to ensure that technology is developed in a way that protects the interests of end-users and stakeholders. Privacy impact assessments (PIAs) are increasingly used, and in certain jurisdictions legally mandated, to foresee risks to privacy and to plan strategies to avoid these (6). Under GDPR, a data protection impact assessment must always be conducted when the processing could result in a high risk to the rights and freedoms of natural persons. Such an assessment is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals and is specifically required at least in the following cases: 1) a systematic and extensive evaluation of the personal aspects of an individual, including profiling; 2) processing of sensitive data on a large scale; 3) systematic monitoring of public areas on a large scale.

1 Stakeholder groups / communities

There are several groups and stakeholders that might be affected by doing a PIA, but the main group are those individuals whose personal data is being collected and processed, and eventually protected by using this solution. Other stakeholders might be National Data Protection Authorities or maybe even the European Data Protection Board. In addition, the "owners" of the solution, i.e. the end-users and the

organization or the people in the organization deciding to carry out a PIA are considered a stakeholder in this case. A final group of stakeholders might be the solution developers, i.e. the people working on improving and revising the PIA templates and guidelines.

2 Background information

In the European context in particular, the awareness of and knowledge about data protection and privacy issues have increased in the last decade. There are several reasons for this, but one development, also highly relevant for Crisis Management, is the emergence and use of new technologies that operate based on the collection of personal data from individuals. For example, crowdsourced responses to crisis include the gathering and analysing data collected from individuals. The implementation of GDPR in May 2018 are expected to have had an impact on the general awareness of data protection and privacy issues in the population. There have been many debates in relation to the introduction of the new legislation, in academia, policy circuits, but also in popular media. The debates often critically discussed the new regulation. One reason that the general population are expected to have increased their awareness of data protection and privacy issues, However, there is also some resistance to the idea that privacy is a value that should be protected to the extent which it is. Statements such as "I have nothing to hide, so it doesn't matter" are evidence of that. In addition, big events and controversies such as data breaches by Facebook, the Snowden-revelations and cyber/phishing attacks where millions of passwords are leaked from databases gained significant public attention and to some extent influenced the general population on these issues. The GDPR requirement which meant that companies holding personal data for example in the shape of mailing lists had to ask again for the consent of people on those lists, have for many people been a repeated reminder of these issues. Certain features of the population in which the PIA solution is to be implemented are also relevant, for example the level of trust in the government institutions, law enforcement agencies and emergency services.

3 Relevant legislation and policies

The most relevant legislation is GDPR, which was introduced in May 2018 to harmonize data privacy laws across Europe, but there are also other policies and documents that are relevant.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Guidelines by national Data Protection Authorities.
- National regulations on data protection and privacy.
- Official Journal of the European Communities (2000), *Charter of Fundamental Rights of the European Union C 364/1,* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.
- ISO/IEC 29134:2017(en) Information technology — Security techniques — Guidelines for privacy impact assessment.
- EDPB Guidelines on Data Protection Impact Assessment (DPIA).
- United Nations, (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948.
- CoE (1950), European Convention on Human Rights, CETS No 005, 1950.
- EU Article 29 Working Party (A29) has defined nine criteria for high-risk processing. The categories include:
    - Evaluation or scoring.
    - Automated decision making that has legal effects.
    - Systematic monitoring.
    - Processing of sensitive data.
    - Data about vulnerable subjects.
    - Data on a large scale.
    - Datasets that have been matched or combined.

- Development of new technology or innovative use of existing technology.
- Processing that prevents individuals from exercising a right or using a service or contract.

4 Identify and predict impacts

Unease - Calmness	**Suspicion - Trust**	Misuse - Protection	New Vulnerabilities - Progress
Technology dependency – Flexible solutions	Function Creep – Specialized and controlled use	Sustainability	**Accountability**
Transparency	Integrity	Negative – Positive Standardization	International relations
State-Citizen-Relationship	Political Reputation	Social Cohesion and Solidarity	Participation
Diversity	**Open – Control Society**	Cultural and Gender Sensitivity	Suitability, Necessity and Proportionality
In/justice & In/equality	Dignity/Autonomy	Non-discrimination	**Privacy & Data Protection**
Freedoms and Protest			

Unease/ calmness. By doing a PIA, the responsible entity can mitigate the unease that might exist in the population, with reference to the increased awareness of data protection and privacy issues as described above. This can happen because doing a PIA is expected to have a positive impact on accountability, and thus calm down insecurities related to privacy.

Suspicion/ trust. The very act of doing a PIA can be interpreted as a way for an organization to gain trust from the public, and mitigate potential suspicion surrounding how the organization handles data protection issues. In addition, it can be said to demonstrate to collaborators, customers, contractors and employees that privacy is properly taken into account by the organization.

Transparency. Doing a PIA can measure the organization's ability to keep personal information safe, and by documenting this process in a clear and open manner the organization appears more transparent and accountable.

Accountability. Doing a PIA might enhance and inform the decision-making processes within the organization, and thus have a positive impact on its accountability.

Open/ control society. Doing a PIA is about seeking to reveal privacy risks and detect potential problems so that they can be taken care of via preventive safeguards, instead of being discovered at a later stage when these risks might have become more acute- or actual threats. An open society values privacy, and measures to pre-emptively protect privacy such as a PIA, will positively impact society in the sense that it becomes less closed and controlled, and more open and transparent. This of course relies on the follow-up after the PIA is made. If risks and mistakes are revealed without any follow-up, this can be seen as a sign of a negative form of control, leaving individuals maybe more vulnerable.

Privacy & data protection. The potential negative societal impacts of doing a PIA are to a significant extent related to criticism of the very concept of PIA. There is a general consensus that using such a solution to better protect people's privacy is in itself a good thing, but there are also some pitfalls. For example, there is a risk that the assessment is done just to tick off a box, without putting too much effort or care into the assessment. And there is the risk that the assessment process is not done in the correct way, or that necessary mitigating measures are not implemented if risks are identified. Uncovering privacy risks without doing anything to lessen the risks, might leave the solution user vulnerable. Positive impacts might be that potentially costly mistakes can be avoided.

An organization may use a DPIA, even if a DPIA is not required, to conduct an assessment to ensure the required data protection controls are in place and to demonstrate compliance with GDPR requirements. DPIAs are required of organizations acting as Data Controllers. Data Processors may also use DPIAs to assess whether they are processing data in a manner that supports the Controller in meeting its compliance obligations under the GDPR (7).

5 Mitigating measures

In sum, the expected positive impacts of doing a PIA by far exceed the potential negative impacts. After deliberation, it is concluded that the negative impacts are mostly seen as risks in occasions where the PIA is not used correctly, such as in instances where privacy risks are uncovered and not followed up on. In such cases, a seemingly "neutral" solution such as a PIA might actually create significantly negative societal impact. Thus, mitigating measures and follow-up from the assessment by using the impact criteria in the previous step relate mostly to how to ensure that a PIA is done properly. These measures are described and reflected upon in the following.

To make sure that the PIA is done correctly, and according to the regulation, GDPR Article 35 should be considered. It provides four elements that a privacy impact assessment must contain: (1) a systematic description of the processing operations and their purposes; (2) an assessment of the necessity and proportionality; (3) an assessment of the risks; and (4) the measures needed to address the risks. Furthermore, other examples of risk mitigating measures could be to update privacy notices as necessary, honouring opt-outs, and to make sure to have and maintain a security program, including an incident response plan in place to detect and respond to data breaches. Follow-ups should be carefully provided after a potential breach.

In order to make sure that the PIA process is transparent and positive for the accountability of the assessor, the PIA methodology should be properly documented. The stakeholder groups should to a certain extent be made aware of the assessment process and should be engaged to participate in the process. The assessment could also be done several times to ensure that it is carried out in the best possible manner, this will also demonstrate compliance and effective management of risks. All identified risks should be followed up and reacted to.

2.5 Assessment from functional area "Response"

0 General description of solution

Solution to be assessed: Crisis communication system.

The solution is a crisis communication system that is to be implemented in Portugal. The solution would provide the community with a communication channel with the law enforcement in crisis situations. The solution will also be used to communicate between different bodies of the Crisis Management, i.e. law enforcement agencies and fire brigades. The solution makes it possible with a reverse 112, meaning that official authorities can communicate information of threats and evolving crisis to the public (8). The main purpose of the communication system is the early detection of crisis situations and then to limit the impact of the crisis with a quick response. When a person is reporting for example rural fires or a terrorist attack, the system automatically detects the position of the caller and makes it easier to find the exact location of the event.

1 Stakeholder groups / communities

- The crisis affected community.
- Law enforcement agencies.
- Fire brigades.
- Emergency services.
- Government.
- Civil defence corps (Autoridade Nacional de Proteção Civil) and volunteer organisations.
- International cooperation partners in Crisis Management.

2 Background information

Portugal has challenges related to the increase in rural fires during the warmest summer months. Portugal is seen to be prone to rural fires because of climate changes making the summer periods longer, warmer and extremely dry. In addition, major changes in the land use as for example agricultural abandonment have led to big areas with woody vegetation in abandoned farmlands (9). The increase of rural fires also leads to the production of landscapes with vegetation that has higher flammability.

Portugal is situated in an earthquake zone and has experienced a number of major earthquakes. In 1755, an earthquake with epicentre close to the capital, Lisbon, is known to be one of the deadliest earthquakes throughout world history. 90 per cent of all buildings in the city were damaged during the earthquake, in the following tsunami and fires in the days following. There have also been two major earthquakes in 1909 and 1969 and latest on January 18th 2018 with a magnitude of 4,9 leading experts to indicate that a bigger earthquake might come in the close future (10). Earthquakes can also lead to tsunamis in the coastal areas of Portugal. The risk of crisis situations in Portugal is therefore closely related to natural disasters and rural fires.

In June 2017, the emergency services in Portugal were battling the deadliest rural fires in the country's history with 64 dead and 254 injured. The emergency communication network, SIRESP (Sistema Integrado de Redes de Emergência e Segurança de Portugal), has been put to blame, as multiple emergency calls from the population did not reach the law enforcement agencies and fire brigades (11). One of the main issues with the existing emergency communication system is that it relies on aerial cables and these cables are vulnerable when there is a rural fire due to the risk of them burning down (12). The existing crisis communication system is therefore not satisfying the demand to protect the safety of the population as it might break down in times of crisis.

Due to the increase in rural fires and mortal consequences, the Portuguese government has put through different measures in order to make the community more resilient to the fires. A website has been created to display on-going and completed forest fires where the population is informed through a map indicating the severity of the fire, location, etc.[4]. The Government has also worked on engaging the population in the preventing of rural fires through a ruling issued in February 2018 that demands landowners to clear fire-prone vegetation around their homes and villages (13). The ruling has been celebrated based on the fact that the population generally have been more attentive to their role in the prevention of rural fires, but the critique has also been overwhelming. Land owners complains because they have been given to much of a burden in the clean-up process. In addition, the Government used the Tax Authority's database for a big email campaign that gave landowners three weeks to clean up fire-prone vegetation or pay fees up to €5,000.

3 Relevant legislation and policies

- **The Sendai Framework for Disaster Risk Reduction**[5] recognises the strong role that science can play in improving the understanding of risk and communicating on new knowledge and innovation.
- **Directive of the European Parliament and of the Council establishing the European Electronic Communications Code**[6] defines the way emergencies is to be handled across EU countries. It includes establishing a reverse 112 that will warn the public about potential threats, locating the caller's location, accessibility for people with disabilities and access to 112 through online platforms.
- The **General Data Protection Regulation** (**GDPR**) Regulation (EU) 2016/679 regulates aspects regarding data protection and privacy of all citizens in the EU and the EEA. (14)
- **The Convention for the Protection of Human Rights and Fundamental Freedoms** with a special weight on article 8 that involve the right to privacy and article 14 that regulate the right to not be discriminated.

4 Identify and predict impacts

Unease - Calmness	**Suspicion - Trust**	Misuse - Protection	**New Vulnerabilities - Progress**
Technology dependency – Flexible solutions	**Function Creep – Specialized and controlled use**	Sustainability	Accountability
Transparency	Integrity	Negative – Positive Standardization	International relations
State-Citizen-Relationship	**Political Reputation**	**Social Cohesion and Solidarity**	Participation
Diversity	Open – Control Society	**Cultural and Gender Sensitivity**	Suitability, Necessity and Proportionality
In/justice & In/equality	Dignity/Autonomy	**Non-discrimination**	**Privacy & Data Protection**

[4] The website can be accessed here: http://www.prociv.pt/en-us/SITUACAOOPERACIONAL/Pages/default.aspx?cID=8.

[5] The Sendai Framework for Disaster risk reduction, available here: https://www.unisdr.org/we/coordinate/sendai-framework.

[6] Directive of the European Parliament and of the Council establishing the European Electronic Communications Code, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG.

Freedoms and Protest			

Unease – Calmness, Suspicion – Trust. Given the history of the existing crisis communication system failing at the most critical moment during a crisis situation, the population could be finding it hard to trust a new similar system. To create calmness, the new solution must foster trust in the population through showing that it is stable and functioning in similar crisis situations. If the trust is established, the system could help to create calmness in the population because the population would know that they would be able to contact the law enforcement agencies in the event of a crisis.

Political reputation, State-citizen-relationship, Social Cohesion and Solidarity. The Government faced great critique after the rural fires in 2017 and it made undoubtedly damage to their political reputation, and it is important to keep this in mind when implementing the new solution. The reputation has been further damaged as farmers and landowners feel that they have been given too much of a burden in the prevention of rural fires, and also risking heavy fines. This has also been enforced by the fact that the Government used e-mail addresses stored in the Tax Authority archive to reach out to the landowners. This meaning that the Government used the addresses for other purposes than which it was intended. With this background, the Government must take actions in a way that does not further damage the state-citizen-relationship. The solution could create positive outcomes regarding solidarity and social cohesion. The Government's plan to make the prevention of rural fires a national project where everybody participates could be enforced by the reliability of a new emergency communication system. When the system is trusted, the population would hopefully use it at an early stage in the evolvement of a potential crisis and therefore participate in the national project. The solidarity would be enforced through sharing the burden equally in protecting human life and nature from damage. A channel that would facilitate the communication channel between the population and the law enforcement agencies good enforce the relationship.

Technology dependency – Flexible Solutions, New Vulnerabilities – Progress. As history has shown, being dependent on one single crisis communication system has produced fatal and even mortal consequences. The new solution must therefore come with a plan on how to deal with a similar failure in times of crisis. The reverse 112 is an example of progress in crisis communication and management, making it possible to issue warnings at early stages during a crisis. A new vulnerability can be created through the fact that the population can go into panic after such a warning, and that it would be difficult to manage for the law enforcement agencies. This could especially be the case if the threat does not materialise. The question is if the reverse 112 would create more unease than calmness.

Privacy and data protection, Function Creep. The data collected from the caller reporting an incident to the law enforcement agencies must be stored safe and may not be used for other purposes for which it was first intended. The intention of collecting the caller's location is to easier locate the incident and to act more quick and efficient to the right area. The data collected could therefore not be used to other purposes as this could lead to a function creep.

Non-discrimination, Cultural and Gender Sensitivity. These criteria are especially relevant in the function of the reverse 112. The notifications sent out to the population with information of threats and evolving crisis must take extra measures so that all members of society are able to understand the distributed information. For example, people with different disabilities connected to hearing and sight might need information in a different format. The solution should therefore make it possible to issue information vi SMS, video, conversation, etc. The information distributed should also be given in a multiple choice of languages so that the information will reach out to all citizens in the society. The solution must also take into account that different genders, cultures and people with disabilities can have different perceptions of risk and the information distributed must be sensitive to this.

