Driving Innovation in Crisis management for European Resilience

D21.21 – State of the Art and Objectives for the DRIVER test-bed

Grant agreement number:	**607798**	**Due date of deliverable: 31 December 2014**
Start date of the project:	**2014-05-01**	**Actual submission date: 30 April 2015**
Duration:	**54 months**	

Lead Beneficiary: Fraunhofer INT

Contributing beneficiaries: FOI, TSC, TNO, Pole, THG, THW, MSB, ITTI, JRC

Keywords:
State of the Art, CD&E, Innovation Management, Capability development, Methods and Infrastructure, innovation eco-system, stakeholder dialogue, objectives

Dissemination level:	
PU	☒
PP	☐
RE	☐
CO	☐

Release History

Release Number	Description	Release date	Released by
0.1	Draft for review	09 December 2014	Fraunhofer INT
0.2	Draft for review	18 January 2014	Fraunhofer INT
0.3	Final draft	25 April 2014	Fraunhofer INT
1.0	Final version	30 April 2015	Fraunhofer INT

Table of content

Table of figures

List of Acronyms

Abbreviation / acronym	Description
ACRIMAS	Aftermath Crisis Management System-of-Systems
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CD&E	Concept Development & Experimentation
CDS	Capability Development Support Group
CM	Crisis Management
CPM	Costumer Product Mechanism
DHS	Department of Homeland Security
DRCs	Disaster Recovery Centres
DRIVER	Driving Innovation in Crisis management for European Resilience
DSATs	Disaster Survivor Assistant Teams
ECML	European Crisis Management Laboratory
E-OCVM	European Operational Concept Validation Methodology
eOSOCC	electronic On-Site Operations Coordination Centre
FEMA	US Federal Emergency Management Agency
FRG	First Responder Group
H2020	Horizon 2020
HSARPA	Homeland Security Advanced Research Projects Agency
ICCRTS	International Command and Control Research and Technology Symposium
JEs	Joint Experiments
JRC	Joint Requirements Council
M&S	Modelling & Simulation
MC	Military Committee
MCDC	Multinational Capability Development Campaign
MIP	Multilateral Interoperability Programme
MNE	Multinational Experiment
MoD	Ministries of Defence
MoDs	Ministries of Defence

NATO	North-Atlantic Treaty Organisation
NORDEFCO	Nordic Defence Cooperation
NUSTL	National Urban Security Technology Laboratory
OIC	Office for Interoperability and Compatibility
R&D	Research and Development
S&T	Science and Technology
SE	Specific Experiments
SoS	Systems-of-systems
SP	Sub-project
T&E	Test and evaluation
TRL	Technology Readiness Level
TSL	Transportation Security Laboratory
TTCP	Technical Cooperation Programme
UN	United Nations

Executive Summary

The present document summarises the methodological background for DRIVER Methodology & infrastructure dimension and the State of the Art in crisis management capability building. On this basis it also derives the objectives for sub-project (SP) 2 – the DRIVER test-bed – and for European crisis management innovation management on the whole. It is the first deliverable in a series of deliverables and therefore does not claim to be exhaustive.

The idea for building a test-bed was inspired from the Concept Development & Experimentation (CD&E) methodology that has been identified by the Aftermath Crisis Management System-of-Systems phase I project (ACRIMAS) as being well suited for the purpose of crisis management capability building. CD&E is used in the military domain that has adapted basic scientific methods - controlled experiments to acquire new knowledge – to their needs. DRIVER SP2 is now trying to do the same for crisis management. The goal is to enable structured and efficient capability development processes acknowledging the complex realities of crisis management operations and requirements formulation. To this end this document describes the CD&E method and how it can contribute to (i) selecting promising crisis management solutions as well as preventing misguided Research & Development (R&D) efforts, and (ii) building a crisis management knowledge base at System-of-systems level.

Further, D21.21 describes the relevant State of the Art for SP2 including current European and US capability building mechanisms. Important to notice in this regard will be that while the American mechanism already exhibit a high level of maturity, European innovation mechanisms in crisis management (and security on the whole) still lack important features for efficient capability building. However, some methods have been developed by past and ongoing research projects and in other domains; these are also described in the present document.

In addition, the history and approach of DRIVER – with a focus on the Methodology & infrastructure dimension – are described in order to explain where we stand today. Based on this, D21.21 derives the objectives of the DRIVER test-bed for the project and beyond. In post-project sustainability it is envisaged to be able to provide test-bed services to the European crisis management innovation community to support evidence-based capability development.

Finally, we describe the vision of a better functioning crisis management innovation eco-system, i.e. a system where the different actors engage in a structured debate on requirements and where capability development is supported by methods and infrastructure for building and maintaining the necessary knowledge basis.

1 Introduction

The DRIVER Sub-project 2 (SP2) "test-bed" represents the Methodology & Infrastructure dimension of DRIVER. As described in the update of the DRIVER concept in D13.2 (Milestone 1 Report), the Methodology and infrastructure is one the three DRIVER dimensions, the other ones being the Solutions dimension and User community building.

The Solutions dimension aims at providing novel solutions that can provide certain crisis management functions, the User dimension at enabling the European crisis management practitioner community to conduct structured exchange about innovation and to formulate requirements that solutions should met. The Methodology & infrastructure dimension (the DRIVER test-bed), however, aims at developing methods & physical infrastructure that supports the process of selection and refinement of solutions based on operational requirements and at improving the knowledge base of System-of-systems level crisis management.

In post-project sustainability, this dimension is envisaged to develop into a distributed European test-bed that enables crisis management capability development by helping demand and supply side to jointly and iteratively formulate requirements, select promising solutions and develop strategic agendas for capability development for various crisis management functions. Associated test-bed services thereby include the ability to perform large scale experimentation as planned for DRIVER SP6 (Joint experiments), but also methods for structured dialogue, table top exercised and other less expensive test-bed services that enable a structured capability development process and dialogue between end-users and solutions providers.

DRIVER SP2 cooperates closely with all other areas of the project, first and foremost with SP3456 that carry out experimentation using the physical infrastructure and methods that SP2 develops and provides. D13.2 gives an overview about the experimental activities that are planned for the next phase of the project. Also, the "Experimentation Coordination Group" has been installed to facilitate joint planning. In relation to DRIVER SP7 special attention is giving to a shared goal of both SPs (and the entire project), being the sustainability of the test-bed. SP8 and SP9 add to the SP2 methods by providing further criteria for the assessment of novel solutions, namely organisational, policy, legal and societal/ethical criteria, respectively.

SP2 has been structured as illustrated in figure 1.

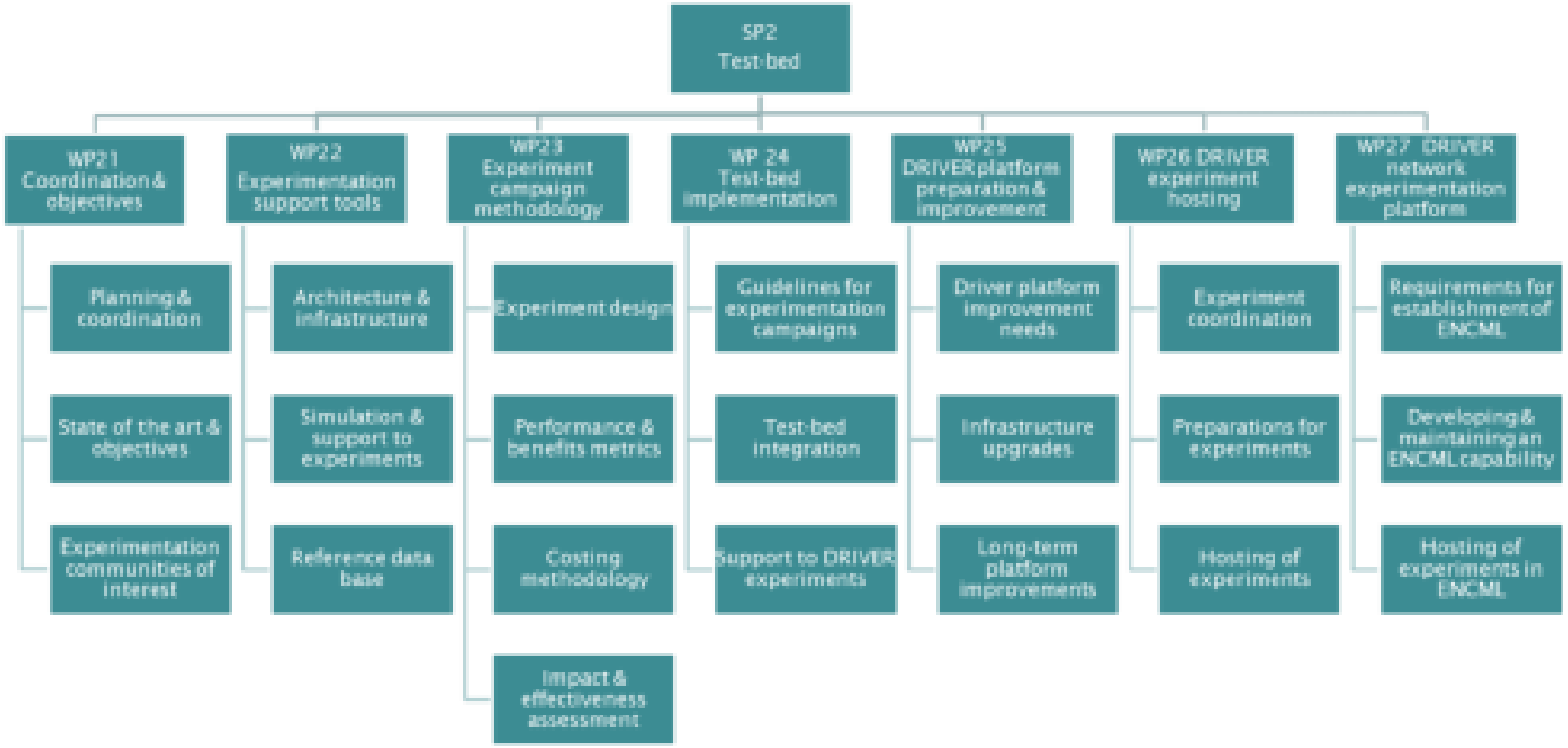

Figure 1: Structure of DRIVER Sub-project

A detailed description of the content of each workpackage can be found in chapter 3.1.

1.1 Structure of the document

The present document aims at describing the current State of the Art in European crisis management innovation management and capability building and at deriving the objectives for the work in SP2 following from this. Also, the document wants to provide an outlook to the longer-term goal of an improved European crisis management capability development mechanism that can – in large parts – also be a model for other Security areas.

To this end, the structure of the document is as follows:

- **State of the Art in crisis management innovation management and capability building**
- **Objectives of the Methodology & infrastructure (test-bed) dimension**
- **Long-term objectives of the DRIVER test-bed in combination with the Solutions and User dimension: Agenda for improving the European crisis management capability development**

2 State of the Art in Crisis management Capability building

2.1 Methodological Background of the test-bed idea

The history of ideas that contributed to the development of the DRIVER test-bed idea contains many different aspects. Among those "General Systems Thinking Theory"[1]**, different discussions on Complexity**[2]**, and definitions of Systems and Systems-of-systems (SoS)**[3] **should be mentioned, but are not discussed in detail in the present document.**

Most relevant and inspirational, however, for developing the methodology for the DRIVER test-bed has been the Concept Development & Experimentation (CD&E) methodology as developed and applied in the military domain. Important to mention in this regard is that DRIVER seeks to adapt the CD&E-way of understanding the problem space of innovation in operational systems as well as the related methodology without trying to impose any military thinking on civil crisis management. In fact, the "E" in CD&E is just an **adaptation of basic scientific practice (controlled experimentation) that has been shaped for military needs. DRIVER now seeks to do the same for the crisis management domain.**

2.1.1 Concept Development & Experimentation (CD&E)[4]

Research activities and capability development in the defence world are embedded into a complex innovation process that is characterised by engagement of multiple stakeholders and different, but well defined stakeholder combinations and interactions at different stages. The present chapter deals with one of the many methods that are being used within this system to support identification of innovation potential and cost-effective capability development in the Research and Development (R&D) phase: Concept Development & Experimentation (CD&E). CD&E is one of the key methodological approaches that the

[1] E.g. Mingers & White (2010) A review of the recent contribution of systems thinking to operational research and management science. European Journal of Operational Research 207 1147–1161;
Thomé, Bernhard (1993). Systems Engineering: Principles and Practice of Computer-based Systems Engineering; Chichester: John Wiley & Sons. ISBN 0-471-93552-2; INCOSE. "What is Systems Engineering". Retrieved 2006-11-26.

[2] E.g. Lowe & Chen (2008): System of Systems Complexity: Modelling and Simulation Issues. SCSC '08 Proceedings of the 2008 Summer Computer Simulation Conference, Article No. 36.

[3] E.g. Lowe & Chen (2008): System of Systems Complexity: Modelling and Simulation Issues. SCSC '08 Proceedings of the 2008 Summer Computer Simulation Conference, Article No. 36.; *Meeting the challenge: the European Security Research Agenda.* A report from the European Security Research Advisory Board (ESRAB), Luxembourg: Office for Official Publications of the European Communities, September 2006 (http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf accessed 11 February 2015) last accessed 25 April 2015.

[4] Mostly taken from: S. Schäfer (2006) Concept Development & Experimentation – eine Einführung. Zentrum für Weiterentwicklung der Luftwaffe, Luftwaffenamt (Ed.).

DRIVER test-bed is based on. It is suitable for assessing the added value of new research results at a systems or SoS level.

Why is CD&E – a methodology so far clearly bound to military capability development - relevant for DRIVER and the DRIVER test-bed? Looking at the characteristics of the operational EU crisis management SoS (cf. also chapter 2.3), it is obvious that selection of new operational concepts (from now on referred to as solutions) for further, often expensive R&D and later inclusion into the operational process - no matter whether of technological, organisational, or any other nature - is far from trivial. Potential operational scenarios are manifold and so are requirements. EU crisis management interoperability requirements range from inter-organisational cooperation across federal states or provinces within one country, via EU cross-border cooperation, to joint EU-operation under UN flag. Obviously, it cannot be afforded to develop individual solutions for any possible incident, but solutions have to be modular. Consequently, when investing into research and development or procurement of novel crisis management solutions, the (lack of) innovation potential of a given concept (i.e. its operational value added across different incidents) is critical for any investment decision, but extremely difficult to assess. In order to define the innovation potential, one has to define functional operational requirements, and to assess novel concepts at a system and SoS level taking different incidents and cooperation modes into account. As described below, the CD&E method is the appropriate approach for exactly these kinds of problems (that often also occur in innovation management in the defence sector) and provides the means for an early "proof of added value" of a novel concept, instead just a "proof of concept", as a typical EU Research Framework Programme demonstration does when conducting a demonstration activity (cf. also section 2.2.1).

DRIVER and the test-bed development in particular will benefit from having a close look at the long-standing experience in the military domain and from involving defence-related CD&E experts into the development of the test-bed (cf. chapter 3.4).

2.1.1.1 CD&E for military capability development

Concept Development & Experimentation (CD&E) was first applied in a defence environment when the political situation after the Cold War changed and new tasks and roles had to be fulfilled by NATO armed forces. Also the rise of information technology led to a situation where defence R&D was no longer the driving force for technological progress. Military capability planning started to be heavily dependent on civil markets and appropriate strategies for formulating requirements as well as on selecting, adapting and integrating technological solutions. Classical evolution of existing platforms ("faster, higher, further") was no longer sufficient, since requirements changed fundamentally (there is no way to develop cars by just breeding faster horses). The answer to these changes within the capability building mechanism of the armed forces was the so called "transformation

process". Transformation here means mainly "disruptive innovations", i.e. innovations that **can help to meet the new challenges as described above.**

The behaviour of big organisations or organisational structures can be described as the interplay of factors that form four main dimensions: people, technology, organisation, and processes. The main feature of disruptive innovations is that they simultaneously cause changes in two or more of these dimensions; the implementation of a new software tool, for instance, requires training of personnel, harmonization of workflows and adaption of organisational aspects[5]. Simultaneous changes in different dimensions often lead to issues with multiple influencing factors (incl. human factors that are difficult to predict) and their interactions. Resulting complexity does not permit the R&D that tries to address an appropriate solution to be defined on a merely theoretical basis. Also, the real dimension of the problem often only materializes on the basis of a constant dialogue between user and solutions developer (i.e. demand and supply side). Prototypical solutions (as e.g. in "rapid **p**rototyping" in the software development domain that **has methodological similarities with CD&E) are often helpful to approach these problem spaces.**

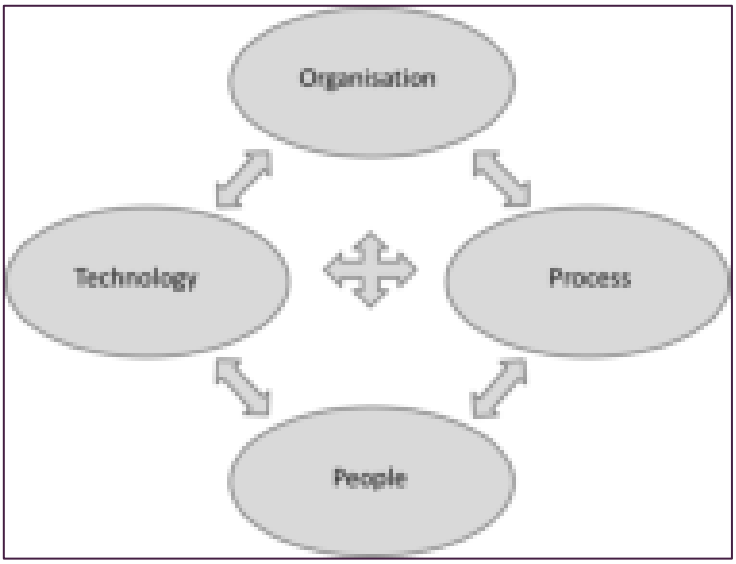

Figure 2: Dimensions of organisations relevant for introducing new concepts

Beside these theoretical considerations of introducing novel solutions into big organisations, costs and time pressure also have an influence on change and the transformation processes of publicly financed organisations like armed forces. The fundamental goal is to react quickly to new requirements while at the same time – also for political reasons - avoiding long-term financial constraints without visible impacts. Consequently, unless a "proof of concept" **includes the practical implementation and the "proof of added value**" in real life operations**, it cannot be regarded as real innovation. The CD&E approach in this regard serves as a**

[5] Often referred to as „Mission Capability Packages" (MCP) that requires harmonised procedures for changes in **different dimensions in order to improve overall performance.**

mechanism that enables early detection of innovation potential and helps to avoid undetected and lengthy misguided R&D endeavours on unsuitable solutions.

In turn, CD&E is also a methodology to systematically improve the performance of complex management and operations systems by comprehensively testing & validating potentially new system components using other techniques like e.g. Modelling & Simulation (M&S).

Through enhanced knowledge about problem areas and capability characteristics, combined with analysis of alternative potential solutions to the capability challenges, quality is created in the preparation phase for development and implementation decisions. The CD&E framework is built on interactive development, continuous validation of results and continuous collaboration with stakeholders. New solutions and ideas (concepts) are iteratively tested (multiple scenarios, interoperability questions etc.) by a series of controlled experiments addressing different research questions. Results of experimentation are then used to further develop the concept, which is again followed by an experimentation phase, until operational capability is reached. Concepts can also be rejected, if it turns out that they do not provide added value or are not cost-efficient.

In sum, CD&E is characterised by

- Careful and systematic identification and description of capability gaps;
- Systematic analysis of solutions (i.e. new ideas, research results) that might have the potential to fill these gaps (at system or SoS level);
- Evidence-based rejection of most and uptake of some solutions for further R&D;
- Participation of stakeholders that are carefully selected and combined in order to exploit expertise and accumulate knowledge;
- Well-structured communication and information exchange between relevant players.

A significant amount of literature is available on defence-related CD&E processes stemming from the NATO transformation process which is, in fact, driven by CD&E. CD&E is further applied at national level (as part of NATO activities or for tackling national capability development questions) as well as in multinational contexts other than NATO, such as The Technical Cooperation Program (TTCP)[6] or the Multilateral Interoperability Programme (MIP)[7] (cf. box below and Annex I). There are a few open forums for discussion of CD&E, both as a concept and as a practice. One example is the International Command and Control Research and Technology Symposium (ICCRTS)[8] series of symposia, now in its 20th year, and other activities sponsored by the Command and Control Research Program (CCRP), directed by Office of the Assistant Secretary of Defence (NII). Results from some small-scale

[6] The Technical Cooperation Program: http://www.acq.osd.mil/ttcp/ last accessed 25 April 2015
[7] Website: https://mipsite.lsec.dnd.ca/Pages/Default.aspx last accessed 25 April 2015
[8] Website: http://www.dodccrp.org/html4/events_symposium_home.html last accessed 25 April 2015

experiments can be found in this literature, although mostly involving concepts of low maturity. There is, for obvious reasons, no unclassified literature available dealing in detail with the conduct and results of specific experiments. Therefore, the present document presents abstract methodological aspect. Further relevant information has to be gathered via expert interviews that have been conducted during the first phase of the DRIVER project, but that will also be conducted focussing on more advanced questions as the project develops.

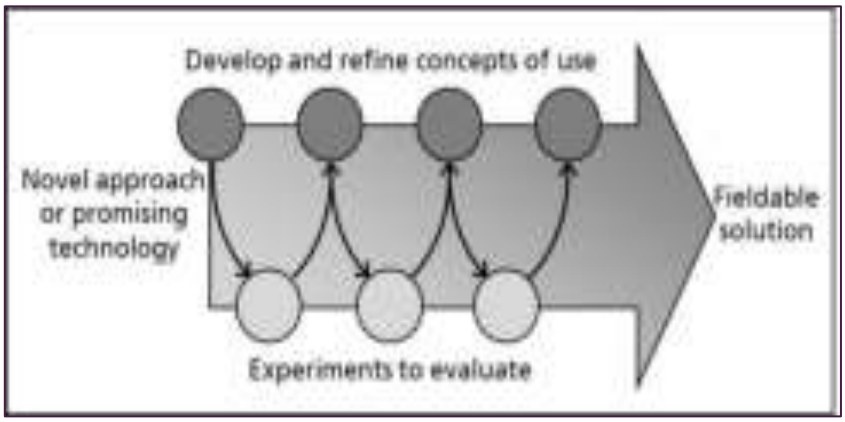

Figure 3: Schematic representation of the DC&E approach

2.1.1.2 Modelling & Simulation in CD&E[9]

Modelling & Simulation (M&S) is usually understood as the development of abstract dynamic models of reality that enable simulation of certain aspects and – through experimenting on the model – facilitate the accumulation of new knowledge. M&S as well as e.g. Operations Research are traditionally important methods to support exercises or to analyse strategies or weapon systems. Classical examples are M&S applications for combat simulation, operations planning, decision support or planning of resources. Recently, increasing availability of computing power and high degrees of interconnectedness facilitate the analysis of a very large variety of possible scenarios. Also, it is possible to model complex systems with a variety of actors and also cognitive and social processes (e.g. leadership).

In order to institutionalise a CD&E process, a flexible and adaptable M&S-based testing environment is required. We will call such an environment a *test bed*. The main benefits provided by this type of test bed are:

- Cost-efficiency of experiments in terms of re-using respective infrastructure;
- Cost-efficiency in terms of personnel when it comes to operations simulations;
- The use of models triggers logical thinking and quantification;
- "background noise" can be eliminated, i.e. lab conditions can be created;
- System-behaviour can be included without re-building the system;

[9] S. Schäfer (2006) Concept Development & Experimentation – Eine Einführung. Zentrum für Weiterentwicklung der Luftwaffe, Luftwaffenamt (Ed.).

- Repeatability and targeted variation of specific conditions can be achieved, especially for statistical analysis of random processes;
- Validation and extension of real experiments;
- Quick iteration of analysis and synthesis (i.e. understanding of component behaviour and the behaviour of the entire system).

Generally, one can distinguish solely model-based (i.e. fully virtual) experimentation and experimentation that includes real life activities, e.g. involving tactical decision making. During simulation-based experimentation, M&S mainly serves as supporting function. For experimentation on high-level decision making solutions, for instance, operational consequences of real life (i.e. simulated) decision making can be virtually modelled in order to compare different tools without having to play through different real-life experiments. Depending on the experiment, different ways of combining modelling and simulation are to be used in a most cost-effective way.

In order to interpret the outcome of an experiment, long standing theoretical and practical experience is necessary, since results always have to be interpreted, taking into account a variety of factors in order to draw the right conclusions. It must be stressed that negative outcomes, i.e. where the system under study does not perform as expected often provides more information than the opposite case. Even inconclusive results may point to new aspects that must be studied in more detail.

2.1.1.3 CD&E in DRIVER

The design of the DRIVER project – dedicated demonstration strands in sub-projects (SP) 345 clustering a range of solutions from specific areas (civil resilience, professional response, learning & training) that are being experimented on using a structured scientific methodology and necessary infrastructure to do so - is based on the CD&E approach as defined above. As described, it is based on fundamental scientific methods that have been adapted by the military domain where it has been developed to understand the effects of newly introduced operational concepts onto the complex operational system.

The theoretical problem space for introducing new solutions (or in other words, for capability development) in crisis management very much resembles the one in the military domain. In order to understand if a new concept (i.e. a technological, conceptual or organisational solution) provides an added value to crisis management operations, its effect on people, other technologies and organisation & procedures, i.e. its effect on the EU crisis management SoS in its different modular configurations has to be assessed. One could argue, however, that crisis management and the analysis of the effects of new solutions onto crisis management operations is even more complex, since – in contrast to the military domain – we are talking about a wide range of heterogeneous first responder organisations being only loosely coupled and deployed in varying configurations in their national and the

EU- and international crisis management SoSs. Also, national systems differ considerably at olitical and organisational level across different nations.

Further, the individual interpretation of CD&E in the different DRIVER sub-projects will be quite divers. While initial concept development for SP4 was already finished before the start of the project (through the work in the ACRIMAS and CRISYS project, see below), SP3 and SP5 are globally less mature and still need time in the first phase of DRIVER to come up with concepts to be included into the CD&E spiral. Also, experimentation will be interpreted differently depending on the SP (i.e. the scientific area to be addressed) and depending on the phase of the project. Therefore, DRIVER defines an experiment not only as a physically played through controlled crisis management situation testing new equipment, but also as well prepared workshops, table to exercises and other means that enable data gathering, learning and refinement of concepts.

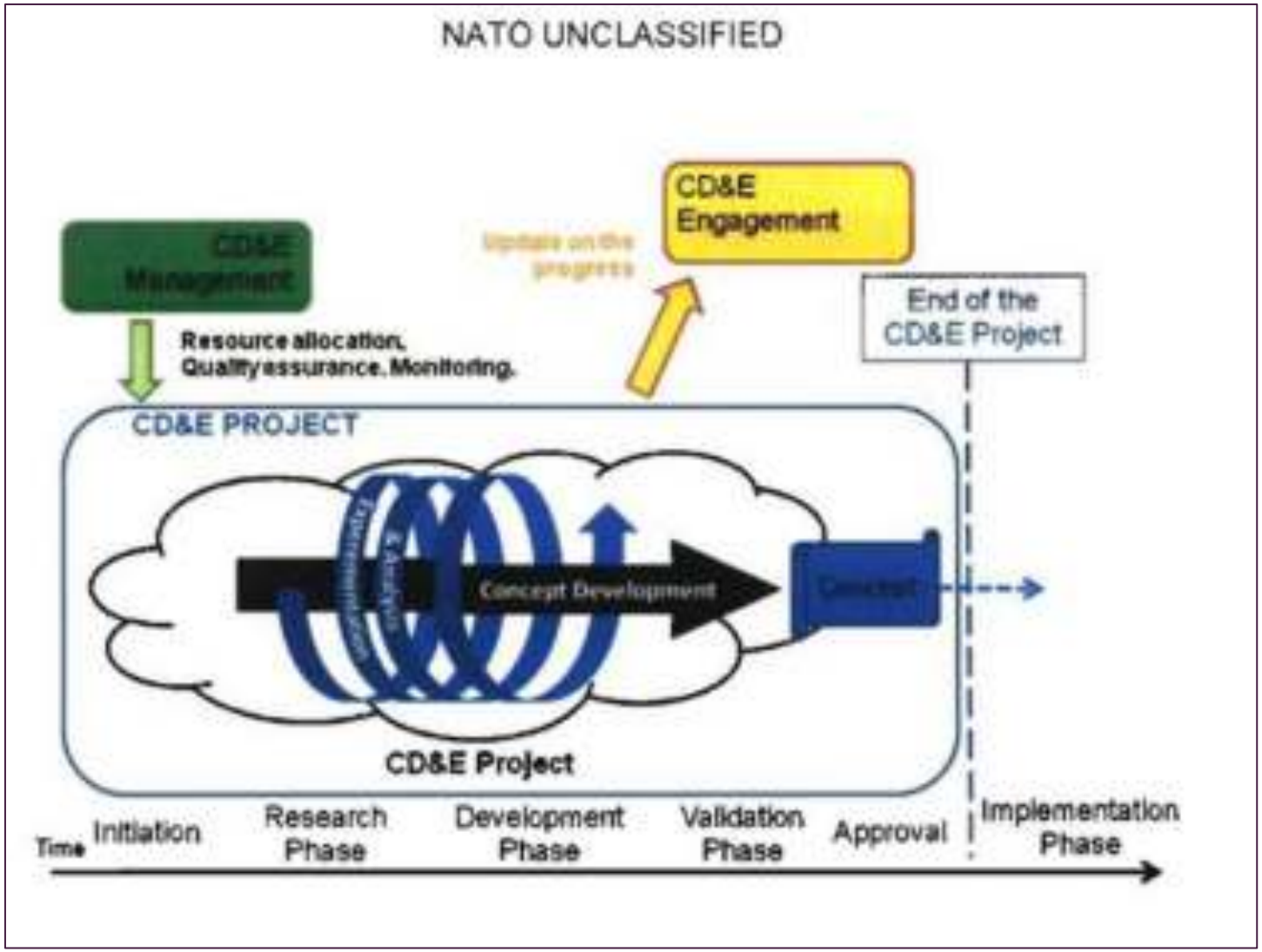

Figure 4: NATO CD&E process[13]

Description North-Atlantic Treaty Organisation (NATO) CD&E approach, Multinational Capability Development Campaign (MCDC), and The Technical Cooperation Programme (TTCP)[10]

In many multinational defence-cooperation-organisations like NATO and different sub-groups CD&E searches for solutions to capability shortfalls that were previously identified and contributes to capability development resulting from new ideas of any kind (i.e concepts). The NATO transformation processes are driven by the ability for CD&E and the subsequent implementation of new solutions.