5 Mitigating measures

A crisis communication system as described in the assessment has both potential positive and negative impacts on societal aspects, but the negative outcomes might be mitigated once they are detected and through taking the right measures to minimise them.

Because the previous emergency communication system in Portugal have failed during a rural fire, it is very important that the implementation of a new system is done in a way that is transparent. To enforce the population's trust in the system the Government implementing it should provide information about its functionalities, what kind of safeguards it has, who is providing the solution, experiences from other countries (if there are any) and show how the system has been tested through different scenarios. This could for example be done through an informative website which can include both texts, interviews with professionals, videos showing the system in use, etc. A website could enhance the public engagement to the system and can also be used to increase the public participation in transforming the system to the Portuguese context and making it useful for the population.

The most important step is anyhow to make sure that the system is reliable and functioning through all different crisis scenarios. This would over time increase the public trust in the system and also strengthen the relationship between the population and the law enforcement agencies. This could in the end lead to a more sustainable and resilient community.

2.6 Assessment from functional area "Recovery"

0 General description of solution

Solution to be assessed: Crowdtasker.

Crowdtasker is a smartphone app, with the aim to give tasks to preregistered volunteers (or crowd) who are willing to help in disasters. Those volunteers usually doesn´t belong to any response organisation on a regular basis. The volunteers can be tasked with different activities such as collecting information about disaster´s impacts, or disseminating safety related information through their relatives, etc.

1 Stakeholder groups / communities

The main group of affected/benefited communities are those who are directly impacted by a disaster. Civil based organisation like sport clubs or church associations are also influenced by the use of the solution in a disaster contexts.

Another group to be considered are made up by the organisations or governments dealing with disaster management, mostly in in the affected area.

If the disaster has a considerably magnitude and the information is widely disseminated by the media to different regions or countries, then the civil population in those regions can be considered as well.

2 Background information

For assessing the impacts of the solution for the CM function "engaging the population" it is important to start defining the socio-cultural characteristics of the community and gathering information that can be used as indicators to measure the impact.

Examples of information collected are:

- Unemployment.
- Family related data-Demographics.

- Community leaders.
- Infrastructure.
- Population.
- Housing availability.
- Education.
- Risk awareness.
- Environmental.
- Access to adequate health services.
- Community culture.
- Existing groups and institutions.
- Social structure.

Table 2.2: Community Characteristics (repeated) (3)

Demography	***Culture***	***Economy***	***Infrastructure***	***Environment***
Population and age distribution	Traditions	Trade	Communication networks	Landforms
Mobility	Ethnicity	Agriculture/livestock	Transportation networks	Geology
Useful skills	Social values	Investments	Essential services	Waterways
Hazard awareness	Religion	Industries	Community assets	Climate
Vulnerable groups	Attitudes to hazards	Wealth	Government structures	Flora and fauna
Health level	Normal food types		Resource base	
Education level	Eating habits			
Sex distribution	Power structures			

3 Relevant legislation and policies

- **Sendai Framework for Disaster Risk Reduction**[7]
  The Sendai Framework for Disaster Risk Reduction 2015–2030 was adopted at the Third UN World Conference in Sendai, Japan, on March 18, 2015. The Framework ensures continuity with the work done by states and other stakeholders under the Hyogo Framework for Action (HFA) 2005–2015: Building the Resilience of Nations and Communities to Disasters.
- **Sustainable Development Goals**[8]
  The UN's Agenda 2030 for Sustainable Development was unanimously adopted by all 193-member states on the 25th September 2015. The Agenda has 17 goals and 169 targets. The SDGs are much broader in scope and more ambitious than the former Millennium Development Goals (MDGs) and cover all economic, social, and environmental aspects of the 2030 Agenda and its Sustainable

[7] The Sendai Framework for Disaster risk reduction, available here: https://www.unisdr.org/we/coordinate/sendai-framework.

[8] All the Sustainable Development Goals of the UN can be accessed through this website: https://sustainabledevelopment.un.org/topics/sustainabledevelopmentgoals.

Development Goals (SDGs).

- **The Paris Agreement**[9]
  In 2015, world leaders adopted the Paris Agreement, a legally binding, international commitment to reduce greenhouse gas emissions while also addressing rising climate risks and building resilience.
- **The New Urban Agenda (adopted at HABITAT III)** (15)
  The New Urban Agenda represents a shared vision for a better and more sustainable future. If well-planned and well-managed, urbanization can be a powerful tool for sustainable development for both developing and developed countries.
- **The New York Declaration for Refugees and Migrants** (16)
  The New York Declaration for Refugees and Migrants expresses the political will of world leaders to save lives, protect rights and share responsibility on a global scale.
- **The Compact for Young People in Humanitarian Settings**
  Given that young people represent a continuously growing cohort within the communities affected by humanitarian crises, the WHS presented an opportunity to recognise the priorities, needs and rights of youth affected by humanitarian crises are addressed.
- **Charter of fundamental rights of the European union (2016/c 202/02)**[10]
- The Charter of Fundamental Rights of the European Union (the Charter) brings together the fundamental rights of everyone living in the European Union (EU). It was introduced to bring consistency and clarity to the rights established at different times and in different ways in individual EU Member States. The Charter sets out the full range of civil, political, economic and social rights based on:
    - The fundamental rights and freedoms recognised by the European Convention on Human Rights.
    - The constitutional traditions of the EU Member States, for example, longstanding protections of rights which exist in the common law and constitutional law of the UK and other EU Member States.
    - The Council of Europe's Social Charter.
    - The Community Charter of Fundamental Social Rights of Workers.
    - Other international conventions to which the EU or its Member States are parties.

  The Charter became legally binding on EU Member States when the Treaty of Lisbon entered into force in December 2009.

- **Decision no 1313/2013/EU of the European parliament and of the council of 17 December 2013 on a Union Civil Protection Mechanism**[11]
  The overall objective of the EU Civil Protection Mechanism is to strengthen cooperation between Participating States in the field of civil protection, with a view to improving prevention, preparedness and response to disasters. Through the Mechanism, the European Commission plays a key role in coordinating the response to disasters in Europe and beyond. When the scale of an emergency overwhelms the response capabilities of a country, it can request assistance via the Mechanism. Once

[9] The Paris Agreement is available on the following URL: https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement.

[10] Retrieved from https://www.equalityhumanrights.com/en/ on 04/06/2019.

[11] A webpage describing the EU Civil Protection Mechanism can be found here: https://ec.europa.eu/echo/what/civil-protection/mechanism_en on 04/06/2019

activated, the Mechanism coordinates assistance made available by its Participating States.

- **General Data Protection Regulation (EU) 2016/679** (14)
  GDPR is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1] Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the EEA, and applies to an enterprise established in the EEA or—regardless of its location and the data subjects' citizenship—that is processing the personal information of data subjects inside the EEA.
- European Parliament, Resolution of 18/12/2008 with recommendations to the Commission on cross-border implications of the legal protection of adults, Procedure File: 2008/2123(INL).
- European Parliament, Resolution of 01/06/2017 with recommendations to the Commission on the protection of vulnerable adults, Procedure File 2015/2085(INL).

4 Identify and predict impacts

Unease - Calmness	**Suspicion - Trust**	**Misuse - Protection**	**New Vulnerabilities - Progress**
Technology dependency – Flexible solutions	Function Creep – Specialized and controlled use	Sustainability	**Accountability**
Transparency	Integrity	Negative – Positive Standardization	International relations
State-Citizen-Relationship	Political Reputation	Social Cohesion and Solidarity	**Participation**
Diversity	Open – Control Society	**Cultural and Gender Sensitivity**	Suitability, Necessity and Proportionality
In/justice & In/equality	**Dignity/Autonomy**	**Non-discrimination**	**Privacy & Data Protection**
Freedoms and Protest			

Suspicion- trust. Technologies used for engaging the population by delivering information or tasking them with activities to do, can be seen as suspicions if the technologies are not properly validated by a competent authority meaning that the expected outcome is not the desired. For instance, if there is any process for collecting information from the population, they can believe that their information will be misused or shared to third parties. Knowing where the information they share goes and what it is used for is also important to improving trust. (17) Similarly, if the source of the information is not recognized by the population, the won´t behave as supposed.

Technology dependency. Nowadays, the concept of innovation is strongly linked or associated with technology and within DRIVER+ we have seen that. Almost all participating solutions in DRIVER+ have had a strong technology component. This dependency on technology may have a negative impact over the population at times of disasters. One of the main services which are affected after a disaster is the communication and power services. The lack of those may create feelings of disorientation, fear, confusion, etc. due not being able to get accurate information on what to do or how the relatives are.

Participation. The willingness of the government to use technology as part of the citizen participation

effort may be restricted. For many of them a culture of holding meetings is very strong, and acceptance for trying out new methods, such as new technology, may face institutional resistance.

Transparency, accountability. Responding to the needs of the local population requires respectful interaction and shared responsibility for gathering information, making assessments based on that information and monitoring and evaluating the effectiveness and fairness of aid delivery. Transparency, accountability and partnership are themes that should inform all aspects of this process. Building local capacity among national staff in all sectors has become a major intermediate-time requirement of humanitarian action in the field. This strategy has developed in response to human rights norms, where mitigation of gaps in power and resources requires attention to issues of inclusion, voice and accountability. The obligations embedded in the potential of crowdsourcing also require further consideration. A current overarching uncertainty is when and whether to share information discernible to the technical and content analysts with the general public whose lives are and will be affected by this information. If good information is needed for responders to develop relevant life-saving strategies of early warning and relief, then it is, at least in some measure, of equal or greater need to the local affected population. (18)

In/justice & in/equality. Governments and aid agencies, particularly well-resourced international actors, have an operational obligation to help communities, local authorities and NGOs to generate, access and use information. This elevates information to the level of a basic need in humanitarian response. Information is not water, food or shelter, but in the list of priorities, it must come shortly after these. Community-centred approach to disaster response seeks to increase local capacity for self-organization and mutual aid, otherwise known as disaster resilience. Scaling resilience, however, requires far greater emphasis on disaster preparedness than currently exists. Correcting this drastic mismatch in policy priorities will take strong and immediate leadership.

Non-discrimination, Data protection & privacy. Access to affected populations must be based on assessed needs, not convenience or political preference; therefore, those solutions intended to gather information from the affected communities must be based on non-discrimination. Information is critical to this assessment as is professional capacity to maintain perceptions of neutrality and non-partisanship in the often extended and incessant negotiations required to sustain whatever access is initially granted.[10] Using solutions for engaging communities for getting information from the field may create a problem of big datasets. Big data do not speak for themselves; they are not objective, and proper interpretation relies heavily on ethnographic contextualization and a critical understanding of how indicators are generated. Although both legitimacy and political relevance are increasingly tied to quantitative data, long-running debates about ownership and participation remain important.

Cultural and Gender Sensitivity, Non-discrimination. Some solutions may be used to engage communities remotely or what is currently known as “digital voluntarism”. These new sorts of digital disaster response force have proven being effective in different contexts. However, these volunteers are often not identifiable beyond an internet username, yet they seem to have responsibility for processing potentially urgent requests for help and feeding this back to responders on the ground in the absence of a system of accountability. They can be relatively ignorant of humanitarian principles, codes of conduct and historical lessons. They do not understand field constraints and issues of access and security. They are not familiar with concepts of vulnerability and voice. They relish problems but resort to technological solutions without apparent respect for the friction introduced by context, culture and politics.

Cultural and Gender Sensitivity, Non-discrimination, Privacy & Data protection. Within communities at risk, access to information technology continues to follow traditional – and deeply unequal – patterns of resource distribution and vulnerability, including variations on the basis of gender. At the same time, settings in which access to technology is more widespread will tend to generate more data. In some cases, protection work or relief distribution may be based on biased or skewed data. (18) While organizations

such as the International Committee of the Red Cross (ICRC) have made enormous strides in developing protection standards for the use of information technology in protection work, many organizations still lack robust guidelines or professional standards for their own use of information technology or for collaboration with emergent/spontaneous volunteers[12]. In terms of gathering information, solutions for gathering crowdsourced data can rapidly be crippled by countermeasures, such as flooding the system with misinformation or invading the programs with malware. Information obtained through crowdsourcing can also be used to track backwards, so that individual or aggregated sources, defined by a certain geographic area settled by certain groups of interest, could be identified and potentially targeted for exposure or reprisal.

Dignity. Attention to vulnerable populations must focus on protecting their rights to life, safety, health and dignity.

New vulnerabilities- Progress. Concern over the protection of information and data is not a sufficient reason to avoid using new communications technologies in emergencies, but it must be taken into account. To adapt to increased ethical risks, humanitarian responders and partners need explicit guidelines and codes of conduct for managing new data sources. (19) The goal of human rights-based approaches was to reconstruct power relationships on an ethical and moral basis, and the goal of humanitarian reform was to improve humanitarian action through structural change. But much of the optimism currently surrounding the role of technology in the humanitarian enterprise appears to be based on two assumptions: first, that adding technology is inevitable; and second, that doing so will generate progress.

5 Mitigating measures

Since engaging the population on the recovery phase brings several challenges, emergency organisations should identify those constraints beforehand and being prepared for them if arise.

For instance, not only the social factors should be included, but the cultural, political and technological as well. Down below there is a list of possible mitigation actions that address some of the challenges identified in the previous step.

Social Level

- Include community leaders during any planning or needs assessment the population will find represented and heard.
- Evaluate the dynamics of the affected population. (e.g. how they interact one each other, important institutions, existing civil groups, etc…).

Technological Level

- Messages or surveys sent out by the government or humanitarian organizations will have to be transmitted in a way that somehow verifies the authenticity of the sender.
- Ensure the protection of users data (e.g. encryption of files- controlled access to the data).
- When working with digital volunteers, it must be assured their location is protected and they won't be

[12] Emergent volunteers are usually understood as members of a community who are not regular volunteers of an emergency response organisation. They act by their own motivation and usually are out of a command chain.

tracked down if they use any sort of smartphone app. If it is required by solutions the tracking of their location, digital volunteers must be informed beforehand under which conditions and why their tracking is needed.
- To avoid misinterpretation of information, texts needs to be clear and written in a language and dialect that is understandable to the user.
- To avoid feelings of disorientation, fear, confusion and the dependence of connectivity, governments should ensure back-up communication systems in case of network failure, so that the population can be informed of what to do in case of emergency.

Political Level

- Technological innovation for disaster management is equally important as policy innovation. To permit the use of solutions in disaster context, policies should be developed in order to allow the use of technology while protecting population rights.
- Governments should raise awareness about the official means of communication during emergencies.

Organisational Level

- For improving trust, organisations should inform the population what they are doing with their data and why specific data is collected.
- Organisations working with spontaneous volunteers should develop robust guidelines or professional standards for their own use of information technology or for collaboration with emergent/spontaneous volunteers.
- to adapt to increased ethical risks, humanitarian responders and stakeholders need explicit guidelines and codes of conduct for managing new data sources.