The Policy MC-0583[11] **for NATO CD&E was approved in September 2009 by the NATO Military Committee (MC) and the incorporation of the CD&E process within the current NATO processes became one of the most important tasks for the NATO Military Committee (MC). The po**licy aims to set out the role of CD&E in support of the Alliance's transformation **goals, to clarify responsibilities between various actors and to provide a robust basis for defining a detailed CD&E process within NATO. In July 2010 the policy on crisis management MC-0056**[12] **was approved. It describes how a CD&E process should develop.**

The first phase is the Concept Development, which presents the rationale for the Experimentation: Firstly, shortfalls/vulnerabilities are identified and suggestions for addressing the shortfalls/vulnerabilities are analysed, described and evaluated. The second phase is the Experimentation, which aims to determine whether the concept under development, i.e. the provided suggestions, will achieve its desired purposes. The experimentation (series of experiments) not only analyses the concept with regard to its potential to address the shortfalls, but also enables an iterative refinement of the concept.

CD&E is an iterative method with spiral development, where concept and validation are steadily in interaction and involve stakeholder working collaboratively for the project development and continuous assessment of results achieved.

Multinational coalition of the CD&E capabilities is one of the objectives of the Multinational Capability Development Campaign (MCDC)[13] **concept which can therefore be understood as (at least partly) a good model for the DRIVER project. This is a multinational concept development and experimentation initiative led by the United States**[14]**. The theme of MCDC 2013-2014 for example is Combined Operational Access**[15]**.**

MCDC 2013-2014 follows the efforts of the previous Multinational Experiment (MNE)

[10] Further multinational cooperation programmes applying the CD&E method include the Nordic Defence Cooperation (NORDEFCO: http://www.nordefco.org/default.aspx) last accessed 25 April 2015

[11] Military decision on MC-0583, 2009: Military Committee for NATO Concept Development & Experimentation. North Atlantic Military Committee. NATO: http://www.act.nato.int/images/stories/events/2011/cde/rr_mc0583.pdf last accessed 25 April 2015

[12] Military decision on MC-0056 (2010): "NATO Concept Development & Experimentation (CD&E) process. Secretary General, NATO: http://www.act.nato.int/images/stories/events/2011/cde/rr_mcm0056.pdf last accessed 25 April 2015

[13] Contributing nations are : Austria, Canada, Czech Republic, Denmark, European Union, Finland, France, Germany, Great Britain, Hungary, Italy, NATO, Netherlands, Norway, Poland, Republic of Korea, Spain, Sweden, Switzerland Turkey, United States.

[14] Cf. https://wss.apan.org/s/MCDCpub/default.aspx last accessed 25 April 2015

[15] For individual projects refer to https://wss.apan.org/s/MCDCpub/Site%20Assets/1.MCDC_COA_Information_Sheet%281May14%29.pdf last accessed 25 April 2015

campaign series initiated in 2001 and has conducted seven campaigns. The first action (MNE1) began with four participants and the last one (MNE7) included 17 participating nations. The first significant attempt in the Multinational Experimentation series to expand the scope and actors involved in coalition operation was in MNE4 (2006) with nine participants. MNE5 (2007) expanded to 12 participants and seven observer including 18 nations. The primary goal of MNE5 was to develop capabilities for effective, day-to-day involvement across agencies, nations, organisations in order to support crisis planning and action. The results of MNE5 contributed to changes in the Operational Planning Process, the Strategic Planning Guide and Cooperative Implement Planning. It developed processes to facilitate multinational information sharing and knowledge management.

The MCDC series is composed of consecutive campaigns each addressing a specific problem set through the use of CD&E and other methods.

The Technical Cooperation Programme (TTCP)[16] focusses on shared defence R&D need between the contributing nations. It covers basic research, but also advanced, i.e. high Technology Readiness Level (TRL), technology development including the joint use of the CD&E approach. The programme is structured into 11 groups that each covers a specific technology or system area[17]. The area of special relevance for DRIVER is Joint System and Analysis (JSA) that focusses on the needs that derive from multinational cooperation. JSA contains of further sub-areas, e.g. Modelling & Simulation, Effects Based Analysis of Systems, Concept Development & Experimentation Sciences, and Complex Adaptive Systems.

2.2 Capability building in civil security and crisis management – state of play

Security including the area of crisis management is still an embryonic field in terms of structured industrial research. Security was only established as a dedicated research area after 9/11[18] - first by the US as a reaction towards the attacks, later by the EU, mostly to compensate industry for a shrinking defence research budget, and as a response to the Madrid and London bombings in 2004 and 2005, respectively. Crisis management followed for similar reasons, since man-made disasters, specifically CBRNE terrorism, and severe natural hazards and threats, such as the effects of climate change, with e.g. extreme weather events, have been becoming more obvious and their occurrence more frequent.

Despite increased attention and awareness, however, research efforts in security and crisis management so far have been rather random and no real innovation ecosystem in crisis management (cf. chapter 3.3) or capability building mechanism – at least within Europe - have emerged[19]. More specifically, the assessments of capability gaps does not follow a structured approach, nor are technical requirements at system- and SoS-level sufficiently described to facilitate and guide a validation & assessment process for new solutions that are coming out of less mature research.

[16] Contributing nations are: Australia, Canada, New Zealand, United Kingdom, United States.
[17] For more details see http://www.acq.osd.mil/ttcp/overview/ last accessed 25 April 2015
[18] Note that, although there has been academic research on Security issues as well as industrial research on security ICT applications or on early detection of natural disasters, these activities have been scattered across the research landscape and have not been bundled to a specific application area before the year 2001.
[19] For the US crisis management system cf. section 2.2.4.

So far, only a few structured approaches dealing with capability development in security in general and crisis management in particular can be identified at a global scale. The most prominent ones are described below. They form an important starting point for what should be developed during the DRIVER project and beyond.

2.2.1 Capability development approach via the EU 7th Framework Programme- or Horizon 2020-Innovation-Model

Horizon 2020 (H2020) - as former European Research Framework Programmes that have been designed for applied research - uses different instruments to acknowledge research needs in different parts of the innovation chain, thereby roughly following a System-of-Systems (SoS) approach with different complexity levels.

.

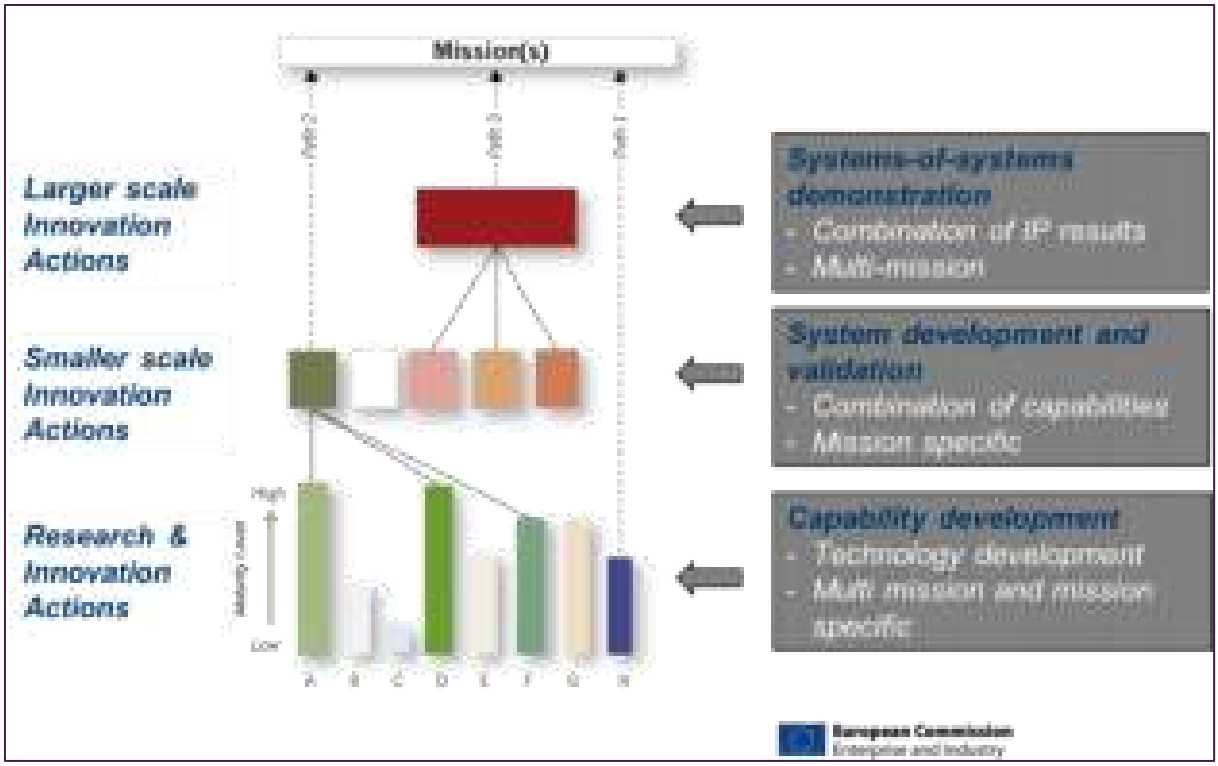

Figure 5: Project "hierarchy" in FP7 security theme

Research & Innovation Actions thereby reflect component level research, the lowest complexity level in a SoS that needs to be further integrated into Sub-Systems, Systems and finally, a SoS. The next complexity level is represented by smaller scale Innovation Actions; these projects typically integrate different components from earlier research into integrated sub-systems or systems. Finally, larger scale Innovation Actions (demonstration activities – here mostly understood a mere "proof of concept" and less as research effort that defines the added value and refines solutions, see below) represent the highest complexity level in

European Framework Programme research. They act at SoS level, (loosely) integrating sub-systems and systems.

Typically, large-demonstrations in the Framework Programme are divided into two parts:

1. The phase I, preparing the ground for the actual demonstration by identifying mature research, i.e. research at high TLR that is ready to be integrated at systems-level, by developing an appropriate demonstration concept acknowledging the systems-characteristics of the area in question, and by widely disseminating the existence of the programme as well as its results.
2. The phase II, the actual demonstration phase that should embrace the SoS view as well as the innovation characteristic of the area in question[20].

2.2.1.1 Definition of capability gaps and translation into research needs in security research in the EU Framework Programme

Theoretically, EU Member States (MS) are tasked (via the Programme Committee responsible for the definition of topics in the Secure Societies Work Programme) to bring in the national end-user perspective with regard to capability requirements for all mission areas in security research. The EU Commission should then formulate (supported by the Security Advisory Group) the topics for the work programme in a way that the requirements are reflected in research needs. However, in practice some call topics are brought in by the Programme Committee, some by the Security Advisory Group, some through other channels. Also, capability gaps identified by past research projects on an analytical basis are seldom taken up into the work programme (this is even true for demonstration phase 1 projects that only rudimentary inform the design of the later phase 2 project, if at all) or are followed up upon with higher maturity research activities in later work programmes. A systematic identification, definition and artculation of capability gaps and a translation of these into solutions that could potentially fill these gaps is absent.

2.2.1.2 Assessment of the added value of novel research results (solutions) and understanding of "demonstration"

Since innovation is mainly achieved by favouring good ideas over bad ideas, research results are normally assessed before one invests into further R&D for a specific idea or tool. Consequently, many Research & Innovation Actions and most Innovation Actions in security research somehow include a demonstration activity in the sense of a "proof of concept". However, an obligatory requirement for a systematic "proof of added value" in a SoS-context acknowledging its different technological and non-technological (people, organisations, coordination, procedures, cultures, societal values etc.) sub-systems is absent

[20] Cf. also related discussion in DRIVER D13.2.

in the European Security Research Programmes so far. Moreover, the results of earlier research projects do not inform the formulation of later calls for research project, so that a systematic selection of concepts exhibiting high innovation potential is not being performed. As a consequence it is also not possible to assess progress that has been made on requirement needs that have been identified earlier. However, instead of investmenting into systematic assessments of research results, security research consortia are tasked to invest up to 10% of their funding in dissemination activities. The latter leads to the impression that it is assumed that advertisement instead of systematic assessment would foster innovation in security. However, this assumption rather fits the characteristics and innovation requirements of a consumer market, not those of the security market with its very special characteristics (cf. also section 3.3).

In sum, the Secure Societies capability development approach lacks

- **An analytical, structured, and across Europe harmonised process of the identification and definition of capability gaps with systematic end-user and other stakeholder involvement including end-users being enabled to articulate their operational** requirements and having them "translated" to research requirements;
- **A systematic approach to assess the innovation potential of novel solutions and an analytical basis for work programme design and research instruments (e.g. PCP, PPI) applied;**
- **Fora for balanced stakeholder discussions that would enable iterative refinement of research results until deployment is possible.**

2.2.2 The EU Joint Research Centre's in Ispra crisis laboratory approach[21]

The EU Joint Research Centre (JRC) in Ispra runs the European Crisis management Laboratory (ECML) that serves as a research, development, testing and validation facility for Information Communication Technology (ICT) focused solutions, integrating devices, applications, and crisis management related information sources to support crisis management needs including threats analysis, common situational awareness, early warning, response and collaborative decision making. The ECML supports testing in a range of crisis scenarios, from intentional threats and natural disasters to health crises. The use of visual analytics for improving information readability, visualisation and effectiveness, particularly in large video screen environments, form an integral part of the Laboratory's ICT R&D and testing **programme.**

Available capabilities at ECML are:

- **Benchmarking of ICT tools and devices;**
- **ICT technology validation;**
- **Testing in-house systems and tools;**
- **Threat Analysis, Situational Awareness, Early Warning;**
- **Command and Control;**
- **Training.**

By following a systematic testing approach that includes analytical benchmarking of different ICT tools (or comparing ICT-tools to non-ICT legacy tools or methods) the JRC ECML is the first organisation in Europe that follows a more strategic approach to technology development for crisis management. However, due to size and limited resources to organize large-scale disaster testing at a SoS level (including people, organisations, coordination, procedures, cultures etc. see above) and an area of expertise that is focused around ICT-

[21] European Crisis management Laboratory : (ECML) : http://lunar.jrc.it/critech/Activities/EcrisismanagementLEuropeanCrisisManagementLaboratory/tabid/99/Default.aspx last accessed 25 April 2015

tools only, the experimental approach and knowledge base at a systemic level is still in its development phase (but will be developed as part of the DRIVER project).

The JRC ECML is partner in DRIVER and provides its laboratory as a platform. This will enable its expertise to be fully integrated into the endeavour of creating a distributed platform for large scale experimentation. JRC was also partner in the preparatory study that laid the foundation for the DRIVER approach – the FP7 demonstration phase I project Aftermath Crisis Management System-of-systems (ACRIMAS[22]). As part of the project the so called ACRIMAS pilot case[23] has been performed.

The ACRIMAS pilot case on Crisis management experimentation: Interoperability of Mobile Devices for Crisis management

The workshop's (pilot case's) purpose was to measure the added value of mobile assessment technology for rapid situation assessment in international emergency operations. Seven mobile assessment systems were deployed among the participants and needed to provide, in an interoperable way, real-time data to a single electronic On-Site Operations Coordination Centre (eOSOCC). The performance of the systems was benchmarked against a traditional paper-based assessment that was conducted simultaneously (pOSOCC).

The field experiment took place on the JRC site in Ispra. 42 Markers were placed over an area of approximately 550000 m2. The clearly visible markers only contained a numerical ID and a verbal description of the situation encountered on the placed location. The eOSOCC received real-time information from the field teams via the feed URLs provided by the technology providers. All participating systems were able to provide either GeoRSS or KML feeds. All information streams appeared in the eOSOCC on a single map utilizing OpenLayers.

The evaluation of the experiment was done collaboratively by practitioners, field experts, strategic level personnel working with national and international headquarters of civil protection and crisis management, and JRC staff.

The major outcomes of the experiment can be summarized as follows.

- The eOSOCC team leaders reported that there was considerable information overload. As much as 328 entities of information were simultaneously streamed to the eOSOCC. Therefore sophisticated editing, filtering, and visualization functionalities have to be available for OSOCC staff in order to produce an electronic situation map; also data had to be confirmed after participant came back to OSOCC.
- The pOSOCC leaders used the A0 map they produced for presentation and they had an overview of the priorities which they marked also with post-it notes.
- Both paper and electronic OSOCC reached similar situation awareness. The final map based briefing material is almost identical with very few exceptions.
- Both OSOCC teams made mistakes with regard to the exact positions. The mistakes of the eOSOCC team made in transferring accurate data to the briefing material underline the need for an OSOCC software suite covering the whole workflow of procedures essential in OSOCC operations.

[22] www.acrimas.eu last accessed 25 April 2015

[23] http://www.acrimas.eu/attachments/category/2/ACRIMAS_pilot%20case_report.pdf last accessed 25 April 2015

- The outcomes showed that both paper and electronic OSOCCs reached similar situation awareness in the same time, identifying similar needs and locations for prioritization, but only the eOSOCC had products available as sharable electronic maps and documents. The pOSOCC would need at least 30 minutes to come to the same result.
- Another advantage of the eOSOCC was the possibility to monitor a situation changing over time and the possibility to keep track of the situation (awareness) evolution.

More general outcomes have been some concrete recommendations by the participating practitioners on how mobile technology can be improved and integrated in humanitarian operations. They considered workshops like this one an essential tool, but it is more important to have a dedicated community that has regular activities or meetings on the topic to keep the momentum of development ongoing. A forum for technology providers to exchange ideas and products would be also useful. The contribution of practitioners to this dedicated community is of great importance because only they can ensure the very vital input for a user and task driven development of proper ICT systems.

Besides physical workshops or exercises, tools like table top exercises and dedicated technical teleconferences are as important. Gradual integration in Standard Operating Procedures and adaptation of training curriculums is a way to integrate mature technology in the existing assessment practices of operational organisations. The more open the architectures and standards of these technologies are, the likelier the integration and adaption process.

The JRC is within DRIVER part of the effort of building a sustainable network of Pan-European research and testing facilities focusing on ICT for crisis management.

2.2.3 US Federal Emergency Management Agency (FEMA) approach: concept development and innovation during operations

After Hurricane Catrina – that was perceived as not being optimally managed by the US Federal Emergency Management Agency (FEMA)[24] – FEMA changed its innovation approach during Superstorm Sandy and deployed so called Field Innovation Teams[25] that would go out and try to come up with all kinds of smart ideas to improve the situation during an ongoing disaster operation.

Recently FEMA also came up with the FEMA Think Tank, which is essentially a crowd sourcing activity where everyone (professional crisis managers but also the general public) can submit novel ideas to improve certain aspects of Crisis management[26].

A recent development is the planned FEMA lab where novel tools are planned to be tested.

Related FEMA activities on innovation include[27]:

[24] http://www.fema.gov last accessed 25 April 2015
[25] http://www.fieldinnovationteam.org last accessed 25 April 2015
[26] https://www.fema.gov/media-library/multimedia/collections/270 last accessed 25 April 2015

- **The Recovery Directorate conducted three field experimentations with Disaster Survivor Assistant Teams (DSATs) to test mobile registration;**
- **Senior Leadership participated in facilitated brainstorming sessions on the redesign of Disaster Recovery Centres (DRCs) so that they are more survivor-centric and community driven;**
- **The Office of External Affairs analysed social media to determine public sentiment during Superstorm Sandy, and implemented the Oklahoma application that survivors could use to find homes and rides;**
- Open FEMA, DHS's Office of Science and Technology, and the University of Virginia's **systems engineering students analysed how to optimize the use of curated data feeds from Open FEMA during a disaster; and**
- the Response Directorate's Office of Chemical, Biological, Radiological, Nuclear and **Explosives (CBRNE) developed a prototype for a Radiological Prep Game and tested the product with FEMA Corps members.**

The FEMA Administrator's Intent (Fiscal Year 2015**-2019)**[28] describes that "FEMA will place a **premium on developing our organisational capacity to encourage new ideas, learn from past experience, rapidly orient and apply that learning in current contexts, and quickly adapt to changing conditions. Through the Think Tank and other innovative efforts at all levels of the organisation, we must expand our efforts to bring together leading entrepreneurs, technologists, academics, stakeholders and subject matter experts from diverse fields to offer fresh perspectives and new approaches that will better allow FEMA and our partner organisations to achieve critical emergency management outcomes. Innovation and learning are the essential tools that allow us to be forward leaning and embrace more effective** processes that will lead to better mission outcomes while still living within our fiscal means." **Also, a Strategic Foresight Initiative has been established.**

However, while FEMA seems to understand that there is a critical need to improve the uptake of innovative tools into disaster management, a systematic approach as described above also seems to be absent. Speaking CD&E, there seems to be a strong focus on concept development (Think Tanks), but not so much on systemic experimentation as discussed in the present document.

Also, it has to be stated that innovation during an ongoing operation (as described for the Sandy event) is risky and can only be limited to small scale solutions (like e.g. the innovative use of social media to better organize shelter). As soon as larger solutions requiring changes in more than one of the four dimensions described in chapter 2.1.1 (like e.g. communication or situational awareness tools) are considered the risks of introducing an untested solution

[27] **Message from Deputy Administrator Serino: Update on FEMA Innovation: https://www.fema.gov/information-employees/message-deputy-administrator-serino-update-fema-innovation last accessed 25 April 2015**

[28] **http://www.fema.gov/media-library-data/20130726-1911-25045-4786/2015_2019_administrator_s_intent_final508.pdf last accessed 25 April 2015**

in an ongoing operation are hardly acceptable and, most likely, also not covered by insurance policies.

2.2.4 Department of Homeland Security (DHS) innovation approach[29,30]

The US Department of Homeland Security (DHS) was founded after the 9/11 attacks to protect the United States and its territories from and responding to terrorist attacks, man-made accidents, and natural disasters. In contrast to EU MS's Ministries of the Interior or comparable government bodies responsible for homeland security, DHS runs, since 2003, its own and dedicated research directorate on Science and Technology (S&T) providing systematic scientific support to security and crisis management practitioners.

Moreover, the DHS systematic approach to security and crisis management (see below) capability development seems to be based on methods and approaches taken from military innovation management.

DHS S&T works with the broader R&D community to identify and adapt existing R&D investments to meet operator needs and challenges in four general areas:

- It creates technological capabilities addressing DHS operational and strategic needs, or capabilities that are necessary to address evolving homeland security threats.
- It conducts systems-based analysis to provide streamlined, resource-saving process improvements and efficiencies to existing operations.
- DHS achieves more effective and efficient operations and avoids costly acquisition failures and delays by leveraging its technical expertise to improve project management, operational analysis and acquisition management.
- Its relationships across DHS and the Homeland Security Enterprise contribute to the strategic understanding of existing and emerging threats and recognition of opportunities for collaboration across departmental, interagency, state and local and international boundaries.

[29] Note that FEMA and DHS only occasionally join forces for capability development.
[30] http://www.dhs.gov/science-and-technology/our-work last accessed 25 April 2015

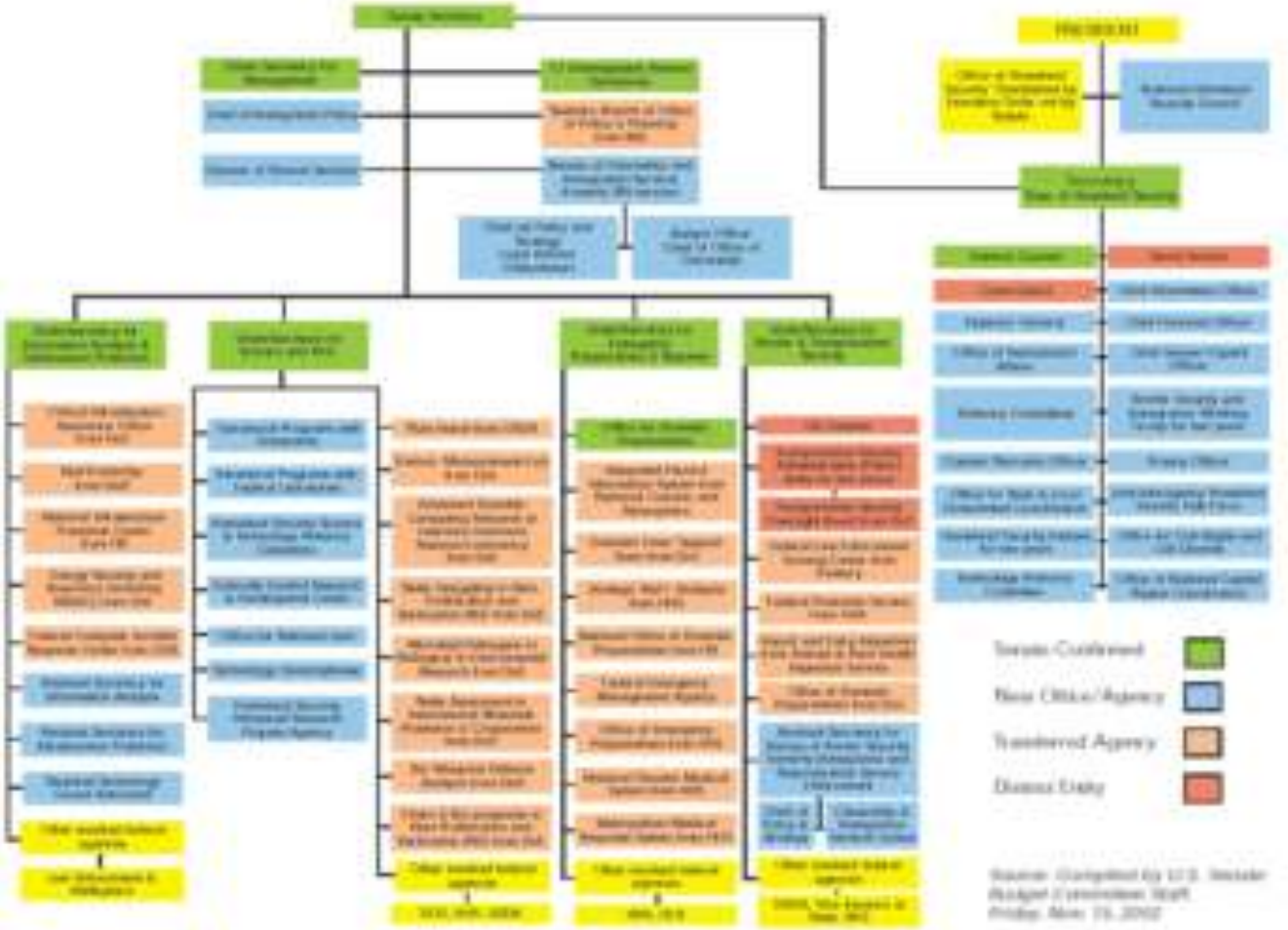

Figure 6: Organisation chart Department of Homeland Security (DHS)

The Homeland Security Advanced Research Projects Agency (HSARPA)[31] uses innovation and modernisation to further scientific advances and produce products that support DHS components such as US Customs and Borders Protection, the US Secret Service, the US Coast Guard, and the Transportation Security Administration, as well as state, local, and private sector entities including first responders and critical infrastructure operators. Selected areas of activity are:

- **Borders and Maritime Security Division;**
- **Chemical and Biological Defense Division;**
- **Cyber Security Division – including a Cyber security test-bed;**
- **Explosives Division;**
- **Resilient Systems Division[32].**

The Capability Development Support Group (CDS) as DHS works closely with the DHS components to ensure programs and systems run smoothly. The Under Secretary for Science and Technology recently realigned CDS' functions to more accurately reflect needed capabilities and respond to DHS component needs for standards, test and evaluation, operations and requirements analysis and systems engineering.