2.7 Assessment from functional area "Crisis communication and Information Management"

0 General description of solution
Solution to be assessed: A multi-channel mass notification system. This multi-channel mass notification system is implemented to help organizations reach all of its employees, customers etc. in case of a crisis, and the solution is used as part of the organization's overall crisis communication plans. The solution, which is software-based, can be tailored to work through different channels, such as SMS text message, E-mail, and social media posts. The texts that are being sent out can be pre-written for different scenarios. Naturally occurring hazards, such as a hurricane or severe thunderstorm, and human-caused hazards, like a fire or civil disturbance are examples of scenarios that could be prepared. Having a multi-channel mass notification system can be useful for protecting life and ensure safety, security and business continuity as well as minimize the negative impacts of these events. The solution complements and feeds into the overall operational emergency preparedness plan of the

organization adopting the solution. The solution, which is assessed in the following, is implemented in Norway in 2019, by The Norwegian Directorate for Civil Protection (DSB).[13]

1 Stakeholder groups / communities

There are several groups and stakeholders that might be affected by a mass notification system solution, but the main group of affected communities are those who are direly impacted by the actual crisis, and who will receive the notification. In addition, the "owners" of the solution, i.e. the Directorate or the responsible individuals in the Directorate deciding to 1) design the messages being sent out, and 2) activate the mass notification system are considered stakeholders in this case. A final group of stakeholders might be the solution developers, i.e. the people working on improving and revising the technical aspects of the mass notification system.

2 Background information

In Norway, the level of trust in state institutions such as the police is very high, also compared to other Scandinavian countries (20). Based on the knowledge that trust is a core element in the way individuals experience safety, (21) this can be a relevant fact in the implementation of this solution insofar the solution requires some sort of direct public participation.[14] Another relevant fact is that most people in Norway have smart phones, and that the expansion of the mobile 4G network in Norway has resulted in good cell reception nationally. In a global survey on digital media use in 2018, Reuters Institute for the Study of Journalisms Digital News Report, approximately 40% of Norwegians report that they fear "fake news", and that it is difficult to distinguish between fake news and facts online[15]. News about false crisis alerts have also been covered in the Norwegian mainstream media, such as the false Hawaiian missile alert in January 2018 and the false alarm issued by Japan over North Korean missiles, just a few days after. However, the Norwegian public does not receive many messages from the authorities and is seemingly inclined to take such messages seriously. There is an increase in Norway's emergency preparedness, and the public are increasingly included in this work. A brochure called "Advise on emergency preparedness" was distributed to all households in Norway, December 2019. In case of big emergencies, e.g. caused by terror attacks or cyber-attacks which strike critical infrastructure, this brochure gives practical advice to the public on how to prepare for such events. The brochure was discussed in the media.

3 Relevant legislation and policies

Since the solution includes some personal data for it to be able to send out information and notifications, the most relevant legislation is GDPR, which was introduced in May 2018 to harmonize data privacy laws across Europe.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Official Journal of the European Communities (2000), *Charter of Fundamental Rights of the*

[13] While the Directorate recommended the implementation of a SMS- notification system in a report in 2017, they have not implemented the solution at stake in this assessment. In that sense, the assessment in fictional, but it also demonstrates how a solution can be assessed before implementation. More information about the report from DSB can be found here: https://www.rbnett.no/ntb/innenriks/2017/12/01/DSB-anbefaler-SMS-varsel-til-alle-ved-terror-og-krise-15691433.ece.

[14] Metropolitan Police, *Serious Crime Gallery*, Available at: http://content.met.police.uk/Gallery/Serious-Crimes-gallery/1400032830436/1400032830436.

[15] The global report can be accessed here: http://www.digitalnewsreport.org/.

European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

4 Identify and predict impacts			
Unease - Calmness	**Suspicion - Trust**	Misuse - Protection	**New Vulnerabilities - Progress**
Technology dependency – Flexible solutions	**Function Creep – Specialized and controlled use**	Sustainability	Accountability
Transparency	Integrity	Negative – Positive Standardization	International relations
State-Citizen-Relationship	**Political Reputation**	Social Cohesion and Solidarity	Participation
Diversity	Open – Control Society	Cultural and Gender Sensitivity	Suitability, Necessity and Proportionality
In/justice & In/equality	Dignity/Autonomy	**Non-discrimination**	**Privacy & Data Protection**
Freedoms and Protest			

Unease/ calmness. By using a mass notification system, the population can be reassured in the event of a crisis. They can receive information about what to do or where to go, and they can be given other kinds of useful information. However, depending on the content of the messages sent out, they can also feel unease. This is not only because the solution is eventually only activated during a crisis and that in itself creates unease, but it might also be that the information received is incomprehensible or incomplete.

Suspicion/ trust. Knowing that you will receive a notification in case crisis occurs can create a trustful relationship between the Directorate and the population. Trust is relevant here in at least two ways: 1) For the Directorate, because their integrity and the way people use the information received relies on the public trusting the Directorate, and 2) for the public, since they are likely not to act upon the information received if they do not trust the Directorate. However, if a crisis of some kind occurs and the population is not notified (either due to error or an active decision) and there is an expectation that they would be, this can also fuel suspicion.

New vulnerabilities – progress/ Technology dependency – Flexible solutions. Using a mass notification system solution might create new vulnerabilities. This is because the user of the solution might become dependent upon the solution, without having a similarly efficient backup solution in place in case of error. In this case, technology dependency might be creating a new vulnerability. For the mass notification system solution, the risk of this happening can be said to be reduced by the fact that several channels are available for the notifications to go through. Although all of them (SMS text message, E-mail message and Social media posts) are all dependent on technology in the sense that they are electronic, in case of the particular technologies fail (due to e.g. fallout of Wi-Fi), other channels can be used and thus the solution is fairly flexible.

Function creep – specialized and controlled use/ Political reputation. All solutions that collect personal data can be misused in some way. The gradual widening of the use of the mass notification system solution

might be defined as function creep when and if it is used also for other purposes. This might erode the trust that the population has in the solution (and even in the Directorate using it), and the risk might be that the advice or recommendations included in the notifications might not be taken as seriously. It might also influence the Political reputation of the Directorate negatively.

Dignity/ Non-discrimination. Dignity is closely related to Article 21 of the European Charter of Fundamental Rights, the right to non-discrimination, which forbids any discrimination "based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation" (22) If the mass notification system solution would be operating on its own and not as an integrated part of an overall emergency preparedness plan, the risk of the solution being discriminating would be real. This could be the case because the solution assumes and is built on the fact that most people own a smart phone, and/ or has access to the internet. This is not always the case (e.g. homeless people, low-income families, etc.), and for those national minorities, informing about and providing emergency help or advise to the people with access to smart phones first can be seen as a discriminatory practice.

Privacy & data protection. The mass notification system solution collects some types of personal data and is based on people registering their phone number, E-mail address etc. with the solution provider (the Directorate) as part of a preparedness step and for being available for the solution. This means that personal data is collected and processed by the solution. It is important that the solution is developed and implemented in such a way that does not go against data protection regulations or threaten people's privacy. It might also be that people wish to withdraw their consent for receiving messages (for various reasons), and if not allowing this, the solution might negatively impact privacy. Or if the personal data is used for different purposes, this would also be a violation of data protection and privacy rights.

5 Mitigating measures

When implementing the mass notification system solution, it is important that the information that is shared with the public is complete and understandable. It should be made clear what the information is about, if there is a timeframe relevant for the information, what the population should do with the information, and so on. The language should be very clear and free from potential misunderstandings, and the owner of the solution, in this case the Directorate, should consider also using several languages. When it comes to trust, the solution seems to have a positive influence, if implemented right. However, it should be made clear to the users of the solution (the population) what the criteria for sending out a notification will be, so that they don't become anxious or suspicions if some crisis occurs and no information is given via the solution. Expectation management seems to be important. Also, if the solution is functioning via social media channels (i.e. posting messages on Facebook automatically when sending out SMS notifications), the Directorate should consider moderating the media forum to avoid false rumours which could create suspicion. The solution owner should also communicate to the users of the solution about potential risks of using the solution, and maybe also encourage the solution users (the population) to subscribe to all the different channels, so to minimize the risk of one of the channels not functioning. Also, E-mails are more flexible in terms of length than for example SMS text messages. On the other hand, emails might have a lower readership rate. To avoid function creep, the solution should only be used for the pre-defined purpose. For the Directorate it seems important to ensure that the mass notification system solution is not the only solution used to inform the public about or in times of crisis, but that other (non-technological) solutions exist in parallel. This is also important to include the full population, including also those who may have a vision impairment and cannot read a text message or email. This could be for example the organization of door-to-door actions or to spread a message by using car mounted speakers. The GDPR should be carefully considered to make sure that the personal data that the

solution is based upon stays protected, and the Directorate should ensure that it is possible to opt-out from the solution.

2.8 Assessment from functional area "Command, Control and Coordination (C3)"

0 General description of solution

Solution to be assessed: BE-alert.

In 2014, the Belgian Crisis Centre launched the BE-Alert Pilot project and enabled for 2 years, 33 municipalities to test, evaluate and suggest improvements to the tool. The idea is to develop a powerful tool to offer to the authorities of Belgium, promoting the security of citizens. BE-Alert is a constantly evolving tool that relies on different technologies that can alert the public wherever it is.

BE-Alert is a functional alert system which allows for faster and clearer diffusion of information. All people affected by the crisis could sign up to this application for free and therefore have access to all alerts regarding crises. The BE-Alert system allows an alert through new complementary channels: by call, text messages, emails. The system has enough capacity to simultaneously alert a large number of citizens, through several channels.

1 Stakeholder groups / communities

The main Stakeholder group / Communities affected are the population (citizens) directly impacted by the crisis.

The first responders will also be influenced by the use of the solution in a crisis context:

- Rescuers.
- Police officers.
- Paramedics.
- Emergency medical technicians.
- Firefighters.
- Other trained members of different organisations.

2 Background information

To assess the impacts of the solution for the CM function "Exploit the C3 System", subfunction "Deliver public information and advice", it is crucial to collect reference information covering key social issues of the citizens and first responders. Some of the specific questions below can be asked:

- Were the targeted citizens already impacted by such a disaster? How can they react?
- Are the citizens familiar with technologies such as social media, phones, mails, mobiles? Which language do they speak (i.e. are they able to understand what is shared by BE-Alert)? Do they trust the tool to receive information?
- Are the first responders familiar with such technologies to intervene in a disaster? Do they trust the tool to receive and disseminate information about the crisis?

3 Relevant legislation and policies

- **Sendai Framework for Disaster Risk Reduction**[16]
  The Sendai Framework for Disaster Risk Reduction 2015–2030 was adopted at the Third UN World Conference in Sendai, Japan, on March 18, 2015. The Framework ensures continuity with the work done by states and other stakeholders under the Hyogo Framework for Action (HFA) 2005–2015: Building the Resilience of Nations and Communities to Disasters.
- **General Data Protection Regulation – GDPR** (14)
  The GDPR is a regulation in EU law on data protection and privacy for all citizens of the European Union and the European Economic Area. It aims to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU
- **Charter of fundamental rights of the European Union (2016/c 202/02)** (22)
  The Charter of Fundamental Rights of the European Union (the Charter) brings together the fundamental rights of everyone living in the European Union (EU). It was introduced to bring consistency and clarity to the rights established at different times and in different ways in individual EU Member States. The Charter sets out the full range of civil, political, economic and social rights based on:
  - The fundamental rights and freedoms recognised by the European Convention on Human Rights.
  - The constitutional traditions of the EU Member States, for example, longstanding protections of rights which exist in the common law and constitutional law of the UK and other EU Member States.
  - The Council of Europe's Social Charter.
  - The Community Charter of Fundamental Social Rights of Workers.
  - Other international conventions to which the EU or its Member States are parties.

4 Identify and predict impacts

Unease - Calmness	Suspicion - Trust	Misuse - Protection	**New Vulnerabilities - Progress**
Technology dependency – Flexible solutions	Function Creep – Specialized and controlled use	Sustainability	**Accountability**
Transparency	**Integrity**	Negative – Positive Standardization	International relations
State-Citizen-Relationship	**Political Reputation**	**Social Cohesion and Solidarity**	Participation
Diversity	**Open – Control Society**	Cultural and Gender Sensitivity	**Suitability, Necessity and Proportionality**
In/justice & In/equality	**Dignity/Autonomy**	Non-discrimination	**Privacy & Data Protection**
Freedoms and Protest			

[16] The Sendai Framework for Disaster Risk Reduction can be accessed here: https://www.unisdr.org/we/inform/publications/43291

Unease – Calmness. The information shared with the public during a crisis can be easily done in a way that creates more unease than calmness. Over-communicating with detailed information can create panic and overload first responders and citizens with a high number of alarming messages.

New vulnerabilities – Progress. The introduction of a new Crisis Management tool can create new vulnerabilities. In case of man-made attacks, informing the public will also inform the attacker as well.

Accountability. During CM situations, many different actors implement a variety of measures. If the accountability for taking and conducting these measures is not clearly set out potential negative side-effects may appear. The authority sending the messages to the public (citizens and first responders) needs to be the one having the responsibility to do it and the hierarchy of decision makers should be clearly established.

Transparency. A lack of clarity and the non-accessibility of the messages shared with the public can lead to a misunderstanding and have a direct impact on the societal acceptance of the measures taken.

Integrity. The messages communicated to the public needs to respect a high level of integrity, i.e. respecting ethical codes and right. The actions taken through the messages shared can then be truthful, accurate and consistent.

State-Citizen-Relationship. The legitimacy of the state results from the public accept the rules regulating the exercise of power and binding. The message expressed by the government to the public needs to be accepted by the citizens and first responders to have an impact on the crisis. Citizens can easily feel alone and first responders exploited.

Political Reputation. Directly linked to the social opinion, a bad political reputation is often accompanied with a low acceptance of the measures proposed by a government. If not accepted by the public the implementation of these measures won't have the intended effects. The reputation of the political entity disseminating the message will influence the message itself.
Social cohesion & Solidarity. The fundamental principle of solidarity of the EU is based on sharing both the advantages and the burdens equally and justly among all group members. The way of disseminating the messages to the public can have direct discriminatory impact on the social cohesion. The citizens do not all have the same access to the technologies used to share the messages. The differences can be seen as discriminatory for a part of the population.

Diversity. The communication towards the public needs to take into account the diversity of the crisis population to avoid cultural, linguistic, racial or gender discrimination of the general population.

Open-Control Society. The manner of informing the public is a characteristic of an open or control society. To be considered as open, the authority must be tolerant and disseminate a transparent and flexible message. The advices given to the public in time of crisis can be seen as achieving security through control.

Suitability, Necessity & Proportionality. The information shared with the public absolutely needs to be proportional to the intensity of the crisis. If the messages are not proportional, they will have some secondary effects such as citizens and first responders acting in disproportionate way and the loss of trust in the authority disseminating the message.

Dignity / Autonomy. Disseminating information and advices to the public during a crisis may lead to the loss of citizens' autonomy if the messages shared give strict order to follow under pressure.

Privacy and Data Protection. If one has to subscribe to a system asking for personal data and allowing tracking to receive alerts, this might concern over privacy and who the data is shared with.

5 Mitigating measures
Since informing the public brings several challenges, authorities should clearly identify these constraints and take all possible measures to avoid the risks described above. The message disseminated should be clear, transparent, proportional and adapted to the crisis situation and the entire population receiving the messages, preserving its autonomy and taking its diversity into consideration. It must be sent by a trustful authority recognized and respected by the population, avoiding any kind of discrimination.