CDS provides an innovative, systems-based approach to help operators define their needs in close cooperation and develop technologies and solutions that can be quickly deployed to frontline operators. CDS' analytic and systems engineering approach assess**es the operational environment and fiscal limitations to ensure the best solutions are chosen. An example of this approach is the Rio Grande Valley Systems Analysis Project[33]. CDS worked closely with US Customs and Border Protection on the south Texas border to help identify system solutions to meet operational challenges. In addition, CDS has worked with US Immigration and Customs Enforcement and the Transportation Security Administration to assist in addressing both process and technological challenges. Currently, CDS is working with US Citizenship and Immigration Services on ways to streamline immigration and citizenship processes.**

CDS' expertise includes systems engineering, operatio**ns analysis, test and evaluations, standards and acquisition. CDS focuses on accuracy and analysis to make smart investment decisions that deliver enhanced capabilities to the Homeland Security Enterprise.**

CDS acts as the principal advisor on operational test and evaluation and oversees test and evaluation for DHS major acquisitions, ensuring homeland security technologies are reliable, interoperable and effective. CDS provides test and evaluation (T&E) oversight for 135 major acquisition programs housed by the DHS components (a $150 billion acquisition enterprise).

[31] http://www.dhs.gov/science-and-technology/hsarpa last accessed 25 April 2015

[32] Might be of interest to the work in DRIVER SP3: http://www.dhs.gov/science-and-technology/resilient-systems-division last accessed 25 April 2015

[33] http://www.dhs.gov/sites/default/files/publications/Research%20and%20Development%20Analysis%20and%20Assessment-Rio%20Grande%20Valley%20Systems%20Analysis.pdf last accessed 25 April 2015

CDS houses the Transportation Security Laboratory (TSL). TSL is a driving force in the T&E area, primarily specialising in evaluating screening and contraband detection technologies.

CDS develops and oversees DHS standards that ensure reliable, interoperable and effective technologies and processes. This includes coordination and representation on a number of standard-setting bodies and organisations.

Established in 2012, CDS' **Operations and Requirements Analysis uses technical and analytic expertise to identify and prioritize cross-DHS capability gaps and find solutions for DHS component operations. The goal is to save money and time while meeting DHS critical missions and to support R&T activties with transitioning technologies to operational use. The Operations and Requirements Analysis also supports the DHS Joint Requirements Council (JRC), a DHS component-led body designed to identify and prioritise cross-department capability gaps and recommend investments to address the gaps. CDS supports the JRC by providing capabilities and requirements analysis to enable DHS leadership to address the gaps, overlaps and duplications at the enterprise-level rather than at the individual component level.**

CDS's **systems engineering promotes a rigorous systems engineering process that transforms customer needs and requirements into operational capabilities.**

2.2.4.1 DHS: crisis management innovation management

The DHS First Responder Group (FRG)[34] is focused on strengthening response capabilities. Its dedicated capability development process that also is very interlinked with the DHS R&T activities described above essentially is based on four pillars[35][36]

- **Test, evaluation and analysis of key capabilities at the National Urban Security Technology Laboratory (NUSTL),**
- **Development of interoperability solutions for first responder communication at the Office for Interoperability and Compatibility (OIC),**
- **Fast track capability development for urgent requirements at the Technology Clearinghouse / R-Tech (TCR), also known as the TechSolutions Program.**
- **Procurement decision support through System Assessment and Validation for Emergency Responders (SAVER) Program[37].**

The National Urban Security Technology Laboratory (NUSTL) located in New York City, is a government-owned, government-operated facility organised under and operated by the Department's Science and Technology Directorate. The laboratory is programmatically aligned to the Science and Technology (S&T) Directorate's Director of Support to the

[34] http://www.dhs.gov/science-and-technology/first-responders last accessed 25 April 2015
[35] http://www.dhs.gov/xlibrary/assets/st_dhs_nustl_strategic_plan.pdf last accessed 25 April 2015
[36] http://www.dhs.gov/st-activities-and-programs last accessed 25 April 2015
[37] http://www.firstresponder.gov/SitePages/Saver/Savers.aspx?s=Saver last accessed 25 April 2015

Homeland Security Enterprise and First Responders, with operational funding through the S&T Office of National Laboratories (ONL).

NUSTL's mission is to test, evaluate, and **analyse homeland security capabilities while serving as a technical authority to first responder, state, and local entities. In fulfilling this mission, the laboratory serves as a federal technical authority promoting the successful development and integration of homeland security technologies into operational end-user environments by objectively:**

- **Conducting test programs, pilots, demonstrations, and other forms of evaluations of homeland security technologies both in the field and in the laboratory;**
- **Applying knowledge of operational end-user environments and support for operational integration (including training, exercises, equipment, tactics, techniques and procedures) to technology development;**
- **Enabling first responders and end-users to address operational mission requirements through the coordination of technology development requirements and opportunities;**
- **Supporting development and use of homeland security equipment and operational standards.**

The laboratory's pilot deployment programs support the transition of homeland security **technologies from the developing and testing phases to operational field trials and provide a critical scientific interface with end-users in the field and thus, support to real innovation.**

Additionally, the laboratory serves as the technical authority to New York area operational-level and responder organisations in applying homeland security technologies and providing technical reach-back capabilities. Through its interface and outreach efforts, the laboratory promotes the acceptance and integration of homeland security technologies and standards, and accelerates the delivery and successful deployment of enhanced technological capabilities to the end-users.

The Office for Interoperability and Compatibility (OIC), an operating unit within DHS Science and Technology's FRG, provides the science and technology that enables emergency communications and facilitates the seamless exchange of information.

The Technology Clearinghouse / R-Tech (TCR), also known as the TechSolutions Program, was established by the Department of Homeland Security's Science and Technology Directorate to provide information, resources and technology solutions that address mission capability gaps identified by the emergency response community. The goal of TechSolutions is to field technologies that meet 80% of the operational requirement, in a 12 to 15 month time frame, at a cost commensurate with the proposal but less than $1 million per project. Goals will be accomplished through rapid prototyping or the identification of existing technologies that satisfy identified requirements.

2.2.1 Research projects with relevance for DRIVER

DRIVER is a large-scale demonstration project within the Security research programme of FP7. Given the structure of projects within this programme, it is interesting to note how it relates to earlier projects. For this report, which is focused on the experimentation aspect, the comparison is made in terms of relevant methodological results.

Projects to be listed in this regard are

- Wide maritime area airborne surveillance: WIMA^{2}S (2008-2011) [38]
- Container Security Advanced Information Networking: CONTAIN (2011-2015) [39]
- Sea border surveillance: SEABILLA (2010-2014) [40]
- Secured Urban Transportation – A European Demonstration: SECUR-ED (2011-2014) [41]

In all the four mentioned projects FOI has been in charge of comprehensive assessment of security solutions, often working together with other DRIVER partners. The methodological tradition thus established is now continued in DRIVER. A characteristic element is broad and pragmatic exploitation of available knowledge resources; information like experiment results and expert cost estimates are of course crucial but generally need to be interpreted and generalised in assessment workshops. Understanding of the security missions is absolutely crucial. For example, in mass transport the fact that urban public transport is about low-budget organisations dealing with very high numbers of passengers must always be kept in mind; solutions from aviation security can seldom be directly imported.

The following means for solutions evaluation have been used e.g. in WIMA^{2}S and might be of interest to the work in DRIVER SP2:

- Simulation based on operational scenarios
- Innovative concepts and technologies held by simulation (algorithmic modelling, remote control, sensor data fusion)
- In flight experiment (remote control, crew concept)
- Cost benefit analysis

From a methodological point of view, SEABILLA can provide important lessons for DRIVER. The project made extensive use of modelling and simulation, using MoS platforms at several of the partners' sites to model and test individual systems and SoSs. The initial ambition of distributed, on-line simulation of separate models, hosted at different sites, could not be fulfilled. The reason was mainly technical complications regarding interfaces and data exchange formats between different modelling platforms.

[38] www.wimaas.eu last accessed 25 April 2015
[39] http://cordis.europa.eu/project/rcn/100574_en.html last accessed 25 April 2015
[40] http://www.seabilla.eu last accessed 25 April 2015
[41] Quote from SECUR-ED's web site: http://www.secur-ed.eu/ last accessed 25 April 2015

Further results from the projects mentioned are discussed in different sections below.

2.2.2 European Operational Concept Validation Methodology (E-OCVM)

The present document is focusing on high-level capability development methodology. Consequently, it does not discuss any individual concept assessment or experimentation methods[42]. However, since DRIVER is about capability development by systems engineering, this document should also have a look at methodologies developed in field other than security and crisis management.

"The European Operational Concept Validation Methodology (E-OCVM) was created as a framework to provide structure and transparency in the validation of air traffic management (ATM) operational concepts as they progress from early phases of development towards implementation. Its aim is to achieve consistency in the collaboration of independent R&D organisations, aiming at a coherent approach and comparability of results across validation activities and projects, while leaving freedom to define the most practical planning and execution of individual activities. It provides validation practitioners, as well as experienced programme and project managers, with both a common understanding of what is required to perform validation and the framework necessary to collaborate effectively. Since 2005 it has been mandatory to apply the E-OCVM in collaborative ATM R&D projects of the European Commission and EUROCONTROL.

The current version 3 of the E-OCVM continues to be a framework for carrying out R&D rather than a strict set of rules. It complements the principles of earlier versions based on real experiences of applying the methodology[65].

In 2007 the European Commission and EUROCONTROL set up a public-private partnership called the SESAR[43] Joint Undertaking (SJU) to represent the principal stakeholders of the ATM system. The role of the SJU is to ensure the modernisation of the European air traffic management system by coordinating and concentrating all relevant R&D efforts in the Community. Version 3 of the E-OCVM was timely in view of the many validation activities currently being initiated in the SESAR Development Phase. Principles of the E-OCVM have contributed to the SJU's approach to validation, which is embodied in the System **Engineering Management Plan (SEMP) and the SESAR Valida**tion and Verification Strategy."[44]

[42] For a more detailed discussion of individual methods, please refer to deliverables of DRIVER WP23.
[43] http://www.sesarju.eu/ last accessed 25 April 2015
[44] Quote taken from https://www.eurocontrol.int/sites/default/files/publication/files/e-ocvm3-vol-1-022010.pdf last accessed 25 April 2015

2.3 DRIVER approach to strategic capability development – state of play

The DRIVER project aims – besides developing improved crisis management capabilities – at developing a more strategic approach to crisis management capability building. This chapter summarizes the developments so far and where we stand today. An outlook to the DRIVER long-term vision is provided below (cf. chapter 3.3)[45].

As described above, EU FP7 Demonstration Projects are divided into two main phases, I and II. While phase I comprises one or more preparatory actions (Coordination and Support Actions, so called CSAs), the phase II is the actual demonstration activity.

For the phase I of the "Aftermath **Crisis management System-of-**systems" De**monstration Project, three projects were granted: ACRIMAS[46] (Aftermath Crisis management System-of-Systems, led by Fraunhofer INT), CRYSIS[47] (Critical Response In Security and Safety Emergencies, led by EOS), and HELP[48] (Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems, led by UP de Catalunya). While HELP was solely focused on communication technologies, ACRIMAS and CRYSIS had a more holistic approach and looked at topics for improvement of European crisis management in general and also for a respective demonstration activity from an all hazards approach potentially covering the full technology spectrum.**

Especially the ACRIMAS gap analysis and potential solutions identification as well as the ACRIMAS demonstration concept formed the analytical basis for the development and design of the DRIVER project and its approach[49]. Further results were taken up from CRYSIS results in order to complete the picture and to achieve a set of demonstration topics that are commonly agreed by a wide range of EU crisis management stakeholders.

ACRIMAS started from the consideration that the project had to prepare a large-scale demonstration in a very heterogeneous and fragmented field. Further the project acknowledged that innovation (that should be achieved by the demonstration activity) in crisis management is not about a wholesale redesign of European crisis management, but has to be performed as a continuous activity that is based on a methodology for test & validation taking into account the complexity of crisis management and the modes of cooperation in European joint operations. Also, ACRIMAS started to build up a European crisis management community, i.e. started to provide a forum for exchange and for interconnecting different existing networks (the ACRIMAS expert database[50]).

[45] Cf. Also DRIVER D13.2 „Milestone 1 Report"
[46] www.acrimas.eu last accessed 25 April 2015
[47] http://www.eos-eu.com/EUfundedProjects/CRiSyS/tabid/303/Default.aspx last accessed 25 April 2015
[48] http://www.fp7-sec-help.eu/ last accessed 25 April 2015
[49] Note that the seemless integration of ACRIMAS results into DRIVER is not based on the structure of FP7 (cf. section 2.2.2.1), but was an accidental result of key-ACRIMAS-partners being also partners in DRIVER.
[50] ACRIMAS D7.3 „Contact database".

In terms of its strategic approach DRIVER was – given the rule that FP7 phase II demonstration projects are rarely informed by their phase I[51] - lucky to be able to build on the preparatory work that was performed in ACRIMAS (merely because there is an overlap between ACRIMAS and DRIVER core partners), namely gap analysis, preliminary concept development, and a proto demonstration concept.

For the capability gaps analysis a wide stakeholder (mainly end-user) survey was performed. Requirements were described in different dimensions (based on an analysis of the political and legal framework and of aspects of the operational crisis management that would be affected by novel tools) and clustered to areas where improvement is needed. Further potential solutions (concepts, in CD&E terms) to fill the gaps were identified. Clustered topics were further grouped to demonstration strands that could reasonably be addressed jointly in a series of experiments, as now being conducted in DRIVER.

In order to come up with a suitable demonstration concept (later series of experiments based on the CD&E approach), ACRIMAS analysed the realm of military capability development and adapted available methods. The result was to propose the development of a crisis management test-bed as space for experimentation activities that are based on a CD&E methodology (cf. section 2.1.1).

ACRIMAS and DRIVER also adapted the System-of-systems approach - based on earlier work on mass transport security in the DEMASST[52] and SECURE-ED project - to European crisis management.