2.9 Assessment from functional area "Logistics"

0 General description of solution
Solution to be assessed: Cold chain centre for medicines and vaccines. Medical logistics is important during both emergency planning and response efforts. The solution to be assessed is a cold supply chain management tool, and more specifically a cold chain centre in Norway. The centre is a storage point for temperature-sensitive medicines and vaccines. The main function of the solution is to ensure that Norway has a sufficient stock of medicines and vaccines that are needed in a crisis situation, to store the products under a strictly controlled temperate environment and to ensure proper transport of these medicines to crisis-affected areas within the Norwegian borders. The centre is of great importance in CM because if medicines and vaccines are stored at wrong temperature it can affect its quality, safety and efficacy. This can lead to problems with stopping infectious diseases from spreading in a crisis affected population.
1 Stakeholder groups / communities
• The crisis affected community. • Hospitals, medical personnel, local doctor's offices and general practitioners. • Law enforcement agencies and emergency services. • Volunteer organisations. • The Norwegian Directorate of Health. • The Norwegian Institute of Public Health. • The Pandemic and Epidemic Committee. • Medical manufacturers and wholesalers. • Transportation and logistics companies.
2 Background information
Medicine shortages are a growing international problem, but Norway is especially vulnerable due to the lack of local production of medicines (23). In a survey performed by the European Association of Hospital Pharmacists, all of the Norwegian respondents answered that medicine shortages in hospitals were experienced weekly (24). The same report shows that Norway has been without a specific antibiotic for a year because the factory in China that produces it exploded and burned down. The financial crisis also left European countries, like Greece, in acute medicine shortage because the country was not able to pay the bills to the medicine manufacturers (25).

Known vulnerabilities in the Norwegian community are tied to extreme weather such as storms and flooding, but also landslides and the outbreak of epidemics[17]. The consequences of extreme weather and landslides can do great harm to critical infrastructure and make the transportation of medicines and vaccines to the affected community difficult. Landslides in residential areas might lead a large group of people without homes and refugee camps might be established. Immediate vaccination programmes are often recommended when a refugee camp is established, because outbreaks of disease are likely and will spread quickly in this context.

Vaccines and attitudes towards vaccines. The Norwegian population is generally positive towards vaccines and 96 % of all 2 year-olds follows the national Childhood Immunisation Programme (26). On the other side, there have been some controversies in relation to the swine influenza pandemic in 2009/2010 and side effects of the vaccine offered at the time. About 1,6 million persons under the age of 30 chose to be vaccinated against the virus, and studies has later shown a strong association between vaccination and narcolepsy (27). The study further showed that vaccinated individuals had about five times higher risk for developing narcolepsy than unvaccinated individuals. This background history related to the vaccination during a pandemic might affect the people's attitudes towards vaccines in the future.

3 Relevant legislation and policies

- **The Norwegian Act of 12 April 1992, No 24 Relating to Medicines and etc.** sets out an established standard of quality for pharmaceuticals and regulates sale, purchase, manufacture and import of pharmaceuticals in Norway.
- **The EU regulatory system for medicines** (28) is a network of 31 EEA countries, the European Commission and the European Medicines Agency (EMA). The goal of this network is to authorise and monitor medicines in the EU and ensure that patients have access to high-quality, effective and safe medicines. The EMA also overviews and controls the situation of medicine shortages in the EU.
- **Regulation (EU) No 1027/2012** (29) aims to reduce the number of adverse drug reactions in the EU through collecting better data on medicines and their safety, rapid and robust assessments of issues related to the safety of medicines and effective regulatory action to deliver safe and effective use of medicines.
- **European Union Falsified Medicines Directive (DIRECTIVE 2011/62/EU)** (30) sets out EU-wide rules for importation of medicines and other active substances, it places an obligation on EU countries to take appropriate measures to ensure that manufacturers of active substances on their territory comply with good manufacturing practices and to overall prevent fake medicinal products to enter the European market.
- **Guideline (2013/C 343/01) on Good Distribution Practice for medicinal products for human use** (31) sets out guidelines for how premises should be designed or adapted in order to ensure that the required storage conditions are maintained. The premises should be suitably secure[18], structurally sound and sufficient capacity to allow safe storage and handling of medicinal products. In addition, suitable equipment and procedures should be in place to check the environment where medicinal products are stored including temperature, light and humidity.
- **National influenza pandemic preparedness plans** (32) is implemented in order to manage the

[17] Reports documenting known vulnerabilities are published every year. See: Norwegian Directorate for Civil Protection (2015) *National Risk Analysis 2014*. Available from: http://www.dsbinfo.no/DSBno/2015/Andre/NationalRiskAnalysis2014/?page=1 [Accessed: 19.06.2019].

[18] The Norwegian Medicines Agency also provides guidelines on how to protect premises that store medicinal products from burglary: https://www.fgsikring.no/siteassets/regler/innbrudd/b-krav-og-registre/b-krav-gjeldende/b-krav-fg-112_7---ny-mal.pdf

challenges that a pandemic can pose to the society and the health sector. When a pandemic hits a society, it is not likely that a vaccine will be fully developed and available, and medicines against influenza will be the only way to curb the impact of the disease as well as infection protection measures that can stop the influenza from spreading. Most EU and EFTA countries have developed such national plans according to guidelines from the World Health Organization (33).

- **Charter of Fundamental Rights of the European Union 2016/c 202/02.** (22) Article 35 of the Charter sets out the right to health care: "Everyone has the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices".
- **International Covenant on Economic, Social and Cultural Rights** (34)**.** The Covenant is fully adapted in Norwegian legislation and article 35 recognises that everyone has the right to the enjoyment of the highest attainable standard of physical and mental health. To achieve the full realisation of the Covenant the states must amongst others prevent, treat and control epidemic, endemic, occupational and other diseases.

4 Identify and predict impacts

Unease - Calmness	**Suspicion - Trust**	Misuse - Protection	**New Vulnerabilities - Progress**
Technology dependency – Flexible solutions	Function Creep – Specialized and controlled use	Sustainability	Accountability
Transparency	Integrity	Negative – Positive Standardization	International relations
State-Citizen-Relationship	**Political Reputation**	Social Cohesion and Solidarity	Participation
Diversity	Open – Control Society	**Cultural and Gender Sensitivity**	Suitability, Necessity and Proportionality
In/justice & In/equality	**Dignity/Autonomy**	Non-discrimination	Privacy & Data Protection
Freedoms and Protest			

Suspicion – Trust, Political Reputation and Transparency. In Norway, the official authorities and politicians have a high level of trust and the state is therefore seen to be reliable and trustworthy and acting in a good and honest way. In fact, Norway is on the top of trust in government and politicians in Europe according to the European Social Survey (35). As already noted, the national Childhood Immunisation Programme is highly supported and might indicate that the population trust the quality of the vaccines offered by The Norwegian Institute of Public Health. In order to develop and implement a cold chain centre that would store medicines and vaccines for crisis situations this trust is essential to the extent that people in crisis affected areas would accept to take the medicines and vaccines in order to prevent infectious diseases from spreading. If this trust is lacking, the centre might lose its legitimacy.

For the centre to be a legitimate and successful step in Norwegian CM and planning for medical logistics, it is dependent upon trust in the official authority. Although there is a high level of trust and the political reputation is seen to be good in most cases in Norway, this can have been affected by the 2009 Swine Influenza vaccination issue where a good proportion of the vaccinated individuals where diagnosed with narcolepsy. This incident can make the population suspicious and more resistant to influenza vaccines in future epidemics or pandemics if the vaccine provided is not properly tested in advance. This incident can have led to unease regarding that type of vaccines in the population and might damage the legitimacy of

the cold chain centre. An analysis of the crisis communication from the official bodies controlling the situation has shown that the authorities were keen to stop media and debate posts that questioned the safety of the vaccine and the mass vaccination strategy, and that there was issued to little official information regarding the uncertainty associated with the vaccine and its limited trial period (36).

New Vulnerabilities – Progress, Technology Dependency – Flexible Solutions. The cold chain centre would represent a progress in the Norwegian context of CM as it would involve an improvement of the planning of medical logistics. With the centre storing an amount of necessary medications and vaccines in case of a crisis situation would mean that there is an improvement in the protection of potential crisis affected communities and would make it easier to respond quick and effectively to crisis situations. There is however a limit to the storage capacity of the centre, and it would not necessarily be possible to store enough medication and vaccines to cover all inhabitants in the country if that would be the case. Relying too heavily on the centre covering enough medicines could therefore create new vulnerabilities. The background information revealed how Norway being dependant on one type of antibiotics has left the country without the medicine for a year because the factory producing it burned down. With the implementation of the centre, scenarios like this should be taken into consideration to minimise negative impacts.

This could create a technology dependency in the crisis situation. The centre is undoubtedly fragile during an electricity breakdown, and could lead to medicines and vaccines being destroyed if there is not an emergency plan at place. To centralise all medications and vaccines in one place instead of spreading it around the country can further worsen the impact of this scenario. The centre is also reliable on a transportation company that have the ability to deliver medical supply in areas affected by a crisis and maybe where the infrastructure has broken down. It is therefore very important to create a flexible solution that can be altered to the situational needs. Flexibility is in itself very difficult especially regarding epidemic and pandemics because it often takes time before there are vaccines in place and to get it tested and approved for European markets. There should also be good routines in place to prevent diseases from spreading, because when the medicine storages are empty it might be empty for a long time, and prevention therefore becomes most important.

Dignity/Autonomy and Cultural & Gender Sensitivity. Last, but not least, even if the cold chain centre exists it does not necessarily mean that the population might want to use the medicines and vaccines that are stored there. Everyone has the right to refrain from health care although it is encouraged. The right to refrain from medical care must be respected, but it is at the same time a right to have access to health care. To be respectful of the individual's choice would strengthen his/her dignity and autonomy. It is also necessary to show gender and cultural sensitivity. Some religious groups would for example resist the use of some medications. Further, a pregnant woman might not like to take a vaccine if she is afraid of it damaging the foster.

5 Mitigating measures

In order to foster trust, it might be an idea to communicate openly and transparently about how the centre functions to store medicines and vaccines needed for crisis situations in a manner that secure its quality, efficacy and safety. Providing solid and informative descriptions about the medicines and vaccines stored there, could lead the population to trust that the Government is capable of providing medicines and vaccines of good quality in times where it is needed. It can also make the population more aware of the importance of storing medicines to prepare for a crisis, and also to have a storage of medicines at home that could be important when a crisis strike. The establishment of the centre is therefore an opportunity for the official authorities to raise awareness around crisis preparedness amongst the population. The successful HBO-series "Chernobyl" has for example put a focus on nuclear accidents and this has led to a doubling in the number of sales of iodine tablets in Norway.

Establishing the cold chain centre would also force the Government to take the appropriate measures to

combat medicine shortages and to realise the importance of having a strong network of medicine suppliers in times of crisis. The establishment of the centre would therefore in itself be a measure to foster positive outcomes for the Norwegian society.

2.10 Assessment from functional area "Security Management"

0 General description of solution

Solution to be assessed: Cyber-Security Enhancement System.

This solution aims at reinforcing the cyber resilience of CM systems and to mitigate its vulnerabilities to external attacks.

Regarding the SIA Functional Area, this solution deals with Security Management (a common CM function), more specifically the function Conduct security orientation and planning. The function includes solutions that develop security component in CM plans and systems, establish programmes for acquisition of security capabilities, establish preliminary coordination, develop preparedness security guidance, provide performance guidelines, and introduce security specific norms.

1 Stakeholder groups / communities

This solution requires interventions from two main groups of people. Firstly, the main stakeholders are the technology developers that build the software. Secondly, the main end-users are law enforcement agencies, first responders, and other CM practitioners, i.e., the broader CM community.

2 Background information

Cyber security has emerged as key component of CM. Cyber-attacks on critical infrastructure are seen as having a high potential for damage, as a growing number of systems and services are linked through large software structures.

Protecting the CM infrastructure from cyber-attacks and reinforcing its resilience is of key importance to ensure an efficient and timely response from the CM community. Failures in the online communication system, for example, can impact the functional management of a crisis, irrespective of the nature and origin of the latter.

3 Relevant legislation and policies

Cyber-security software needs to observe specific national legislation on the cyber domain, as well as potential international legislation. These systems also need to attend to privacy and data protection provisions. In the case of the EU, these include national provisions, as well as the GDPR.

4 Identify and predict impacts

Unease - Calmness	Suspicion - Trust	**Misuse - Protection**	New Vulnerabilities - Progress
Technology dependency – Flexible solutions	**Function Creep – Specialized and controlled use**	Sustainability	Accountability
Transparency	Integrity	Negative – Positive Standardization	**International relations**
State-Citizen-Relationship	Political Reputation	Social Cohesion and Solidarity	Participation

Diversity	**Open – Control Society**	Cultural and Gender Sensitivity	**Suitability, Necessity and Proportionality**
In/justice & In/equality	Dignity/Autonomy	Non-discrimination	**Privacy & Data Protection**
Freedoms and Protest			

Because the cyber and the material domains are increasingly difficult to disentangle, measures impacting the cyber domain need to be understood as having the potential to impact the society at large. Therefore, evaluating the potential impact of cyber-security measures need to consider impacts on the society at large.

Function creep, Misuse/ Protection, Transparency, Suitability/ Necessity & Proportionality. Cyber-security systems may end up in logics of function creep. Precisely because vast parts of social and material life are connected through communication systems, any measure aiming at protecting them will be in contact with data that refers to several domains. The protection of these systems may lead to misuse of the data collected, to control over societies, and to mission creep, i.e., to the use of the solution for a different purpose that the one it was created for. For this reason, cyber-security measures may pose challenges around transparency over the specific data collected, as well as debates about suitability, necessity and proportionality.

Privacy & Data protection. Cyber-security measures can also trigger questions about privacy and data protection, given that they interact with private data of all the citizens that need to be protected.

Open- Control society, State- citizen relationship. Ambitious and comprehensive cyber-security systems can impact the state / citizen relationship and challenge the openness of the society while affecting international relations as well.

5 Mitigating measures

Cyber-security systems need to be designed in a way that does not challenge the equation between privacy and security. The full observance of data protection legislation is a mandatory requirement and should be a main concern of the system designers. Specific measures about the possible collection and storage of data need to be in place and should observe national and international legislation.

In order to pre-emptively face potential societal impacts, the design of the cyber-security solution should be monitored by a national ethics committee, so that the highest standards of research ethics can be observed.

The risk of control over the society needs to be mitigated with measures that address transparency about the functioning of the system and the role of both public actors in the implementation of that solution. Building cyber resilience is crucial but it cannot come at the expense of other societal norms and values. The principles of necessity and proportionality should frame the contours of the system, and logics of mission creep need to be avoided. It is important to make sure that relevant public monitoring schemes involving state agencies and commissions are involved in the monitoring of the functioning of the system.

3. Conclusion and way forward

The ten societal impact assessments that are collected in this deliverable illustrate the broad applicability of the SIA framework to a variety of solutions addressing various CM functions. The assessments will be available as supporting documents to the SIA Framework which has been submitted as **D913.31** ***Societal Impact Assessment Framework- version 2***. The SIA Framework is currently being integrated into the TGM Handbook, which will be delivered in M66. Here, the ten assessments can be included as supporting documents (a sort of reference implementation) for the SIA Framework. Exactly how this implementation will be done is still work in progress at the time of delivery of this deliverable (M63). In addition, a CEN Workshop Agreement (CWA) will be developed for the DRIVER+ SIA Framework. This process is explained in detail in section 5.2 of **D913.31** ***Societal Impact Assessment Framework- version 2***. This will be collaboration between DIN, PRIO, PSCE and the University of Lancaster, and it will be kicked off in September 2019. An initial teleconference with all four members was organized on 16/07/2019, and the formal kick-off meeting is planned for September 2019. An ultimate goal for this process is that our CWA is within the interest of the CEN Technical body - CEN/TC391 - Societal and Citizen Security, and that they may take it forward to consider for full normative standardisation later. The ten assessments delivered in the current deliverable will serve as input to the standardisation process. Furthermore, the ten assessments will feed into the development of **D913.52** ***Training modules for Societal Impact*** (M66), where they can be used as examples of SIA. The SIA training module will be part of the overall Training Module of the TGM.

References

1. **DRIVER+ project.** *D913.31- Societal Impact Assessment framework- version 2.* 2019.