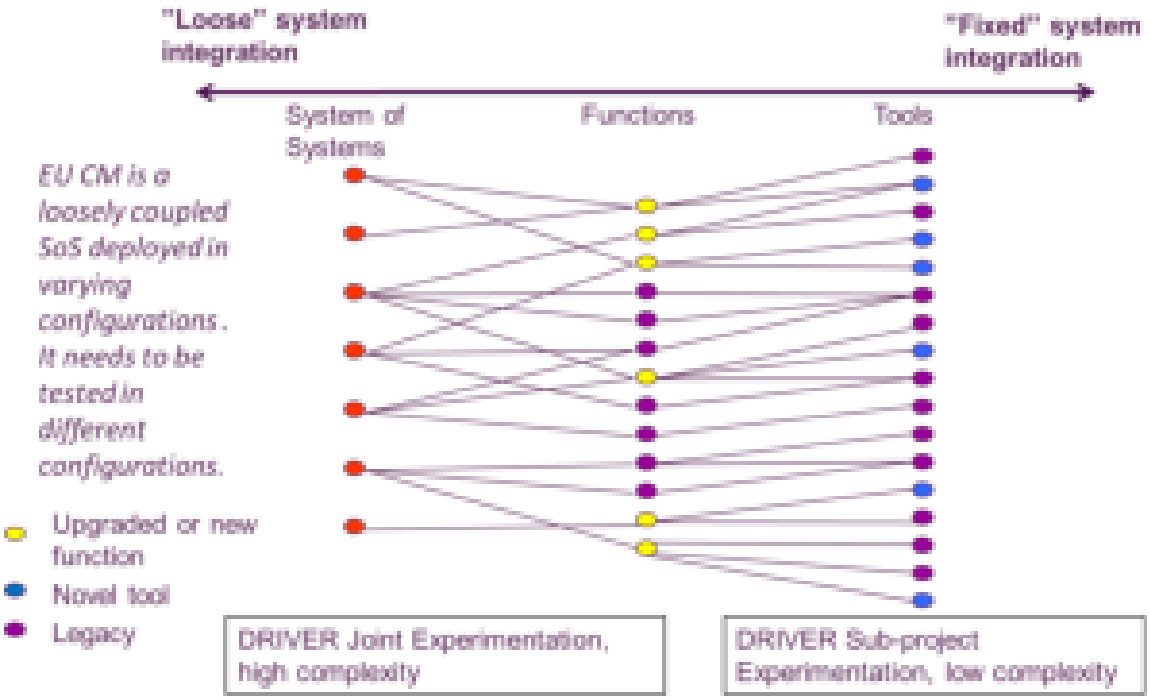

Figure 7: DRIVER understanding of the crisis management System-of-Systems approach[53]

[51] Cf. section 2.2.1.
[52] http://www.demasst.eu/ last accessed 25 April 2015

As described above, DRIVER starts with the consideration that operational European crisis management already is a loosely coupled SoS that is fed by varying elements of individual crisis management SoS of the different EU Member States (these, in turn, consist of different first responder types, operational assets, organisational structures, procedures, policy, legal provisions, training & education, national crisis management cultures, societal cultures etc.). The different elements are grouped into modules that can address different sorts of incidents, and are being deployed on a temporary basis in national, bilateral or multilateral operational cooperation depending on the task and the scale to be addressed. This means that system integration at SoS-level is rather "loose", modula**r and temporary. In contrast, new solutions that are being developed to improve cross-border crisis management are** subject to "fixed" system integration by being a component or an upgrade of an e.g. **Situational Awareness Systems. The resulting integrated systems however, combinded at a SoS-level have to be validated & assessed in varying module configuration with other systems, depending on the operational and cooperation context. This assessment is planned to be done in the DRIVER experimental campaigns using the DRIVER test-bed (see below). At** the same time this approaches "**allows the risk-taking necessary to create genuinely new knowledge at system-of-system level**"[54].

On the basis of the work in ACRIMAS (but also DEMASST and SECURE-ED[55]) and on thoughts described above, the three DRIVER objectives were developed:

1. **The development of a tested and validated portfolio of emerging crisis management solutions.**
2. **The development of a pan-European test-bed.**
3. **The creation of a more shared understanding of crisis management in Europe.**

From these objectives the three DRIVER dimensions can be derived:

1. **The Solutions dimension represented by SP3456.**
2. **The Methodological dimension (the test-bed) represented by SP2 (supported by SP8 and SP9).**
3. **Community building represented mainly by SP7.**

For a more detailed description of each dimension please refer to D13.2 (Milestone 1 Report).

[53] Adapted from SECURE-ED.
[54] DRIVER D13.2, p. 12.
[55] http://www.secur-ed.eu/ last accessed 25 April 2015

2.3.1 Components of the Methodological & infrastructure dimension

The DRIVER pan-European distributed test-bed framework is envisaged to be built on five pillars.

1. The first pillar is made of people & knowledge, i.e. crisis management experts and data from experiments and past crises. Building up this pillar starts from DRIVER partners and will be subsequently followed on by setting-up the DRIVER SP2 Community as the project evolves. Note that this community is supposed to have a different function than the User dimension.
2. The second pillar of the test-bed is the DRIVER platforms, i.e. the physical test facilities to run experiments. At this point DRIVER has six platforms for experimentation, namely
   - Pôle Risques: Several sites and partner organisations, southern France
   - MSB (Swedish Civil Contingencies Agency): Revinge, southern Sweden
   - THW (Technisches Hilfswerk): Several sites across Germany
   - City of Hague: Operational crisis management organisation, extensive networks at Den Haag Safety Region
   - Polish Crisis management Organisations: several sites across Poland, managed through DRIVER partner ITTI
   - JRC Crisis Lab[56]: Hub for the DRIVER Network Experimentation Platform, northern Italy

   In post-project sustainability (see test-bed objectives below), it is not envisaged as a static infrastructure, but as a methodological framework and network of people that is based on a variable and flexibly attachable pool of physical platforms depending on the research question to be tackled. Critical will be to developed virtual interfaces that support flexible plug-in of additional platforms depending on the experimentation to be run. Large-scale experimentation fully exploiting the platforms will, due to budgetary constraints, rather be the exception than the rule.
3. Data recording & storage tools will form the third pillar of the test-bed. These include all tools that have to be added to the DRIVER platforms to enable their use as an experimental platform. Tools will include e.g.
   - Modelling and Simulation tools
   - Data recording and data base systems to take-up and store experimental data
   - Data analysis tools to technically enable scientific evaluation of the DRIVER experiments
   - System architecture for the test-bed.
4. The fourth pillar will be made of experimentation methodology that supports

[56] The JRC platform has a specific role to develop a capacity for distributed experimentation..

- Designing of experiments and campaigns of experiments
- Planning of experiments and campaigns of experiments
- The scientific evaluation of the DRIVER experiments.

It will include the selection of available statistic methods and adaption of methods form the military realm as well as the definition of performance parameters for crisis management tools, systems and capabilities and metrics to assess those.

5. Ideas will form the fifth and last pillar of the DRIVER test-bed. It refers to bringing new concepts into the CD&E process and will be fed by the Solutions dimension.

3 Test-bed objectives

3.1 Test-bed objectives during the lifetime of the project

The goal of DRIVER SP 2 "Test-bed" is to build up a distributed test-**bed** – **consisting of five pillars: people, platforms, data recording & storage tools, methods, and ideas – for the conduct of experimentation leading to an enhanced knowledge base as well as assessment and refinement of novel crisis management tools from component to SoS level. The building process started with the start of the DRIVER demonstration project in May 2014. The starting point for the test-bed is the DRIVER platforms (see above)) as well as the State-of-the-Art analysis conducted in preparation of the present document, which aims at informing the DRIVER project and SP2 about available methodology as well as comparable innovation mechanisms for crisis management elsewhere.**

While the first phase of the DRIVER project (Sub-project experimentation 1, SE1) - characterised by SP3-5 defining the State of the Art in their respective thematic domain, by doing inventories of the tools available to the consortium, and by thinking and trying of different experimental approaches – for SP2 was a phase of starting to develop tools, methods, infrastructure and ideas, the second phase, i.e. SE2, should be characterised by the test-bed actually starting to be able to practically support experimentation in SP3-5[57].

The support should be carried out from M12 (April 2015) and should materialise in different dimensions, including

- **The development of a wider network of experts that can support DRIVER experimentation with their expertise and experiences**
- **Practical plans, guidelines and information to enable coordination between experimentation teams and platform providers**
- **First methodological support for planning, execution and evaluation of experiments (first set of proto-guidelines)**

Further activities that will support experimentation at a later stage, but should be starting to become more concrete now are

- **Decision on test-bed architecture and tools to be implemented**
- **Plans & inventory of issues related to platform preparations and improvements needed for the Joint Experimentations**
- **Starting the work on requirements for the establishment of the ENCML**

Plans at a work package level include what is described below.

[57] **Cf. Also D13.2, chapter 5** "**Subproject experimentation campaign 2 – SE2**" and Annex I.

3.1.1 DRIVER Work Package 21: Coordination and SP2 Objectives

WP21 deals with the overall coordination of the SP and with the strategic objectives. It is also in charge of building the SP2 community.

It is responsible for developing a shared understanding of objectives, roles and responsibilities among the involved platforms, and throughout the whole project to ensure the activities are aligned and coherent with the actions carried out in other work packages and sub-projects.

WP21 ought to realise a benchmark of the existing resources for developing Crisis Management capabilities throughout Europe. Specific objectives and long term goals for the DRIVER test-bed will be drawn based on that analysis of the state of the art.

Last but not least, the role of this WP is to build a strong Crisis Management community of interest among the DRIVER partners and beyond, encompassing all Crisis Management functions and organisational levels.

Eventually, all these actions aim at ensuring the sustainability of the DRIVER test-bed, in cooperation with SP7.

3.1.2 DRIVER Work Package 22: Experimentation Support Tools

WP22 is concerned with designing and describing the architecture and data-exchange standards for the DRIVER test-bed. The architecture of the DRIVER-test-bed is defined using existing simulation tools developed by DRIVER partners. A comprehensive overview of simulation tools is made to select suitable models contained within these tools (e.g. scenario presentation, models of incidents, models of crisis management actors and systems, simulated environments, simulation orchestration tools) and to help identify suitable DRIVER-test-bed infrastructure related software components (interfaces, middleware etc.). The architecture description describes how the different elements are integrated in a (secure) distributed DRIVER-test-bed using the selected middleware. The DRIVER-test-bed architecture will take into account specific requirements from DRIVER platforms owners and DRIVER experiments. Identifying these requirements and translating them to DRIVER-test-bed requirements is done in the next phase of the WP. The implementation of the DRIVER-test-bed is done in a subsequent work package.

One element of the DRIVER-test-bed will be a reference database, to support the planning and analysis of experiments. A DRIVER reference database for crisis management analysis will be developed and maintained. This database will contain: descriptions of actors and data (e.g. objectives, organiser(s), participants, location(s), date, duration), how to use live real world and virtual components (test-bed, simulation tools, orchestration tools), experiment results (main outcomes, such as lessons identified). It will also contain data on historical crisis events and catastrophes including economic effects of past disasters and an

assessment of overall impact (e.g. casualties, material damage, affected infrastructures & economic sectors, socio-psychological and environmental effects) where necessary, to support analysis where experimental data are impossible to obtain, and to guide the creation of realistic scenarios for future experiments.

Success of WP22 is key for the DRIVER project to meet one of its main objectives: "*The development of a pan-European test-bed: An assembly of virtually connected, distributed operational or training facilities dedicated to experimentation plus test-bed tools (modelling and simulation, data recording, data analysis), methods (experiment design, campaign planning, analysis, evaluation), people (cf. DRIVER community), and ideas) enabling the testing and iterative refinement of new crisis management solutions*"[58]**.**

WP22 delivered the first version of document "*DRIVER-test-bed: Architecture, Integration and Orchestration*" (**Deliverable D22.21). This document describes the services oriented approach used in developing the test-bed architecture. The document identifies the** relationships with other key WP's in the project where it concerns input and output of **information. It also provides a number of skeleton chapters on test-bed elements, standards, etc. Subsequent versions of this document will contain more details on the DRIVER-test-bed architecture based amongst others on the requirements from platforms and DRIVER experiments, and on information becoming available from other DRIVER tasks and work packages.**

WP22 delivered a first version of document "*DRIVER-test-bed: Simulation models for Experiment Support*" (Deliverable D22.21). This document describes models and tools that **are available from the DRIVER partners and might be relevant for the test-bed. To make an inventory of the relevant test-bed elements, a questionnaire was designed and sent out to all partners to fill out. The result are being collected and put in D22.21 and its successors.**

WP22 delivered a first version of "*DRIVER Reference Database*" (Deliverable D22.31). This **version contains an overview and work plan, description and function of the database, implementation issues, and a literature study. To structure information on experimental results for Reference Database a questionnaire was designed to collect the information from SP3-5. Relevant findings in the DRIVER experiments, the database structure and implementation, will be provided in next versions of the document.**

To get a clear view on the objectives of the DRIVER-test-bed, a key activity in the next phase of WP22 will an analysis of the requirements of the platform owners and the envisioned experiments, and how this relates to the required capabilities of the test-bed. Another activity with high priority, will be an inventory of the information (including a time-line) coming from other DRIVER WP's and an analysis of the requirements and objectives **emerging from it for the DRIVER test-bed during the project and in the foreseeable future.**

[58] http://driver-project.eu/ last accessed 25 April 2015

3.1.3 DRIVER Work Package 23: Experiment Campaign Methodology

WP 23 is in charge of developing the DRIVER Experiment Campaign Methodology, i.e. methods and tools that support the experimental design, the assessment of crisis management solutions' performance in a given experimentation, the assessment of life cycle **costs of crisis management solutions, and the assessment of contributions of novel solutions to operational crisis management functions.**

Initially, the work package will set basic methods and best practices adapted to the specific needs for DRIVER. As the project evolves, and the complexity of experiments increases, the framework will be updated to more complex experiments by using the feedback from experiments owners. At the end, the methodology outlined here should be able to support a large range of complexity in experimentation, from simple conceptual systems to highly complex system-of-systems.

WP 23 is divided into three main areas:

- **Experiment design: describes the design phase of experiment campaigns, taking into account the assessment of validation from the initial concept development.**
- **Performance and metrics: establishes the indicators to quantify the performance of the experiments in specific areas. Besides, it proposes multi-criteria decision theory to choose the appropriate solution.**
- **Cost methodology: illustrates the capital importance of cost assessment as a key indicator in the implementation of a solution. It pays special attention to cost-effectiveness evaluation for crisis management solutions.**
- **Effectiveness assessment: develops methods to evaluate the overall performance. The importance of this task is directly proportional to the complexity of the experiment in study.**

The work on experimental design will include not only to design individual experiments around specific research questions to be explored or answered, but also the design of related series of experiments (experimental campaigns) that build on one another and look at crisis management tools in increasingly complex interrelationships. The aim of the assessment is to be able to assess the value added of a given solution in carrying out an existing or novel crisis management function[59].

Experimental design elements to be developed include formulation of research questions and their stepwise analysis across different complexity levels, selection and generation of the appropriate scenario definition of the experimental setting and supporting tools (see also description of WP22, above) including the appropriate use of Modelling & Simulation tools, compilation of plans and guidelines for the experimentation team and further participants including the selection of the right participants in terms of stakeholder group

[59] DRIVER D13.2 „Milestone 1 Report"**, p. 12.**

and expertise, and guidelines for selecting evaluation, assessment and interpretation methods of results.