2. *Taxonomy of CM functions for classification of solutions.* **DRIVER+ project.** 2017.

3. *Community Emergency Preparedness: A Manual for Managers and Policy-Makers.* **WHO.** 1999.

4. **Hao, Karen.** Technology Review. *Police across the US are training crime-predicting AIs on falsified data.* [Online] February 13, 2019. [Cited: July 16, 2019.] https://www.technologyreview.com/s/612957/predictive-policing-algorithms-ai-crime-dirty-data/ .

5. *Predictive Policing: Review of benefits and Drawbacks.* **Wessels, Albert Meijer & Martijn.** 2019, International Journal of Public Administration .

6. *Analysing the Role of Privacy Impact Assessments in Technological Development for Crisis Management.* **Easton, C.** 2017, Journal of Contingencies and Crisis Management.

7. **Deasy, Dave.** Corporate Complience Insights. *PIAs and GDOR DPIAs- A best practice guide.* [Online] 2017. https://www.corporatecomplianceinsights.com/pias-gdpr-dpias-best-practice-guide/ .

8. **European Emergency Number Association EENA 112.** *Emergency calls in the upcoming EU-legislation.* Brussels : European Emergency Number Association, 2018.

9. **Centre for Climate Adaption.** Climate Change Post. *Forest Fires for Portugal.* [Online] 2019. [Cited: June 23, 2019.] https://www.climatechangepost.com/portugal/forest-fires/.

10. **The Portugal News.** Experts warn this week's quake was a "wake-up call". [Online] Januar 18, 2018. [Cited: June 23, 2019.] https://www.theportugalnews.com/news/experts-warn-this-weeks-quake-was-a-wake-up-call/44487.

11. **BBC News.** BBC News. *Portugal's Siresp rescue network "failed forest fire victims".* [Online] June 27, 2017. [Cited: March 03, 2019.] https://www.bbc.com/news/world-europe-40415815?fbclid=IwAR32adHRL8OCyQEBrkXlhFeCq4lObQYpH6LKU4bEMFeEcbrYgU54SHe2sGk.

12. **Review, The Critical Communications.** The Critical Communications Review. *Portugese Government Demands Pressure from SIREPS on Portugal Telecom.* [Online] August 21, 2017. [Cited: July 17, 2019.] https://www.criticalcommunicationsreview.com/ccr/news/34650/portuguese-government-demands-pressure-from-siresp-on-portugal-telecom.

13. **Ames, Paul.** Politico. *Portugal scrambles to prevent forest fires.* [Online] March 29, 2018. [Cited: July 16, 2019.] https://www.politico.eu/article/portugal-scrambles-to-prevent-more-forest-fires-cleanup-eucalyptus-trees-antonio-costa/.

14. **EU.** General Data Protection Regulation GDPR. [Online] Intersoft consulting, 2018.

15. **United Nations.** Habitat III. *New Urban Agenda* . [Online] 2017. [Cited: July 15, 2019.] http://habitat3.org/wp-content/uploads/NUA-English.pdf.

16. —. Refugees and Migrants. *New York Declaration for Refugees and Migrants.* [Online] October 3, 2016. [Cited: July 16, 2019.] https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/1.

17. **Pètursdòttir, Sonja Dögg Dawson.** *Technology Enabled Citizen Participation.* Reykjavik : Reykjavik University, 2011.

18. **International Federation of Red Cross and Red crescent societies.** IFRC. *World Disasters report- Focus on technology and the future of humanitarian action.* [Online] 2013. https://www.ifrc.org/PageFiles/134658/WDR%202013%20complete.pdf.

19. **OCHA.** OCHA Policy and Studies Series. *Humanitarianism in the network age- Including world humanitarian data and trends 2012.* [Online] 2013. [Cited: July 15, 2019.] https://www.unocha.org/sites/unocha/files/HINA_0.pdf.

20. Politiet. *Politiets omverdensanalyse 2012.* [Online] 2012. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/omverdensanalyse/politiets-omverdensanalyse-2012.pdf.

21. **Slovic, Paul Ed.** *The perceptions of risk.* s.l. : Earthscan publications, 2000.

22. **Nations, United.** *Charter of Fundamental Rights of the European Union.* s.l. : United Nations, 2000.

23. **Legemiddelverket.** LMI. *Legemiddelmangel? Meld fra i god tid.* [Online] https://www.lmi.no/2015/10/26/legemiddelmangel-meld-fra-i-god-tid/ .

24. **European association of hospital pharmacists.** 2018 Medicing shortage survey. *EAHP's 2018 Survey on medical shortages to improve patient outcomes.* [Online] [Cited: July 15, 2019.] http://www.eahp.eu/practice-and-policy/medicines-shortages/2018-medicines-shortage-survey.

25. **Sukkar, E. & Smith, H.** Panic in Greek pharmacies as hundreds of medicines run short. *The Guardian.* 2013.

26. **Health, Norwegian Institute of Public.** Continued high uptake for the Childhood Immunisation Programme in Norway. 2019.

27. **Norwegian Institute of Public Health.** Narcolepsy after swine influenza pandemic. 2017.

28. **European Medicines Agency.** *The European regulatory system for medicines and the European Medicines Agency- A consistent approach to medicines regulation across the EU.* 2014.

29. **European Union.** REGULATION (EU) No 1027/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. 2012.

30. —. DIRECTIVE 2011/62/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 . 2011.

31. —. Guidelines of 5 November 2013 on Good Distribution Practice of medicinal products for human use. 2013.

32. **Regjeringen.** Nasjonal beredskapsplan pandemisk influensa . October23 2014.

33. **WHO.** Essential steps for developing or updating a national pandemic influenza preparedness plan. 2018.

34. **United Nations.** International Covenant on Economic, Social and Cultural Rights. 1966.

35. **European Commission.** European social survey. *Exploring public attitudes, informning public policy.* s.l. : Engage Group.

36. *Handling og usikkerhet. Norske myndigheters kommunikasjon om svineinfluensapandemien i 2009.* **Ole Andreas Brekke, Kari Ludvigsen & Kristian Bjørkdahl.** 1, 2017, Norsk statsvitenskapelig tidsskrift, Vol. 3.

Annexes

Annex 1 – DRIVER+ Terminology

In order to have a common understanding within the DRIVER+ project and beyond and to ensure the use of a common language in all project deliverables and communications, a terminology is developed by making reference to main sources, such as ISO standards and UNISDR. This terminology is presented online as part of the Portfolio of Solutions and it will be continuously reviewed and updated[19]. The terminology is applied throughout the documents produced by DRIVER+. Each deliverable includes an annex as provided hereunder, which holds an extract from the comprehensive terminology containing the relevant DRIVER+ terms for this respective document.

Table A1: DRIVER+ Terminology

Terminology	Definition	Source
Crisis management	Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of the organization's key interested parties, reputation, brand and value-creating activities, as well as effectively restoring operational capabilities. Note 1 to entry: Crisis management also involves the management of preparedness, mitigation response, and continuity or recovery in the event of an incident, as well as management of the overall programme through training, rehearsals and reviews to ensure the preparedness, response and continuity plans stay current and up-to-date.	ISO 22300:2018(en) Security and resilience — Vocabulary. Link: https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en:term:3.60
Crisis Management Function	Crisis management functions aim at achieving effects, e.g. coordination, a direction of effort, shared awareness, etc., in a crisis management system-of-systems. The "function" focuses on what is to be achieved, not how or by whom. Several systems, tools, building blocks, etc. may individually or in concert deliver a given function and, conversely, may support several different functions. Crisis management functions are grouped in three functional areas: operational (protection, response, recovery), preparatory (mitigation, capability development, strategic adaptiveness) and common (security management, logistics, C3, comms & Info management).	Initial DRIVER+ definition

[19] The Portfolio of Solutions and the terminology of the DRIVER+ project are accessible on the DRIVER+ public website (https://www.driver-project.eu/). Further information can be received by contacting coordination@projectdriver.eu.

Terminology	Definition	Source
Crisis Management Taxonomy	A taxonomy of Crisis Management Functions describing strategically-directed activities to prevent, prepare, respond to and mitigate the effects of and recover from a crisis. Note 1 to entry: Taxonomy is a scheme of categories and subcategories that can be used to sort and otherwise organize itemized knowledge or information that are processed, organized and correlated to produce meaning.	ISO 5127:2017(en) Information and documentation — Foundation and vocabulary. Link: https://www.iso.org/obp/ui/#iso:std:iso:5127:ed-2:v1:en:term:3.8.6.07.
Portfolio of Solutions (PoS)	A database driven web site that documents the available Crisis Management solutions. The PoS includes information on the experiences with a solution (i.e. results and outcomes of Trials), the needs it addresses, the type of practitioner organisations that have used it, the regulatory conditions that apply, societal impact consideration, a glossary, and the design of the Trials.	Initial DRIVER+ definition
Societal impact	Dimension of Crisis Management that refers to its unintended positive or negative impacts on different societal groups or society as a whole, as well as on its core values and societal principles as captured for example in fundamental rights, constitutional laws, but also in public debate.	Initial DRIVER definition
Societal Impact Assessment	The process of identifying, analysing and managing intended and unintended (positive or negative) societal consequences.	Initial DRIVER+ definition
Solution	A solution is a means that contributes to a crisis management function. A solution is either one or more processes or one or more tools with related procedures	Initial DRIVER+ definition
Trial	An event for systematically assessing solutions for current and emerging needs in such a way that practitioners can do this following a pragmatic and systematic approach.	Initial DRIVER+ definition
Trial Guidance Methodology (TGM)	A structured approach from designing a Trial to evaluating the outcomes and identifying lessons learnt.	Initial DRIVER+ definition
Trial Guidance Tool (TGT)	A software tool that guides Trial design, execution and evaluation in a step-by-step way including as much of the necessary information as possible in form of data or references to the Portfolio of Solutions.	Initial DRIVER+ definition

Annex 2 Template- A Guide for Assessing the Societal Impact of Crisis Management Solutions

A GUIDE FOR ASSESSING THE SOCIETAL IMPACT OF CRISIS MANAGEMENT SOLUTIONS

Before you start:

- **Text in *italics* should be replaced by text.**
- **For identifying the functions of the solution to be assessed, please consult Annex 3, which contains the taxonomy of CM functions.**
- **For step 4: Please consult Annex 4, which contains a list of societal impact criteria, i.e. parts of society that might be affected by the CM function.**

GENERAL DESCRIPTION OF SOLUTION:

Name of solution to assess: *Write the name of the solution here*

By consulting the taxonomy of CM functions in Annex 3, which functions does the solution have?

Write a general description of the Crisis Management function that you want to assess. What is the purpose of the function? What does it do? Which activities is it used in? You can for example give some detail about why the specific function is relevant and needed in Crisis Management, at what point in time the function is most relevant, or who are involved in using the function.

STEP 1 STAKEHOLDER GROUPS / COMMUNITIES

The first step is to identify the stakeholders and the community/ communities that could potentially be impacted by the implementation of the solution at stake. Here, relevant questions to ask would start with "how could this specific function that my CM solution have, have an impact on the stakeholder groups or communities?" Who are the stakeholder groups or communities that could potentially be affected by the solution? General society, practitioners, law enforcement agencies? The rest of the assessment should be made with these in mind.

STEP 2 BACKGROUND INFORMATION

The next step is to collect reference information covering key social issues of the identified impacted communities such as community history, culture and key events that have shaped the development of the community. Are there known vulnerabilities in the community? Specific social challenges? Who are the major industrial actors? Relevant questions could be: Are there historical reasons to believe that the community where my solution will be carried out could find it problematic? Have there been controversies regarding the use of similar solutions in this area/ region/country?

STEP 3 RELEVANT LEGISLATION AND POLICIES

The third step is to provide an overview of relevant national/ EU legislation and policies that are directly related to the CM function you are assessing. Which formal restrictions exist that will influence the use of the solution? What are the policy discussions in the field? Have new legislations been introduced to regulate Crisis Management efforts? Are you dealing with a situation where there are identified gaps in terms of legislation, e.g. when if you are dealing with new technologies? What are the rules that you need to follow?

STEP 4 IDENTIFY AND PREDICT IMPACTS

The fourth step is the main part of the SIA, where a structured assessment, based on the information acquired in the previous steps takes place. The full aim is to identify potential direct social impacts and try to predict their significance, duration and extent. The SIA criteria (which is a list of how we think society could be affected by CM activities) listed in Annex 4 should be used to structure this thinking, but the idea is not to say something about each criterion. In some cases, the impacts may be rather obvious, and isolated maybe to issues of privacy and data protection, in which case only that one criterion might be relevant; yet, in other cases the societal issues might be more complex. Read through the list of criteria (a short version is given below) and try to think about which impacts could be relevant for the CM function you are assessing. Are some of the real-life examples in the criteria list in Annex 4 related to the function? Can you foresee similar impacts?

*Go through the collection of criteria below, highlight in **bold** the ones you think are relevant for your solution, and write a*

*reflection on how these criteria can be influenced positively or negatively by your solutions. For inspiration or guidance, you can also consult the ten example assessments which are available in the supporting document **D913.41 A guide on assessing unintended societal impacts of different CM functions - version 2**).*			
Unease – calmness	Suspicion – trust	Misuse – protection	New vulnerabilities – progress
Technology dependency – Flexible solutions	Function creep – specialized and controlled use	Sustainability	Accountability
Transparency	Integrity	Negative – positive standardization	International relations
State-citizen-relationship	Political reputation	Social cohesion and solidarity	Participation
Diversity	Open – control society	Cultural and gender sensitivity	Suitability, necessity and proportionality
In/justice & in/equality	Dignity/autonomy	Non-discrimination	Privacy & data protection
Freedoms and protest			
STEP 5 MITIGATING MEASURES			
As a fifth and final step of making an assessment, in order to lower the risk of negative unintended impacts, and/ or to increase the possibility for positive impact, a list of measures should be made. The list should be based on the potential impacts identified in the previous step and could include actions such as providing extra follow ups for volunteers, establish rapport with local community leaders, engaging with the communities, and sharing more information about the CM solution at stake. The background information you wrote in Step 1-3 should be underpinning the mitigating measures. A basic plan should be made to describe how the mitigating measures will be followed up on.			

Annex 3 DRIVER+ Taxonomy of Crisis Management Functions

Functional Area	Functions	Sub-functions
MITIGATION	Organise for mitigation	- Define national mitigation Framework - Provide expertise for hazards mapping, vulnerabilities and risk assessment
	Assess the risks	- Conduct all-hazards tracking - Assess vulnerabilities to hazards - Estimate the risks - Estimate collateral damage - Estimate cascading effects - Estimate cross-border impact
	Elaborate mitigation policy and strategy	- Provide policy guidance - Formulate the mitigation strategy - Establish planning and coordination - Conduct a mitigation communication campaign
	Implement mitigation measures	- Build-in safety, security and resilience into design and operations - Consider risks when locating new infrastructure - Promote PPPs to reduce vulnerabilities and hazards' impact - Control access to critical systems - Enhance awareness on vulnerabilities and mitigation measures - Enhance hazards education
	Keep the mitigation strategy relevant	- Establish a reporting mechanism - Assess mitigation strategy's implementation - Amend and update the mitigation strategy
CAPABILITY DEVELOPMENT	Plan for CM capabilities	- Establish a CM policy Framework - Determine future crises' scenarios and key characteristics - Define required CM capabilities - Assess current capabilities - Identify gaps and redundancies - Define capability options - Test the capability options - Coordinate and approve capability development plans
	Manage CM system of systems development	- Develop integrated warning and alerting - Develop the C3 system - Develop the communications and information management system - Develop decision support systems - Establish resource management and mutual aid system - Establish crisis logistics management system - Establish a solid waste collection system

Functional Area	Functions	Sub-functions
		- Manage equipment and infrastructure acquisition - Manage the system of reserves
	Manage human resources	- Manage professional responders - Manage volunteers
	Organise for crisis management	- Establish an integrated CM organisation - Define minimum activation requirements - Identify and analyse bottlenecks - Establish CM rules and standard operating procedures - Establish protocols for cross-border emergencies
	Establish CM doctrine and train organisations and people	- Develop doctrine - Coordinate and conduct research and education - Train individuals, teams and organisations - Certify personnel, training and education - Train resilient communities
	Establish a CM lessons learning system	- Develop after-action and lessons learned reporting - Provide cross-border learning
STRATEGIC ADAPTIVENESS	Promote CM organisational agility	- Establish continuous monitoring - Promote knowledge centricity - Maintain diverse and evolving competencies - Facilitate networking and cooperation - Exchange foresight experience and findings - Establish international exchange on adaptiveness
	Conduct civil security foresight	- Identify key drivers and trends - Identify plausible futures - Explore the implications of alternative futures
	Develop capacity to adapt	- Develop options and estimate required resources - Create and maintain materiel reserves - Establish hazards and CM research capacity and agenda
	Build and measure community resilience	- Strengthen community assets for resilience - Provide for bonding and linking communities' assets across borders - Improve communities' preparedness, responsiveness, learning, self-organisation, and innovation - Strengthen the community's capacity for collective actions - Establish measures and measurement of resilience
PROTECTION	Conduct systematic monitoring and data collection	- Conduct monitoring and anticipation - Raise awareness and anticipate

Functional Area	Functions	Sub-functions
	Conduct operational planning	- Establish an operational planning Framework - Plan across ranges and level of activities - Coordinate planning with support providers
	Conduct incident/ emergency response (below the level of "crisis")	- Detect pending emergencies and provide early warning - Coordinate and conduct incident SAR operations - Conduct emergency fire-fighting - Conduct emergency CBRN protection operations - Conduct ammunition and counter-IED operations - Conduct limited emergency evacuation operations
	Coordinate and provide public protection	- Safeguard public health - Assess safety, integrity and security of buildings - Provide safety during mass public events
	Protect critical infrastructures	- Maintain list of national and EU critical infrastructures - Establish Operator security plan - Introduce Security Liaison Officer - Develop training courses for CI vulnerability assessment - Apply case-specific protection measures - Establish CI reporting mechanism
	Coordinate and provide CII protection	- Protect physical and cyber assets, networks, applications, and systems - Secure networks and CI based on risk assessment - Protect personal data - Share cyber threat information and analysis - Implement standards for security, reliability, integrity, and availability of critical information - Identify, track, investigate, disrupt, and prosecute malicious actors - Back-up information and processes
RESPONSE	Orient and decide	- Determine the nature of the crisis - Conduct damage and needs assessment - Provide decision support - Manage warnings - Decide on the introduction of crisis legislation - Review and adjust the response plan
	Respond to the hazard	- Activate crisis management bodies - Maintain shared situational awareness - Conduct coordinated tasking and resource management - Deploy responders - Manage international sup-port - Safeguard emergency/crisis responders

Functional Area	Functions	Sub-functions
	Limit the impact of the crisis	- Contain hazardous causes of the crisis - Minimize threats of potential HAZMAT release - Take immediate law enforcement measures - Protect CI from secondary damage
	Support affected people	- Conduct SAR operations - Provide on-site first aid - Provide evacuation and shelter - Decontaminate persons - Provide off-site health and MHPSS services - Provide essential services to the affected community - Provide MHPSS - Establish emergency mobile phone - Provide care for animals
	Build the ground for relief and recovery	- Restore the delivery of basic services - Decontaminate assets and infrastructure - Initiate disaster area cleaning - Manage the transition from response to recovery
RECOVERY	Adjust the recovery planning	- Establish and share detailed COP - Modify recovery plans and policies - Amend norms and legislation - Provide for evidence-based decision-making
	Provide immediate relief support	- Expand the immediate health care - Upgrade the temporary sheltering - Provide psychosocial support - Provide electricity - Open critical transportation lines
	Engage the population	- Maintain population's operational awareness - Organise volunteers and communities for recovery - Identify communities' priorities and perceived benefits
	Manage humanitarian recovery	- Restore critical medical and MHPSS services - Provide reliable temporary sheltering - Establish temporary school organisation - Provide food, water, and energy for the population - Support families' reunification - Address the needs of vulnerable populations - Manage volunteers providing social services

Functional Area	Functions	Sub-functions
	Recover public lifelines	- Restore sustainable delivery of electricity - Restore delivery of potable water - Re-establish food supply chains - Restore mass transportation - Restore delivery of fuels - Restore local public services - Restore mass communications and Internet - Restore banking and commercial services - Restore postal services - Restore the solid waste collection system
	Manage economic recovery	- Assess economic reconstruction needs - Plan long-term economic recovery - Provide jobs incentives or unemployment assistance
	Manage infrastructure recovery	
	Manage environmental recovery	- Conduct environmental decontamination - Clean up the affected area - Develop policy for sustain-able rehabilitation - Remove damaged structures and debris
CRISIS COMMUNICATION AND INFORMATION MANAGEMENT	Establish CCIM [20] organi-sation	- Set-up an integrated CCIM network - Establish a concept of CCIM operations - Regulate access to CM communications and information - Provide secure storing and exchange of content
	Conduct and coordinate communications and information planning	- Activate an inter-agency CCIM team - Develop communications policy, plans and procedures - Establish relationships between CM authorities and media - Manage the frequency spectrum in a crisis - Manage visibility in media - Maintain a record of planning and decisions
	Create CCIM networks	- Build CCIM components and functionalities - Establish crisis communications capabilities - Establish emergency call services - Establish information management capabilities - Provide CCIM technology support

[20] CCIM – Crisis Communications and Information Management.

Functional Area	Functions	Sub-functions
	Continuously improve CCIM	- Establish equipment and training standards - Implement training programmes for CCIM
	Exploit CCIM for protection, response, and recovery	- Secure warning and alerting - Provide communications and information support to C3 - Support C3 decision making - Provide information to media and the public - Monitor media coverage - Detect and debunk deception and rumours in social media
COMMAND, CONTROL AND COORDINATION (C3)	Build and maintain the C3 system	- Design, test, and validate the C3 system - Prepare C3 personnel - Establish C3 information systems - Establish C3 procedures - Provide equipment, software, codes - Provide fixed and mobile command facilities - Maintain system's integrity
	Establish the command component	- Define the CM chain of command - Establish decision-making environment and resources
	Establish the control component	- Design a control system - Establish control capability at each command level - Determine the principles of information exchange - Establish all-hazards data-base - Provide scientific and technical advice - Establish rules for reporting
	Establish the coordination component	- Establish internal coordination - Establish coordination with societal, private and international organisations - Establish professional co-ordination - Establish transborder co-ordination - Establish coordination in transition from response to recovery - Establish coordination with media

Functional Area	Functions	Sub-functions
	Exploit the C3 system	- Monitor the affected area - Provide situational awareness, share COP - Provide orientation of decision-makers - Take and disseminate decisions - Task responders - C3 SAR and first responders operations - C3 volunteers operations - Manage and support International responders - Provide continuous deliberate planning - C3 delivery of critical support assets - Establish ad-hoc task groups - Maintain science and technology advisory capacity - Manage resources to cope with priority tasks - Provide warning and alerts for secondary hazards - Deliver public information and advice
LOGISTICS	Establish crisis logistics management system	- Identify the components of crisis logistics support - Establish supply chains - Provide end-to-end visibility of resources - Develop logistics policy, plans, and programmes - Establish logistics C3 - Provide norms for procurement in crises
	Manage materiel logistics	- Determine materiel requirements - Perform production logistics within "Preparedness" - Perform consumer logistics - Perform supply logistics - Perform maintenance and repair logistics - Create common operational Framework for prioritisation
	Conduct transportation logistics	- Plan, organise, and resource transportation logistics - Provide transportation of responders and supplies - Provide transportation equipment and procedures for its use - Provide transportation support to other stakeholders - Transport debris and waste
	Provide medical logistics	- Plan medical logistics - Provide medical supplies - Direct additional national and international medical support
	Manage facilities	- Select storage and distribution facilities - Operate facilities and manage related services - Manage evacuation camps and related services - Manage acquired property - Operate waste and debris management facilities

Functional Area	Functions	Sub-functions
	Provide logistics services	
SECURITY MANAGEMENT	Conduct security orientation and planning	- Develop security component in CM plans and systems - Establish programmes for acquisition of security capabilities - Establish preliminary coordination - Develop preparedness security guidance - Provide performance guidelines - Introduce security specific norms
	Establish security management organisation	- Establish security coordination and control organisations - Establish a crisis security clearance system - Introduce chief security officer - Establish security information exchange - Provide expertise and co-ordination for security planning
	Provide key security capabilities	- Staff with qualified personnel - Develop and conduct security management training - Supply security control equipment
	Exercise on-site security control	- Test critical infrastructure security plans - Ensure safe and secure CM environment - Perform access, traffic, and crowd control - Coordinate security measures with other operations

Annex 4 List of societal impact assessment criteria

SECONDARY IN/SECURITIES

Unease - Calmness	Whilst **unease** refers to anxiety or discontent[21], **calmness** refers to the state or quality of being free from agitation or strong emotion, disturbance or violent activity[22]. To create calmness, research indicates that the distributed information in CM needs to be experienced as being real and trustworthy (cf. *trust*), and that it doesn't feed rumours[23] and misconceptions during the crisis[24]. *Illustration: The CEO of German Wings has been celebrated for his communication strategy after one of their pilots, who were later known to suffer from depression, crashed a passenger airplane into the Alps. Many believed that he communicated information concerning the incident in a manner that had the right balance between truthfulness and at the same time only giving the necessary amount of information about the incident to the public[25]. In contrary, Malaysia Airlines were accused of creating more unease than calmness after experiencing one of their airplanes going missing in 2014. By not using the proper communication tools as well as failing in providing information based on well-established facts about the incident, this led to false rumours about the missing plane being an act of terrorism.[26]*
Suspicion - Trust	**Suspicion** refers to the feeling of suspecting something or being suspected of something dangerous or malicious[27]. In contrast, **trust** is tied to the firm belief that someone or something is reliable, good and honest. It also refers to the reliance on the integrity, strength, and ability of a person, a state, an institution, a system, or an organization[28]. High levels of trust are believed to have "virtues and tangible benefits for a society"[29].

21 https://en.oxforddictionaries.com/definition/unease

22 https://en.oxforddictionaries.com/definition/calmness

23 To control rumours and misconceptions spreading in the population during the hurricane Irma, the Federal Emergency Management Agency (FEMA), created a web page that listed the most common rumours and then confirmed them as correct/incorrect as well as giving additional information. See: https://www.fema.gov/hurricane-irma-rumor-control

24 Schnackenberg, A.K., Tomlinson, E.C. (2014), Organizational Transparency. A New Perspective on Managing Trust in Organization-Stakeholder Relationships. Journal of Management. doi:10.1177/0149206314525202

25 https://www.thedrum.com/news/2015/03/28/pr-experts-applaud-lufthansas-crisis-communications-approach-germanwings-disaster

26 https://www.missionmode.com/disaster-recovery-lessons-learned-malaysia-airlines/

27 http://dictionary.reference.com/browse/function%20creep?s=t

28 http://dictionary.reference.com/browse/trust

Illustration: The information shared during a crisis is trustworthier if it derives from sources that the general public finds reliable. A general trend in Europe and North-America, is that Police Departments use social media like Twitter to build relations with the public and to spread information concerning actual events in their geographical area[30]. For this to be a productive measure, the public's trust in the police needs to be at a certain level, and can in the long run lead to enforcement of the public's co-operation and collective action during a crisis[31]. The Boston PD used Twitter as their main communication tool in the aftermath of the Boston marathon bombing in 2013 to provide accurate and updated information. The use of Twitter led to a two-way communication with the public creating calmness (cf. calmness) and perhaps also a more cohesive (cf. social cohesion) community[32].

Misuse - Protection

Protection means to preserve or protect the population or infrastructure from harm and protection can also refer to protecting non-material assets, such as central societal values[33]. **Misuse** refers to the wrong or inappropriate use of materials, methods, knowledge or technology, and/or to the use for the wrong purpose[34] (cf. *function creep*). When a CM tool or solution is misused, it can undermine its protection value.

Illustration: Protection of human lives is one of the most important tasks in the event of a crisis and that means that rescue operations must be conducted quickly and effectively. In the case of natural disasters, Unmanned Aerial Vehicles (UAVs), can be used to gather information during the crisis, to see how the crisis population move

---

29 Thomassen, G. (2013). Corruption and trust in the police: A cross-country study. European Journal of Policing Studies, 1(2), 152-168. Link: https://brage.bibsys.no/xmlui/bitstream/handle/11250/174706/corruption%20and%20trust.pdf?sequence=3&isAllowed=y

30 Kudla, D., & Parnaby, P. (2018). To Serve and to Tweet: An Examination of Police-Related Twitter Activity in Toronto. Social Media + Society, 4 (3), pp. 1-13. https://journals.sagepub.com/doi/abs/10.1177/2056305118787520#articleCitationDownloadContainer

31 Thomassen, G. (2013). Corruption and trust in the police: A cross-country study. European Journal of Policing Studies, 1(2), 152-168. Link: https://brage.bibsys.no/xmlui/bitstream/handle/11250/174706/corruption%20and%20trust.pdf?sequence=3&isAllowed=y

32http://apps.prsa.org/intelligence/Tactics/Articles/view/10197/1078/How_the_Boston_Police_used_Twitter_during_a_time_o#.XIorVvZFybg

33 https://en.oxforddictionaries.com/definition/protect

34 http://www.oxforddictionaries.com/definition/english/misuse

in the affected area and to perform a damage assessment[35]. The use of UAVs to make an assessment of the area can therefore be a tool that protects both the affected crisis population and aid workers from harm. UAVs have been used in CM activities such as forest fires[36] to better direct the firefighting activities and detect hotspots. However, UAVs can also be misused to the extent that they propose a threat to the safety of emergency workers[37]. In the context of forest fires, unauthorized use of UAVs by civilians have forced fire fighters to ground their aircrafts due to aerial safety and therefore not been able to continue their work[38].

New Vulnerabilities - Progress

Progress indicates that something is developing to an improved or more advanced condition[39] which is often the case in the field of CM. When new tools and solutions are developed and implemented they face the risk of creating additional (new) vulnerabilities. Such **vulnerability** refers to the risk of being exposed to the possibility of being attacked or harmed, either physically or mentally[40].

Illustration: A new vulnerability in relation to CM can be technology dependency (cf. technology dependency). The Norwegian Public Safety Network (Nødnett)[41] is a digital radio connection implemented in 2015 for the emergency services to provide secure and robust communication during crisis and emergencies. It has although been shown in several cases with bad weather, that the Nødnett has collapsed, and that emergency services in small towns and villages have not been able to communicate for several hours[42] [43]. The consequence is that the emergency services do not get information about incidences that requires them to respond, putting both the public and their workers in danger and therefore representing a new vulnerability that makes it more difficult to

35 Erdelj, M. & Natalizio, E. (2016) UAV-assisted Disaster Management: Applications and Open Issues. Link: https://www.researchgate.net/publication/301710340_UAV-assisted_disaster_management_Applications_and_open_issues

36 See for example: https://www.uasvision.com/2017/07/24/forest-fire-control-using-drones/

37 https://www.thejournal.ie/drones-wildfires-hot-weather-4112336-Jul2018/

38 https://www.theatlantic.com/science/archive/2018/06/dont-fly-drones-into-disasters/562997/

39 https://en.oxforddictionaries.com/definition/progress

40http://www.oxforddictionaries.com/definition/english/vulnerable?q=vulnerabilities+#vulnerable__7

41 https://www.nodnett.no/en/

42 See for example: https://www.nrk.no/norge/_knud_-slo-ut-nodnettet_-_-det-er-en-skandale-1.14219126

43 See for example: https://www.nrk.no/sognogfjordane/rapport_-_-det-nye-naudnettet-er-sarbart-og-lite-robust-under-ekstremver-1.12984984

protect (cf. protection) the public from harm.