Performance and benefits metrics are to be developed in order to support the definition of what data needs to be captured to assess the contribution of a given crisis management solution to specific functions. An important part of this task will be to acknowledge the different perspectives of the various stakeholders of crisis management. Whereas first responders might be most or solely interested in a more effective crisis management operation, procurement agencies will be also interested in cost-efficiency, while European policy makers take an interest in tools that support European crisis management policy and that are capable of being integrated into the crisis management modules being set-up on a cross-border basis[60]. It has to be kept in mind that often stakeholder interests have to be balanced, since compromises that can be worked out often might be trade-offs or even conflicts. So, the right measures have to be selected and their characteristics in terms of "what exactly do they tell us" have to be understood in order to be able to **measure (in the right experimental design) and store the right kind of data and appropriately assess a novel solutions and its contribution to one or more crisis management functions.**

Costing methodology strongly relates to the performance assessment, since decision makers always have to balance the costs and the benefits of individual tools that are to be invested in. Financial costs of crisis management tools are subject of the work in SP2, whereas potential societal or environmental costs are being taken care of in DRIVER SP9[61]. Costs of individual tools are obviously not limited to their procurement costs, but include costs related to the entire life cycle of the tool or systems (procurement, costs of operating the tool, maintenance, decommissioning etc.) and costs that occur through its relation to other parts of the crisis management SoS (costs for technical integration, training of personnel, adjustment of procedures, impact on other systems that need to be adapted or changed etc.).

Methods for overall impact and effectiveness assessment are being developed in order to enable the synthesis of the DRIVER experimental campaign and to provide an indication of the overall impact of a tool in interrelation with other tools and the legacy crisis management SoS on the crisis management process. Again, it will be critical to incorporate views of different stakeholder groups to provide a multi-criteria assessment. The work in WP23 will provide the basis and will later be continued in WP65 (SP6).

[60] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1401179579415&uri=CELEX:32013D1313 last accessed 25 April 2015

[61] SP2 and SP9 to coordinate on this.

3.1.4 DRIVER Work Package 24: Test-bed Implementation

As soon as the work in WP22 and WP23 reached a certain level of maturity it needs to be put together in a framework that (i) will later build the interface of the DRIVER platforms (and potentially further platforms later) and the common methods of the test-bed, and (ii) will support experimentation in SP3-6. The underlying rule for distinguishing between (i) what will later be the test-bed framework and (ii) what will support experimentation is that the experimentation support will end after the DRIVER experimental campaigns are ended, while the test-bed architecture and methods are aimed to survive the end of the project and are sought to be transferred into the "sustainability-phase" of the test-bed. The test-bed takes up everything that is of general added value to any crisis management experimentation, the experimentation support is dedicated to the specific experiments conducted in Subproject-experimentation SE1, 2 and the Joint Experimentation (JEs).

WP24 will develop guidelines for experimentation that compile the work done in WP23. The task is to transfer the methods developed into a generic manual for DRIVER-style crisis management experimentation.

Also, the different test-bed tools developed in WP22 need to be integrated. Moreover, it needs to be ensured that also the SP3-5 tools experimented on (and also other tools in the future) can be integrated into the test-bed architecture. To support this, SP345 tools will undergo iterative compliancy tests with a set of key configurations that are being used during the experimentation and that will later become part of the test-bed to support also tools that are experimented in future, i.e. post-DRIVER experiments for which the test-bed is being used.

3.1.5 DRIVER Work Package 25: DRIVER Platforms Preparation and Improvement

As described above, the DRIVER platforms are infrastructures that already exist and are brought into the project. Their original purposes vary from crisis management training and exercise (e.g. THW, Pole Risque), via being operational crisis management systems of a big city (City of The Hague), to being software development laboratories (JRC test crisis room). Consequently, they have – to a varying extend – to be adapted to their use as an experimental platform. Since most likely these upgrades will be not sufficient to fully equip most of the platforms for their new role as an experimentation platform, also a long-term plan for further adjustments are sought to be developed.

WP25 is concerned with the preparation of the platforms for the DRIVER experiments.

Based on the long term objectives drawn in WP21, WP25 will identify the platform improvement needs and produce a plan to make sure the respective platforms have the necessary capacities to host the DRIVER experiments (WP26). The platforms will be asked to fill in a questionnaire to identify their own gaps, in a standardized format so that comparison is made possible between the capacities they offer.

When necessary, selected upgrades will be performed. These will only concern basic infrastructures, notably basic ICT support.

This WP is built as an iterative process with WP26. Indeed, the lessons learned from the successive experiments will be used to update the upgrades and improvement needs to meet the future experiments needs. Therefore, the timeframe of WP25 is aligned with the experimentation periods.

Finally, WP25 will also produce a plan for continued improvements, to ensure the long-term objectives of the test-bed are met.

3.1.6 DRIVER Work Package 26: DRIVER Experiment Hosting

WP 26 is concerned with the coordination, preparation and the actual hosting of experiments. All partners of this WP are platform owners and therefore have an equal interest in the success of each experiment taking place on their platforms. The aim of this work package will be firstly, to define in accordance with SP3-SP6, which experiment should be run preferably on which platform. Through close cooperation with the other SP, responsibilities will be determined. Supporting materials such as checklists will be created, assisting platform owners in preparing the platforms for an experiment. Secondly, as the WP is responsible for the preparation and alteration of platforms according to experiment needs, it will assist platform owners setting up ICT infrastructure (closely interlinked with WP 25), recruiting local end-users, crisis managers, volunteers and other groups and make all logistic arrangements. Thirdly, the WP is responsible for the documentation of all upgrades and its experience obtained by running DRIVER experiments on the various platforms.

3.1.7 DRIVER Work Package 27: The DRIVER Network Experimentation Platform

A sub-objective of DRIVER SP2 is to form and establish a European Network of Crisis management Laboratories (ENCML). In order to do this WP27 will develop requirements to be fulfilled to be part of the network and a strategic plan to further improve the capabilities with regard to crisis management experimentation of the network and its members.
The network will start with respective facilities several DRIVER partners, namely of TNO, TCS, FOI and members of Pôle Risques. Post-DRIVER sustainability will include efforts to take further labs on board (cf. Table 1).

Organisation	Physical Infrastructure	Tools & Competencies
Airbus (France)	System Design Center	Analysis Tools, Evaluation Methodologies, etc.
IABG (Germany)	Simulation Integration Test (SIT) Laboratory	Simulation Models, Orchestration Tools, etc.
Siemens AG (Germany)	Siemens Airport Center (SAC)	Full-Scale Airport Simulation Center
MSB	MSB College Revinge MSB College Sandö	Necessary Equipment for Large-Scale Field Exercises

Table 1: Potential candidates for the European Network of Crisis Management Laboratories (ENCML)

3.2 Mid- to long term test-bed objectives

The DRIVER Methodology & infrastructure dimension (the test-bed) will grow stepwise through co-evolution with the complexity of the DRIVER experimentations, i.e. as a result of SP3456 demanding an ever more complex infrastructure for experimentation on crisis management tools.

The ultimate goal is to create an infrastructure that enables evidence-based decision making with respect to crisis management R&D and – to a lesser extend - procurement decisions. The development of infrastructure is not limited to physical and methodological components, but is envisaged to also include the creation of a test & validation expert community. Further, the results of SP2 can contribute to a standardised way to test & evaluate novel crisis management solutions and to give recommendations for future research and research instruments.

The DRIVER test-bed is envisaged to be built during the DRIVER project and further enlarged and improved (in all five pillars) after the project has ended, in the so-called post-DRIVER sustainability-phase. This is a goal that cannot be achieved by SP2 alone. SP2's task in this **endeavour is to build up a functioning test-bed that provides a recognisably added value to innovation processes in crisis management. To run the test-bed even after the end of the project, however, requires more than just the test-bed. It requires reaching out to all crisis management stakeholders and has to be done by convincing project results and a tailored and clear communication strategy to be developed by DRIVER SP7 and WP13.**

For post-DRIVER sustainability we currently foresee the following "business model" for the **test bed and its relation to the other two dimensions of DRIVER (Solutions & Users):**

The DRIVER (innovation) Community dimension aims at enabling crisis management end-users at local, but also cross-border level to articulate their requirements and to enter a structured debate with research and industry (and other stakeholders) about capability development. In post-DRIVER sustainability User community interactions might be facilitated by some sort of organisation that provides a hub for different other networks interested in crisis management innovation and enables sharing of best practices etc.

The DRIVER Solutions dimension will be – and is already today – represented by solutions providers, i.e. any organisation that develops novel ideas and crisis management solutions of any kind (technical solutions, but also doctrines, training courses, and information programmes). These organisations will mostly, but not exclusively be of a research or industry type. DRIVER will enrich this dimension by providing a functional architecture for crisis management and by giving an elaborated indication of the maturity of certain crisis management areas as of today.

The Methodology & infrastructure dimension, i.e. the subject of the present report, is envisaged to act as a mediator/translator between the two other dimensions. Its representatives in the crisis management innovation ecosystem will be any organisation that is capable of providing test-bed services enabling a structured and evidence-based debate

on requirements, potential solutions, and capability development. It aims at providing support to the User side in terms of requirements analysis and to the Solutions and User side in terms of solutions assessment with regard to their contributions to given requirements. That way it will support the end-user in selecting the right solutions for further R&D decisions and appropriate instruments. Methodological and infrastructural means for executing this role will range from large to smaller scale experimentation to table top "dry" experimentation and moderated workshops. The latter two options will – due to the high costs of real experimentation – rather be the rule, whereas large and even smaller experimental campaign, like the DRIVER JEs, will only be possible, if appropriate budget and appropriate pre-planning time to prepare the necessary platforms is available. Test-bed services provided – in order to be reliable – have to be executed according to the methodology developed by DRIVER. Some sort of certification for this is envisaged.

3.3 Agenda for improving EU crisis management capability development – long-term goals of the development of the methodology & infrastructure dimension

As stated in before DRIVER wants to develop a capability building mechanism for crisis management. A first version will be built during the lifetime of the project. The test-bed is envisaged to be further enlarged (in terms of platforms, methods and research questions/solutions to be tackled) after the project has ended. To this end, it is planned to develop a strategy for test-bed sustainability.

Also, as mentioned above, DRIVER plans to contribute to the European crisis management eco-system by improving its three dimensions, which are also the three dimensions of DRIVER (cf. above).

3.3.1 Definition of an innovation eco-system

According to Wikipedia "the concept of the **innovation system stresses that the flow of technology and information among people, enterprises and institutions is key to an innovative process. It contains the interaction between the actors who are needed in order to turn an idea into a process, product or service on the market »**[62]**. Since interactions among participants of the system are understood to be key in that process, DRIVER uses the term innovation eco-system**[63] **to emphasise this notion.**

In terms of crisis management innovation (or even overall security innovation for that matter) – which is still an embryonic field as regards structured research and innovation processes – we define the eco-system as consisting of supply and demand side as well as of scientific support that compensates for the heterogeneity of research areas to be involved and for the characteristics of crisis management. The latter can be summarised as

- **Crisis management includes many types of potential task (often definable as threats) to consider;**
- **It does normally not make sense focusing only on a few high impact/(relatively) high probability threats;**
- **Threat events are typically rare;**
- **Due to the rare occurrence of many high impact threats, operational experience** cannot be fully trusted like in a 'normal' industry**;**
- **The scope of insecurity – number of distinct types of potential task – grows as societies grow more complex, but not necessarily frequency and consequences;**

[62] http://en.wikipedia.org/wiki/Innovation_system last accessed 25 April 2015

[63] Definition of the Oxford dictionary: A biological community of interacting organisms and their physical environment.

- It is impossible building dedicated solutions for each crisis type, i.e. a modular approach the only option;
- Responsibilities are fragmented, i.e. costs and benefits often affect different stakeholder groups;
- Solutions must be adapted to the local realities;
- Solutions must be legally and ethically acceptable;
- Solutions may have unexpected counterproductive side effects;

In sum this means that a solid knowledge base needed for legitimate uptake of new solutions among end-users – positive thinking and advertisement of research results is not enough!

Consequently, we structure the crisis management innovation eco-system along three dimensions: Solutions (=supply), Community (=demand), and Methodology & infrastructure (=knowledge base and structured interaction between the other two).

3.3.2 Current state of the crisis management/security innovation eco-system

In section 2.2.1 we describe what can be regarded as the current state of the security innovation eco-system and as the state of the art of innovation management in EU Security Research. Looking at it from the three dimensional eco-system perspective, we observe different states of maturity for each of the dimensions.

The EU and associated countries have quite a good research & industry base at their disposal. We are definitely not lacking novel ideas and we put a considerable amount of budget into developing them in different research programmes. Thus, the Solutions dimension of the eco-system can be regarded as relatively mature. However, at least for crisis management it lacks a functional architecture and – at least when compared to other industries – a long standing tradition of industry and research to work with civil security users, and especially at EU-level.

Looking at the User community dimension, we notice that end-users are contributing to research activities in some sense, but without (i) their role in the process being well defined, (ii) being trained to influence the process the way it is needed, (iii) being involved at the right time during the innovation process (requirements definition and formulation, update of requirements, filtering novel solutions), and (iv) being supported by scientific assessment.

The Methodological & infrastructure dimension is currently virtually absent, which is true for the entire security innovation eco-system. As a consequence, the end-user community as well as solution providers lack an appropriate knowledge base as well as support in executing an informed and structured debate. Here is where the DRIVER test-bed comes in.

3.3.3 The defence innovation eco-system

Looking at defence innovation eco-systems – here done by taking the example of the German Ministry of Defence's (**MoD) Costumer Product Mechanism (CPM, see also figure 8) – gives a good indication of the types of interactions needed for a (relatively) well working eco-system. Comparing its Solutions dimension to civil security, one also notices no lack of novel ideas, but also a long history, grown relations and a common culture for structured debate between national industry and MoDs[64]. On the User community site Armed Forces and procurement agencies traditionally have well-defined and well-timed roles in the innovation eco-system (cf. figure 8). Finally, the Methodological & infrastructure dimension is characterized by continuous scientific support, by constantly creating and updating a knowledge base, and by assessments of solutions on the basis of well-defined requirements. Also, analysis of novel solutions is, as described in the above, characterized by CD&E processes.**

We do not claim that the defence innovation eco-system is a perfect model for the security or crisis management eco-system, however, we claim that both systems exhibit some important similarities (e.g. expensive R&D phases; few costumers, limited budget etc.) that make it worthwhile to look at the defence system in order to realise what security is missing.

[64] One of the reasons why it is also difficult here to establish EU-level defence R&D co-operations or even procurement.