Technology Dependency - Flexible Solutions

Flexibility[44] is important when responding to the needs of a country struck by crisis, as this means that the crisis management efforts can be easily modified to respond to the altered circumstances and situational needs. When a society becomes dependent on a certain technology, making the society vulnerable in case that technology falls out or becomes temporarily unavailable, we talk about **technology dependency.**

Illustration: Ensuring flexible CM capability in an organization can make it easier to maintain effective lines of communication, e.g. because several solutions to communicating exist at the same time. This can create a CM operation that is able to not only better communicate relevant and true information to the public, but further, have positive spill over-effects on such factors as transparency (cf. transparency) and calmness (cf. calmness) in the population. During the Boston Marathon Bombing, the Boston Police District, had to shut down the cell phone service in the affected area as there was a belief that cell phones were used to detonate bombs[45]. The PD decided to use Twitter as their main communication tool to reach out to the public, and thus showing flexibility in times of crisis.

Function Creep - Specialized and Controlled Use

Function creep can be defined as the gradual widening the use of a technology, function or system beyond the purpose for which it was originally intended.[46] A **specialized and controlled** CM solution however is tailored to special conditions or restricted to special functions and is less easy to misuse (*cf. misuse*) and minimises the risk of function creep.

Illustration: Function creep is often discussed in relation to surveillance technology and information systems. Information systems, i.e. forensic DNA-databases, are one of the most flexible solutions because both their material assets (computers, servers,

44 https://en.oxforddictionaries.com/definition/flexible

45 See for example: http://apps.prsa.org/intelligence/Tactics/Articles/view/10197/1078/How_the_Boston_Police_used_Twitter_during_a_time_o#.XIorVvZFybg

46Dahl, J. Y. & Sætnan, A. R. (2009). "It all happened so slowly": On controlling function creep in forensic DNA databases. International Journal of Law, Crime and Justice, 37(3), 83-103. Link: https://brage.bibsys.no/xmlui/bitstream/handle/11250/174624/it%20all%20happened%20%20so%20slowly.pdf?sequence=5&isAllowed=y

etc.) and the information content can be used in many ways[47]. Due to progress (cf. progress) in DNA-technology, in the UK, it is now possible to perform familial searching in the forensic DNA-database. This means that when a DNA-profile is retrieved from a crime scene but does not have a clear match in the database, it is possible to search for similar profiles. Because relatives are more likely to have similar DNA-profiles than non-relatives, it is possible to find matches that are close to the profile of a registered offender and then may point to someone in the close family of that person. This opens for further surveillance not only of registered offenders, but also their relatives, and this can be defined as function creep.

SUSTAINABILITY

Sustainability

In the context of CM, this refers to the **sustainability** of an organization or a community (e.g. in terms of fostering and balancing resilience) and the endurance of certain values. This includes that something can be maintained at a certain level or rate, or that it can be upheld or defended[48].

Illustration: A sustainable society, DRR is described as a good practice, and essential to strengthening resilience as it enables communities to anticipate, absorb and bounce back from shocks.

POLITICAL & ADMINISTRATIVE PRINCIPLES

Accountability

Accountability is the obligation of an individual or organization to account for its activities, accept responsibility for them, and to disclose the results in a transparent (*cf. transparency*) manner[49]. In the context of CM, accountability should be primarily directed in a responsible manner to those who are directly affected and vulnerable to crisis.

Illustration: Typically, during CM situations, many different organizations and actors implement a variety of measures. If the accountability for conducting these measures or using CM

47 Dahl, J. Y. & Sætnan, A. R. (2009). "It all happened so slowly": On controlling function creep in forensic DNA databases. International Journal of Law, Crime and Justice, 37(3), 83-103. Link: https://brage.bibsys.no/xmlui/bitstream/handle/11250/174624/it%20all%20happened%20%20so%20slowly.pdf?sequence=5&isAllowed=y

48http://www.oxforddictionaries.com/definition/english/sustainable?q=sustainability#sustainable__6

49 World Bank (2015), Accountability in Governance, http://siteresources.worldbank.org/PUBLICSECTORANDGOVERNANCE/Resources/AccountabilityGovernance.pdf

tools is not clearly set out beforehand, potential negative side-effects and damages cannot be regulated effectively in the aftermath. Failure to decide who was accountable in the prediction of hurricanes led to conflicts in the aftermath of the hurricane Katrina. The consequence became that the local, state and federal actors target of great criticism[50]. It is thus crucial to determine accountability beforehand as a part of planning measures and tools, in order to reach the most positive societal effects.

Transparency

Transparency means information disclosure, clarity and accuracy to enhance "the perceived quality of intentionally shared information from a sender"[51].
Not all actions under CM are visible to the crisis population, but they may nonetheless have consequences for the population's rights, actions and reactions. It is therefore important to communicate about and make such actions visible as this can make the societal acceptance of such measures higher *(cf. trust).*

Illustration: Automatic Number Plate Recognition (ANPR) is an advanced police surveillance technology that may be used to track a citizen's movements, but the storing of such data raises privacy (cf. privacy and personal data protection) and safety concerns. In the UK, a study that examined the population's perception of ANPR has showed that the population calls for more transparency from the police in regards to the objectives, purposes and exact use of the information collected with ANPR[52]. There is also a need for the police to communicate more transparently about the advantages and consequences the population might expect of such technology. This is also closely related to the levels of trust (cf. trust) in the police and the respondents believed that the level of trust in the police would incline if the technology is used in a fair and effective manner that protect people's rights[53].

50 Brändström, A. (2016) Crisis, Accountability and Blame Management: Strategies and Survival of Political Office-Holders. Crismart volume 44. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A896367&dswid=-1103

51Schnackenberg, A.K., Tomlinson, E.C. (2014), Organizational Transparency. A New Perspective on Managing Trust in Organization-Stakeholder Relationships. Journal of Management. doi:10.1177/0149206314525202

52 Haines, Alina (2009) The role of automatic number plate recognition surveillance within policing

and public reassurance. Doctoral thesis, University of Huddersfield. Link: https://core.ac.uk/reader/54165

53 Haines, Alina (2009) The role of automatic number plate recognition surveillance within policing

and public reassurance. Doctoral thesis, University of Huddersfield. Link: https://core.ac.uk/reader/54165

Integrity

Integrity means to adhere to ethical principles[54] when planning and implementing CM measures and tools, but it also means "standing for something" and showing this through truthful, accurate and consistent actions, values and principles[55] [56]. This also means to be predictable and following a certain set of rules.

Illustration: A CM measure/organization has a high level of integrity when it respects widely accepted ethical codes and rights, such as the European Charter for Fundamental Rights. Integrity is also an important aspect of network security and resilience, which means that the operators' obligation to meet risks in an appropriate way and to report security breaches must be strong[57].

Negative - Positive Standardisation

Standardisation generally describes the process of developing a specific level of quality or attainment[58] for materials, products and services to ensure that they are "safe, reliable and of good quality"[59]. In relation to SIA it refers to a qualitative and social process. **Positive standardisation** refers to the process of implementing standards that have positive societal effects. **Negative standardisation** refers to the overarching social process of establishing a procedure as normal although it has detrimental effects**.**

Illustration: CM tools and principles that are ethically acceptable, suitable, necessary and proportional (cf. acceptability, suitability, necessity & proportionality) can be considered for standardisation, as they are likely to contribute to a positive societal impact. This could e.g. be to promote the standardisation of a common international terminology to

54 Merriam-Webster Dictionary (2015b), Integrity, http://www.merriam-webster.com/dictionary/integrity retrieved November 20, 2015.

55 Lucaites, J.L., Condit, C.M., (1999), Contemporary rhetorical theory: A reader, New York, Guilford Press.

56 Merriam-Webster Dictionary (2015b), Integrity, http://www.merriam-webster.com/dictionary/integrity retrieved November 20, 2015

57 European Commission (2009), Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

58 http://www.oxforddictionaries.com/definition/english/standard

59 International Organization for Standardization https://www.iso.org/standard/23390.html

ease international cooperation in CM[60].

International Relations

International relations describe the relations and collaboration across borders. International relations are often organized and officially regulated in international treaties. Emergencies can easily become a matter of international concern and therefore necessitate international cooperation, but such cooperation also involves the risk of causing (unwanted) spill over effects in other domains of international relations if not properly managed.

Illustration: Working together in global and local partnerships (e.g. through research cooperation) is central to strengthen resilience. For countries facing recurrent crises, working with regional and international organizations to create platforms at country level for facilitating the exchange of information can be important to strengthen resilience[61]*. The European Forest Fire Information System (EFFIS) is a collaboration between 40 countries in Europe and plays an important role in the prevention of forest fires by the sharing of information and expertise. In the summer of 2018 there were severe forest fires in multiple European countries and cooperation and emergency assistance between countries were important. In Sweden, the national fire fighters were assisted with fire-fighting aircrafts from Norway and Italy*[62]*.*

LEGITIMACY

State-Citizen-Relationship

The state derives its legitimacy from its interaction with citizens[63]. States are legitimate when elites and the public accept the rules regulating the exercise of power as proper and binding[64]. **The state-citizen relationship** is thus a relationship marked by the legitimate exercise of power.

60 The DRIVER+ deliverable **D955.11** offers an overview of relevant standardized terminology in CM at both international and European level.

61 European Commission (2013), Action Plan for Resilience in Crisis Prone Countries 2013-2020, http://ec.europa.eu/echo/files/policies/resilience/com_2013_227_ap_crisis_prone_countries_en.pdf retrieved November 20, 2015

62 https://www.theguardian.com/world/2018/jul/18/sweden-calls-for-help-as-arctic-circle-hit-by-wildfires

63 Papagianni, K. (2008), Participation and State Legitimation, in: Call, C.T., Wyeth, V. (eds), Building States to Build Peace, Boulder, Lynne Rienner Publishers.

64 Papagianni, K. (2008), Participation and State Legitimation, in: Call, C.T., Wyeth, V. (eds), Building States to Build Peace, Boulder, Lynne Rienner Publishers.

Illustration: The Fukushima Daiichi nuclear disaster in March 2011 is an example of how a state can undermine its legitimacy by not communicating transparently (cf. transparency), fact-based and not being accountable (cf. accountability) for its actions and responsibilities towards the population during a crisis[65]. The state was unaware of an already existing system that can predict the geographical spreading of radioactive material. The evacuation zone was therefore set in an arbitrary way which led it to being expanded three times in under 24 hours making the population move several times. A short time after, radioactivity was shown far outside the last evacuation zone. This led to unease (cf. unease) in the evacuated population and eventually distrust (cf. trust) in the government. The state-citizen relationship was further weakened as recommendations came from the U.S. government to its citizens in Japan to move even further away from the last evacuation zone.

Political Reputation

Political reputation refers to the social opinion[66] and evaluation of a political entity. Bad political reputation is often accompanied with a low acceptance of policy measures. If the crisis population does not trust (cf. *trust*) the administrational- or governmental actors that are implementing the crisis effort, it is less likely to be successful. The reputation of a political entity is therefore strongly influenced by public discourses[67].

Illustration: In crisis situations, it is important to follow principles of transparency and integrity to foster political and societal acceptability of measures (cf. integrity; transparency). During the CM of the Fukushima Daiichi nuclear disaster, Prime Minister Kan's handling of the situation gave him a bad political reputation, which forced him to retire after a short period. This was related to the fact that he did not take any responsibility or held himself and the government accountable for preventing the situation at the nuclear plant from

65 Kim, Y. (2018) Analyzing Accountability Relationships in a Crisis: Lessons From the Fukushima Disaster. American Review of Public Administration, 48 (7), pp. 743-760. Link: https://journals-sagepub-com.ezproxy.uio.no/doi/pdf/10.1177/0275074017724224

66 http://www.oxforddictionaries.com/definition/english/reputation

67 Bennett, C. J. (2011), Review: In Defence of Privacy: The concept and the regime. Surveillance & Society 8(4): 485-496.

escalating into a man-made disaster[68]. Instead he blamed the situation on the tsunami as being bigger than what could be imagined in advance. In addition, he decided to make an official visit to the nuclear plant to show his support, but the consequence of this visit was that the emergency work were upheld for two hours. A case study on floods in Sri Lanka has shown that officials who arrive in disaster areas just to observe might create negative and uncomfortable feelings amongst the affected crisis population[69]. The prime minister's visit to the nuclear plant might therefore have worsened his political reputation in the time of crisis.

SOCIETAL & ETHICAL PRINCIPLES

Social Cohesion & Solidarity

Social cohesion is the capacity of a society to ensure the wellbeing of all its members, minimising disparities and avoiding marginalisation[70]. Cohesive societies manage differences and divisions and ensures the means of achieving welfare for all members[71]. Social cohesion thus refers to the reduction of disparities, inequalities (cf. *in/equality*) and social exclusion within or between societal groups, as well as the strengthening of social relations, interactions and trust (cf. *trust*)[72]. **Solidarity** refers to the feeling or action that produces a community of interests, objectives and standards. It is a common way to show mutual support within a group. The fundamental principle of solidarity of the EU is based on sharing both the advantages, i.e. prosperity, and the burdens equally and justly among all group members. Also, the solidarity clause in the Treaty on the Functioning of the EU (TFEU- Lisbon Treaty) introduces a legal obligation on the EU and its member States to assist each other when an EU State

68 Kim, Y. (2018) Analyzing Accountability Relationships in a Crisis: Lessons From the Fukushima Disaster. American Review of Public Administration, 48 (7), pp. 743-760. Link: https://journals-sagepub-com.ezproxy.uio.no/doi/pdf/10.1177/0275074017724224

69 Samarakoon, U. & Abeykoon, W. (2018) Emergence of Social Cohesion after a disaster: (With reference to two affected locations in Colombo District-Sri Lanka). Procedia Engineering, 212, pp. 887-893. Link: https://doi.org/10.1016/j.proeng.2018.01.114

70 Council of Europe (2008), Towards an Active, Fair and Socially Cohesive Europe. Report of High-Level Task Force on Social Cohesion, http://www.coe.int/t/dg3/ retrieved November 20, 2015.

71 Council of Europe (2008), Towards an Active, Fair and Socially Cohesive Europe. Report of High-Level Task Force on Social Cohesion, http://www.coe.int/t/dg3/ retrieved November 20, 2015.

72 http://dictionary.reference.com/browse/trust

suffers a terrorist attack or a natural or man-made disaster[73].

Illustration: CM measures have the potential to positively affect social cohesion if they are applied equally and not in a discriminatory or unequal manner against a specific social group. Creating a societally cohesive community of volunteers and responders can positively influence the resilience and flexibility of the CM organization. An equal and non-discriminatory (cf. non-discrimination) distribution of emergency help, taking the needs of different societal groups into account, can also foster trust (cf. trust).

Participation

Participation is both the action of taking part in something, and the state of being (actively) related to a community, region, or nation[74]. As a core societal value, participation is understood as public participation - the belief that those who are affected by a decision have a right to and an interest in being involved in the decision making-process. Participation is also an opportunity for the population to hold decision makers accountable *(cf. accountability)*[75].

Illustration: Public participation during the decision-making processes is thought to increase its acceptance among the affected population once it is implemented. In Denmark, developers planned to build a bridge that would cross over a small, populated island. The island residents were left out of the decision-making process, and they feared that the bridge would ruin the island atmosphere and inflict social aspects of their daily life. When it was discovered that a certain endangered newt lived on the island, the residents started to protest using arguments of the environmental impact of the bridge as they felt that the societal aspects were not considered important enough to stop the developers from building it[76]*. This example underlines the importance of implementing SIAs into all kinds of developments that affects the society.*

---

73 European Union (2007), Official European Union, C 306, 17 December 2007, http://www.-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-5-external-action-by-the-union/title-7-solidarity-clause/510-article-222.html & http://europa.eu/lisbon_treaty/full_text/index_en.htm retrieved November 20, 2015.

74 http://www.oxforddictionaries.com/definition/english/participation

75 UNDP report, p. 58. Link: http://www.undp.org/content/dam/undp/library/crisis%20prevention/disaster/Strengthening%20Disaster%20Risk%20Governance-Full-Report.pdf

76 Larsen, S. V., Hansen, A. M., Lyhne, I., Aaen, S. B., Ritter, E. & Nielsen, H. (2016) Social Impact Assessment in Europe: A Study of Social Impacts in Three Danish Cases. Journal of Environmental Assessment Policy and Management, 17 (4). Link: http://vbn.aau.dk/files/262085253/Larsen_et_al_2015_VBN_version.pdf

Diversity

Diversity[77] refers to the condition of having or being composed of differing elements, especially, the inclusion of different types of people in a group, organization or country. It involves the wide range of racial, cultural, ethnic, linguistic, and religious variation that exists within and across societies. Cultural, religious and linguistic diversity is recognized and protected by the European Charter of Fundamental Rights (art. 22) (Cf. *dignity*; *non-discrimination; cultural & gender sensitivity*).

Illustration: In the CM context, recognizing the diversity in the affected crisis population is important. According to research, minority communities recover slower after a crisis because they are more likely to experience cultural barriers. This is first and foremost linked to the fact that these communities often receive inaccurate or incomplete information because of cultural differences and language barriers[78]*. Failing to give accurate information in the right language can in the worst case make the crisis bigger. As shown during the Ebola crisis, just a small percentage of the population at risk where given information about how to avoid infection in a language that they understood. The people that was not informed properly had to lean on rumours on how to avoid infection. These rumours were often completely wrong, and the consequence was that the disease spread quickly and came out of control. Further, it created unease (cf. unease) in the population and suspicion (cf. suspicion) to all sorts of sources that spread information about infection dangers*[79]*.*

Open - Control Society

An **open society** is characterized by a flexible structure, freedom of belief, a wide dissemination of information[80] and a respect for core societal values. This creates a feeling of trust and security in society (cf. *trust*)[81]. **Societies of control**, however, might use control technologies to establish security,

77 http://www.merriam-webster.com/dictionary/diversity

78 Davidson, TM, Price M, McCauley JL, Ruggiero KJ, Disaster Impact Across Cultural Groups: Comparison of Whites, African Americans, and Latinos. American Journal of Community Psychology. 2013;52(1-2):97-105.

79 https://odihpn.org/magazine/ebola-a-crisis-of-language/

80 http://www.oxforddictionaries.com/definition/english/open-society?q=open+society

81 Studies suggest that when there is trust in the government, there is also trust in the police which is important in the CM. See for example:
https://brage.bibsys.no/xmlui/bitstream/handle/11250/174706/corruption%20and%20trust.pdf?sequence=3&isAllowed=y

which may also apply to CM tools. Societies of control create a feeling of security that is based on distrust (cf. *trust*).

Illustration: The use of technologies to single out potential troublemakers during a large event may contribute to the preparedness and responsiveness of CM, but they are also based on the idea of establishing or achieving security through control. To ensure that this kind of control is perceived as proportional, it is important to ensure the acceptability of the use of such technologies, which can streamline and improve CM.

Cultural & Gender Sensitivity

CM decisions, communication, tools and measures can have different effects on men and women and groups with different cultural backgrounds. It is therefore important that they show **sensitivity to gender and cultural background** throughout all phases of the CM cycle. Research indicates that racial and ethnic minorities are disproportionality vulnerable to, and impacted by, a crisis. In the same manner, differences are correlated to gender in terms of exposure to and perceptions of risk, preparedness, response, and physical and psychological impact, as well as capacity to recover[82].

Illustration: Women's role as breastfeeding mothers should be taken particular care of during a crisis[83] [84]. However, at the same time, a single father with the responsibility for feeding a new-born needs equally good care. There is also research that shows that women often face issues related to increased violence and sexual harassment in evacuation centres as well as lack of privacy[85]. A solution might be the availability of female crisis managers to female aid recipients and male managers for male aid recipients as this may contribute positively towards gender sensitivity.

LEGAL VALUES

82 https://www.phe.gov/Preparedness/planning/abc/Documents/gender-2017.pdf

83 European Commission (2013), Disaster Risk Reduction. Increasing Resilience by Reducing Disaster Risk in Humanitarian Action, http://ec.europa.eu/echo/files/policies/prevention_preparedness/DRR_thematic_policy_doc.pdf retrieved November 20, 2015.

84 European Commission (2014), AGIR – Building Resilience to food and nutrition crisis in the Sahel & West-Africa, http://ec.europa.eu/echo/files/aid/countries/factsheets/sahel_agir_en.pdf retrieved November 20, 2015.

85 Saito, F. (2012) Women and the 2011 East Japan Disaster. Gender & Development, 20 (2), pp. 265-279. Link: https://www-tandfonline-com.ezproxy.uio.no/doi/pdf/10.1080/13552074.2012.687225?needAccess=true

Suitability, Necessity & Proportionality

The «**proportionality** test» is an instrument in EU law[86] to determine fairness and justice. It examines a measure/tool in terms of its **suitability,** asking whether the appropriate means are being used to pursue the given objective. In a second step, the test examines the **necessity** of a measure/tool, asking whether there is an alternative measure that is less restrictive than the measure in question and that is equally effective in achieving the pursued objective[87]. Finally, the test examines the proportionality in strict sense, namely whether the effects of the measure "are disproportionate or excessive in relation to the interests affected. At this stage the true weighing and balancing takes place."[88]

Illustration: Airborne sensors in unmanned aerial vehicles (UAVs) can be a suitable means to get an overview of an emergency. Alternative measures, for example manned helicopters (for non-automated data collection), do exist to fulfil this task as well. Helicopters may, however, be more expensive, so there is potentially a financial necessity to use airborne sensors; or sensors might have an added value as compared to human surveillance. The key question is then whether an airborne sensor, by collecting vast amounts of data that is not relevant for the situational analysis, is proportional to the objective in the narrow sense. This must be balanced vis-à-vis the benefits of the airborne sensor. If CM measures are not proportional, they will cause several secondary effects, for example a low level of acceptability of negative standardisation (cf. negative standardisation), which could contradict the effect/ aim of CM.

In/justice & In/equality

Just and equal CM means that the activity is exercised according to certain principles (e.g. human rights) and that it is equitable, fair, non-partial and proper. Further, it means that it is rightful and lawful, and facilitates the treatment of all individuals in the same way. While it is a standard to provide support for the most affected and the most vulnerable first, the fair, just and equal distribution of help and resources during crises needs to be assured. Equal treatment cannot always be a given, since time and resources are often limited

86 Craig, P., & de Búrca, G., (2011), EU Law: Text, Cases, and Materials, Oxford : Oxford University Press.

87 Dzabirova, L., (2009), European Proportionality in Macedonia's Political and Judicial Systems, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/d-mk/dv/0120_09/0120_09en.pdf

88 Dzabirova, L., (2009), European Proportionality in Macedonia's Political and Judicial Systems, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/d-mk/dv/0120_09/0120_09en.pdf

and sometimes seemingly unfair decisions have to be taken and priorities set. The idea is anyhow to avoid unfair, unequal or disproportionate treatment of two social groups or between two individuals wherever possible (cf. *non-discrimination*; *gender- and culture sensitivity*).

Illustration: The absence of women in the decision-making process (cf. participation) has been shown to create issues during the response and recovery phase in CM[89]. This is especially related to the fact that women play a significant role at the household level. In the evacuation shelters in Japan after the 2011 tsunami and nuclear plant incident, women were expected to cook meals for the shelters for free, but men were given the opportunity to do paid work within the shelter[90]. This was especially problematic for single mothers who then struggled to take care of their children in the recovery phase. Thus, by taking efforts to promote the inclusion of and influence by, women in CM and decision-making about CM in all levels of the CM organization (locally, regionally and internationally) could result in a more equal CM organization.

FUNDAMENTAL RIGHTS

Dignity /Autonomy

Dignity is considered to be a universal value of the European Union. It means that a human being has an innate value and the right to be treated with respect. This right is inviolable and must be protected in accordance with Article 1 of the European Charter of Fundamental Rights[91]. Dignity is very closely related to **autonomy**, that can either mean independence of freedom or the condition of being autonomous[92].

Illustration: *It is not a given that residents wish to be evacuated during crisis[93]. The choice to evacuate regardless can be said to affect the autonomy of the residents. Leaving the choice to inhabitants to act against authorities' advice*

89 Hemachandra, K., Amaratunga, D. & Haigh, R. (2017) Role of women in disaster risk governance. Procedia Engineering, 212 (2018), pp. 1187-1194. Link: https://www-sciencedirect-com.ezproxy.uio.no/science/article/pii/S1877705818301796

90 Saito, F. (2012) Women and the 2011 East Japan Disaster. Gender & Development, 20 (2), pp. 265-279. Link: https://www-tandfonline-com.ezproxy.uio.no/doi/pdf/10.1080/13552074.2012.687225?needAccess=true

91 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf retrieved November 20, 2015.

92 http://dictionary.reference.com/browse/autonomy?s=t

93 Associated Press (2008), Even after Hurricane Katrina, many won't leave. http://www.nbcnews.com/id/25819569/ns/us_news-life/t/even-after-hurricane-katrina-many-wont-leave/#.Vijr034rKJA

while clarifying the consequences of staying and leaving their homes, including all related responsibilities, will respect the autonomy of the individuals. However, such a guideline of informing aid recipients about consequences of taking their own choice is highly contextual. In some situations there is little time to inform aid recipients. These considerations thus need to be weighed against the responsibilities that a state has towards their citizens to evacuate effectively in case of an acute emergency.

Non-Discrimination

Dignity (cf. *dignity*) is closely related to Article 21 of the European Charter of Fundamental Rights[94], the right to **non-discrimination**, which forbids any discrimination "based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation"[95] (cf. *diversity*; *cultural & gender sensitivity*). A consequence of discrimination in CM is that it can increase the vulnerability of certain groups during a crisis.[96] [97]

Illustration: The Federal Emergency Management Agency (FEMA) issued a set of guidelines[98] to use under the Hurricane Harvey in Texas and Louisiana to effectively communicate with all parts of the affected population in a non-discriminatory way. The guidelines included for example the provision of sign language interpreters, crisis information translated in all major languages used in the affected areas, reaching out to local ethnic media services and making information websites accessible for disabled persons.

94 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf retrieved November 20, 2015.

95 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

96 Bethel, JW, Burke, SC, Britt, AF. Disparity in disaster preparedness between racial/ethnic groups. Disaster Health. 2013;1(2):110-16. Link: https://www.tandfonline.com/doi/abs/10.4161/dish.27085

97 See for example a video on how the Red Cross prioritize aid to elderly and disabled persons in the time after the flood in the Tabasco region, Mexico, in 2007: http://www.rcrc-resilience-southeastasia.org/document/non-discrimination-in-disaster-response-2007-tabasco-floods/

98 https://www.dhs.gov/publication/tips-effectively-communicating-protected-populations-during-preparedness-response-and

Privacy & Data Protection

Article 7 of the European Charter for Fundamental Rights[99] protects **the right to privacy** as the right for private and family life. But privacy is no longer "the right to be let alone"[100]. It has become a concept, a regime, a set of policy instruments and a way to frame civil society activism. A working definition is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". As such, it is closely related to **the protection of personal data** (Article 8). Protection also means that data has to be processed fairly, with the consent of the concerned person, who also has the right to access this data. The General Data Protection Regulation (GDPR)[101] governs the processing of personal data within the EU and includes collection, storage, alteration, consultation, transmission, or erasure of personal data[102].

Illustration: To gather situation-sensitive information through social media during a crisis represents progress (cf. progress) in CM as it gives the crisis managers the opportunity to gather information from eyewitnesses in the affected area. The Crisis Centre in Belgium especially asked citizens to communicate situational information through social media during the terrorist attack in Brussels the 22 March 2016[103]. It can result in a more effective response, but it also involves concerns for privacy and protection of personal data (cf. privacy and data protection)[104] (cf. function creep, misuse). It is therefore necessary to reflect upon what kind of keywords (or hash tags) that are used in the data processing, so that data that are not necessary for the purpose of the needed analyses are not collected. CM measures that respects, and even advances best practice solutions in the area, have the opportunity to foster trust in the population and improve the (political) reputation of the CM actor(s). This opportunity is closely linked to the notion

99 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

100 Warren, S., & Brandeis, L. (1890), The Right to Privacy. Harvard Law Review 4:193-220.

101 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

102 http://www.isitethical.eu/portfolio-item/privacy-and-personal-data-protection/

103 Mirbabaie, Milad and Zapatka, Elisa, (2017). "Sensemaking in social media crisis communication – a case study on the Brussels bombings in 2016". In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017 (pp. 2169-2186).

104 Imran, M., Meier, P. & Boersma, K. (2018) The use of social media for crisis management. In: Big Data, Surveillance and Crisis Management. Edited by: Boersma, K. & Fonio, C. Routledge.

of transparency and legality (cf. transparency; legality)[105].

Freedoms & Protest

The European Charter for Fundamental Rights addresses a range of freedoms[106]. The most relevant for the CM context are the **freedom of thought**, **conscience and religion** (Article 10), which means that it is possible to "change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance"[107]. Second is the **freedom of expression and information** (Article 11), which states that everyone can hold and express their opinion and has the right "to receive and impart information and ideas without interference by public authority"[108]. A third important article is the **freedom of assembly and of association**[109], which includes the freedom to form peaceful associations. According to the "Hyogo Framework for action 2005-2015", in order to foster positive societal impact, the media should be engaged in stimulating a culture and climate of resilience and community engagement[110]. This includes allowing for protest, and people having the freedom to voice their opinion. In general, protecting societal values like freedom can make the population more resilient against shocks.

Illustration: The so-called "chilling effect"[111] *(that people change their behaviour because of the awareness of surveillance measures) be a negative consequence of a lack of freedom and the right to protest, because the surveillance happens covertly and thus does not allow for protest. Data collection can also positively influence the right to freedom and protest, e.g. by allowing participants in focus groups or*

105 http://www.oxforddictionaries.com/definition/english/legality

106 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf retrieved November 20, 2015.

107 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

108 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

109 Official Journal of the European Communities (2000), Charter of Fundamental Rights of the European Union C 364/1, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

110 UNISDR (2014), A catalyst for change: How the Hyogo Framework for Action has promoted disaster risk reduction in South East Europe, http://www.unisdr.org/we/inform/publications/39269

111 Cohn, C. (2014), NSA Surveillance Chilling Effects: HRW and ACLU Gather More Evidence. The Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2014/07/nsa-surveillance-chilling-effects

interviews to speak their mind about something that they care about relating to CM, to someone that actually has the possibility of making it better.