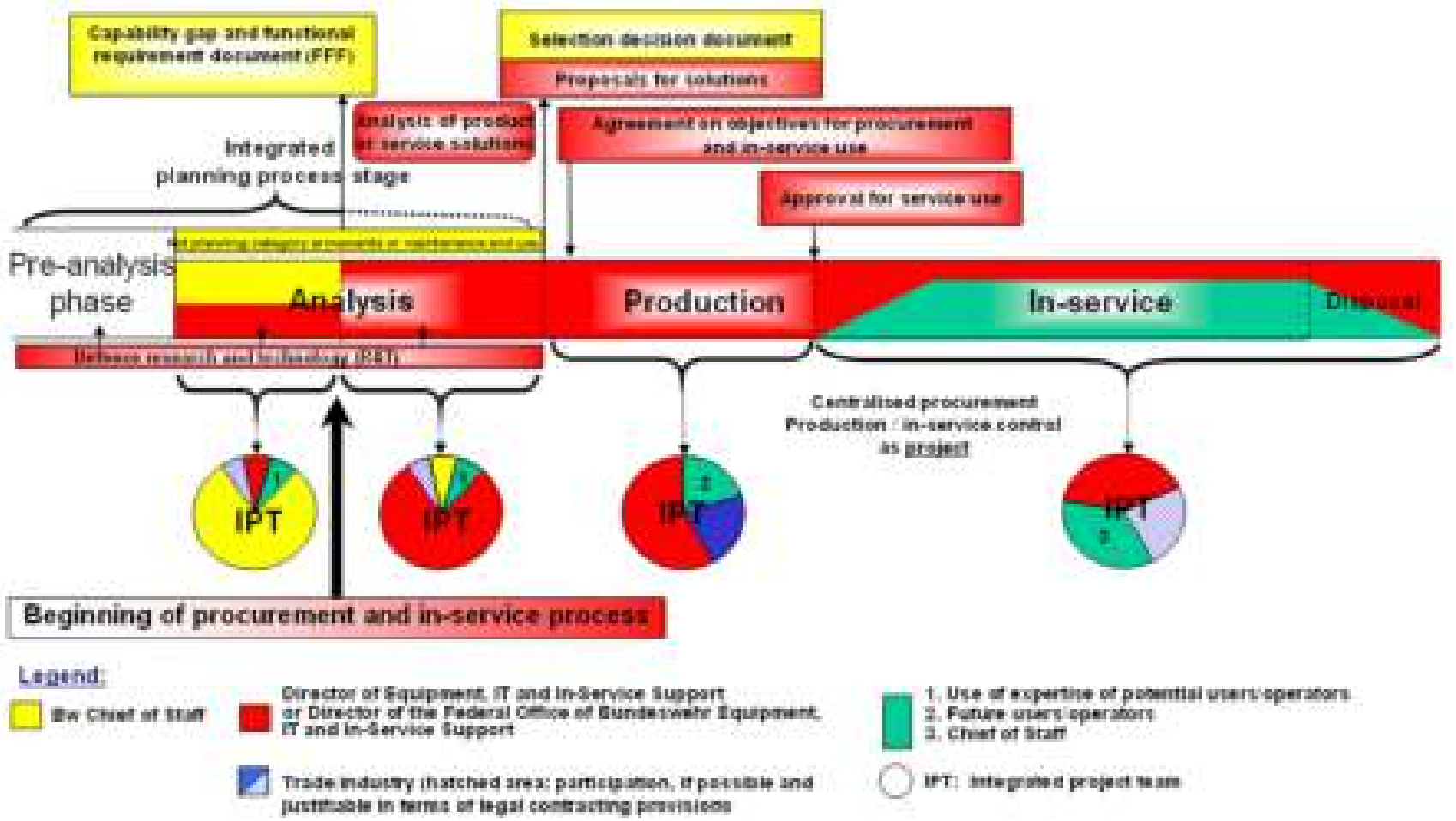

Figure 8: German Costumer Product Management Process for defence procurement

3.3.4 Contribution of DRIVER SP2 to the security innovation eco-system 2020

As described in the present document, DRIVER SP2 develops methods and infrastructure that support building a knowledge base at SoS level and help end-users and industry to assess the added value of solutions for further investment decision. We think that the three dimensional model, as used in DRIVER to describe the innovation eco-system's dimension **needed for proper innovation management in crisis management, can serve as a model also for Security innovation management on the whole.**

DRIVER aims at sustainably running these three dimensions, including the test-bed, and enable European scientific organisations to carry out certified experimentation and assessments. If DRIVER sustainability efforts are successful, end-users are enabled to base their investment decisions on actual knowledge about novel solutions and their effects on the overall crisis management SoS.

All three dimensions have to be able to run autonomously after DRIVER ended. One of the objectives of the project therefore is to create the necessary conditions for this.

3.4 Stakeholder Dialogue

The definition of the stakeholder dialogue that has to be performed in relation to the DRIVER test-bed and test-bed sustainability and that has, in the proposal phase for DRIVER, been envisaged to be part of WP21, had been thought through and further developed during the first phase of the project.

While some interaction with stakeholders has been conducted in the preparation of the present document (mainly discussions with CD&E experts from the military realm), some more while working on other SP2 work packages, it has also become clear that stakeholder discussion is a project task that has to happen across all DRIVER subprojects and not only in SP2 or WP21.

Thereby, one has to distinguish between two main areas of stakeholder interaction, one being discussions and knowledge exchange on dedicated capability development in the thematic areas in SP3-5, the other one being discussions and knowledge exchange on test-bed infrastructure (incl. methodology) and capacity development in general. The latter is to some extend inseparable from wider discussions with the community on test-bed sustainability, i.e. from the question on how to build methodology and infrastructure that provides positive impact for all stakeholders.

This being said, at this point two main dimensions of capacity development / test-bed related stakeholder dialogue – happening at different points in the project – can be identified.

1. General discussions on the need of an EU crisis management capacity building mechanism and the added value a crisis management test-bed infrastructure could bring. This discussion is happening at coordination level (WP13) with the involvement of SP2 (WP21, i.e. SP2 leaders) and SP7 (WP73 on test-bed sustainability) and SP8 (WP85 on analysis of potential business models for the sustainable test-bed).
2. Expert discussions on the different areas to be covered by the SP2 work packages: CD&E methodology in general; architecture; test-bed simulation, data recording and storage tools; methods for experimentation etc. These discussions are aimed at collecting expertise and knowledge from outside the project (form interviews and workshops) in order not to re-invent the wheel when developing the test-bed infrastructure.

For the preparation of the present document, expert opinion (interviews) with national military CD&E experts (Germany, The Netherlands, Poland[65]) and crisis managers with experience in questions related to innovation from several countries have been conducted.

Interviews were guided by the questions as given in section 2.4.1, but should be conducted as freely as possible at this point in order to be able to explore expert knowledge in the field of CD&E and innovation management in crisis management. Some experts also provided

[65] Note that the analysis of further countries was impossible due to time and budget constraints in task 21.2.

written contributions. The inputs and results are given in Annex I and have also been incorporated into different sections of the document.

Both kinds of stakeholder interaction (see above) are planned to go on and to be intensified as the project develops. Moreover, as soon as experimentation at the DRIVER platforms starts, different kinds of stakeholders and experts for different research questions will be an integral part of the activities.

3.4.1 Method

3.4.1.1 Structured interviews guiding questions for consultations of researchers of the CD&E community

1. Describe your level of experience with regard to
    a. experimentation approaches in the military domain (CD&E)
    b. experimentation approaches in the crisis management domain
    c. general innovation mechanisms in crisis management and civil protection

2. in case of 1a oder 1b: Describe your experience with regard to different components of experimentation
    a. concept development (what exactly?)
    b. experiment planning (what exactly?)
    c. experiment execution (what exactly?)
    d. experiment evaluation incl. specific methods, metrics and performance indicators definition (what exactly?)
    e. supporting tools: e.g. test-bed architecture, M&S, databases to support experimentation
    f. assessment of concepts on the basis of results; implementation of results into concepts (what exactly?)
    g. In the light of what you know about DRIVER, how do you think your knowledge could help the project to achieve its objectives
    h. What are the biggest obstacles for DRIVER to expect?
    i. What is essential to keep in mind for successful experimentation?
    j. What else can you tell us?
3. In case of 1c:
    a. describe the innovation mechanism(s) you have experience with
    b. In the light of what you know about DRIVER, how do you think your knowledge could help the project to achieve its objectives
    c. From your point of you: What are the biggest obstacles for DRIVER to expect?
    d. From your point of you: What is essential to keep in mind for successful experimentation?
    e. What else can you tell us?

4 Bibliography

[1] E.g. Mingers & White (2010) A review of the recent contribution of systems thinking to operational research and management science. European Journal of Operational Research 207 1147–1161; Thomé, Bernhard (1993). Systems Engineering: Principles and Practice of Computer-based Systems Engineering; Chichester: John Wiley & Sons. ISBN 0-471-93552-2; INCOSE. "What is Systems Engineering". Retrieved 2006-11-26.

[2] E.g. Lowe & Chen (2008): System of Systems Complexity: Modelling and Simulation Issues. SCSC '08 Proceedings of the 2008 Summer Computer Simulation Conference, Article No. 36.

[3] E.g. Lowe & Chen (2008): System of Systems Complexity: Modelling and Simulation Issues. SCSC '08 Proceedings of the 2008 Summer Computer Simulation Conference, Article No. 36.; *Meeting the challenge: the European Security Research Agenda.* A report from the European Security Research Advisory Board (ESRAB), Luxembourg: Office for Official Publications of the European Communities, September 2006 (http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf accessed 11 February 2015) last accessed 25 April 2015.

[4] Mostly taken from: S. Schäfer (2006) Concept Development & Experimentation – eine Einführung. Zentrum für Weiterentwicklung der Luftwaffe, Luftwaffenamt (Ed.).

[5] Often referred to as „Mission Capability Packages“ (MCP) that requires harmonised procedures for changes in different dimensions in order to improve overall performance.

[6] The Technical Cooperation Program: http://www.acq.osd.mil/ttcp/ last accessed 25 April 2015

[7] Website: https://mipsite.lsec.dnd.ca/Pages/Default.aspx last accessed 25 April 2015

[8] Website: http://www.dodccrp.org/html4/events_symposium_home.html last accessed 25 April 2015

[9] S. Schäfer (2006) Concept Development & Experimentation – Eine Einführung. Zentrum für Weiterentwicklung der Luftwaffe, Luftwaffenamt (Ed.).

[10] Further multinational cooperation programmes applying the CD&E method include the Nordic Defence Cooperation (NORDEFCO: http://www.nordefco.org/default.aspx) last accessed 25 April 2015

[11] Military decision on MC-0583, 2009: Military Committee for NATO Concept Development & Experimentation. North Atlantic Military Committee. NATO: http://www.act.nato.int/images/stories/events/2011/cde/rr_mc0583.pdf last accessed 25 April 2015

[12] Military decision on MC-0056 (2010): “NATO Concept Development & Experimentation (CD&E) process. Secretary General, NATO: http://www.act.nato.int/images/stories/events/2011/cde/rr_mcm0056.pdf last accessed 25 April 2015

[13] Contributing nations are : Austria, Canada, Czech Republic, Denmark, European Union, Finland, France, Germany, Great Britain, Hungary, Italy, NATO, Netherlands, Norway, Poland, Republic of Korea, Spain, Sweden, Switzerland Turkey, United States.

[14] Cf. https://wss.apan.org/s/MCDCpub/default.aspx last accessed 25 April 2015

[15] For individual projects refer to https://wss.apan.org/s/MCDCpub/Site%20Assets/1.MCDC_COA_Information_Sheet%281May14%29.pdf last accessed 25 April 2015

[16] Contributing nations are: Australia, Canada, New Zealand, United Kingdom, United States.

[17] For more details see http://www.acq.osd.mil/ttcp/overview/ last accessed 25 April 2015

[18] Note that, although there has been academic research on Security issues as well as industrial research on security ICT applications or on early detection of natural disasters, these activities have been scattered across the research landscape and have not been bundled to a specific application area before the year 2001.

[19] For the US crisis management system cf. section 2.2.4.

[20] Cf. also related discussion in DRIVER D13.2.

[21] European Crisis management Laboratory : (ECML) : http://lunar.jrc.it/critech/Activities/EcrisismanagementLEuropeanCrisisManagementLaboratory/tabid/99/Default.aspx last accessed 25 April 2015

[22] www.acrimas.eu last accessed 25 April 2015

[23] http://www.acrimas.eu/attachments/category/2/ACRIMAS_pilot%20case_report.pdf last accessed 25 April 2015

[24] http://www.fema.gov last accessed 25 April 2015

[25] http://www.fieldinnovationteam.org last accessed 25 April 2015

[26] https://www.fema.gov/media-library/multimedia/collections/270 last accessed 25 April 2015

[27] Message from Deputy Administrator Serino: Update on FEMA Innovation: https://www.fema.gov/information-employees/message-deputy-administrator-serino-update-fema-innovation last accessed 25 April 2015

[28] http://www.fema.gov/media-library-data/20130726-1911-25045-4786/2015_2019_administrator_s_intent_final508.pdf last accessed 25 April 2015

[29] Note that FEMA and DHS only occasionally join forces for capability development.

[30] http://www.dhs.gov/science-and-technology/our-work last accessed 25 April 2015

[31] http://www.dhs.gov/science-and-technology/hsarpa last accessed 25 April 2015

[32] Might be of interest to the work in DRIVER SP3: http://www.dhs.gov/science-and-technology/resilient-systems-division last accessed 25 April 2015

[33] http://www.dhs.gov/sites/default/files/publications/Research%20and%20Development%20Analysis%20and%20Assessment-Rio%20Grande%20Valley%20Systems%20Analysis.pdf last accessed 25 April 2015

[34] http://www.dhs.gov/science-and-technology/first-responders last accessed 25 April 2015

[35] http://www.dhs.gov/xlibrary/assets/st_dhs_nustl_strategic_plan.pdf last accessed 25 April 2015

[36] http://www.dhs.gov/st-activities-and-programs last accessed 25 April 2015

[37] http://www.firstresponder.gov/SitePages/Saver/Savers.aspx?s=Saver last accessed 25 April 2015

[38] Quote from WIMAAS web site: www.wimaas.eu last accessed 25 April 2015

[39] Quote from CONTAIN website: http://cordis.europa.eu/project/rcn/100574_en.html last accessed 25 April 2015

[40] Quote from SeaBILLA 's web site: http://www.seabilla.eu last accessed 25 April 2015

[41] http://www.secur-ed.eu/ last accessed 25 April 2015

[42] Quote from SECUR-ED's web site: http://www.secur-ed.eu/ last accessed 25 April 2015

[43] For a more detailed discussion of individual methods, please refer to deliverables of DRIVER WP23.

[44] http://www.sesarju.eu/ last accessed 25 April 2015

[45] Quote taken from https://www.eurocontrol.int/sites/default/files/publication/files/e-ocvm3-vol-1-022010.pdf last accessed 25 April 2015

[46] Cf. Also DRIVER D13.2 „Milestone 1 Report"

[47] www.acrimas.eu last accessed 25 April 2015

[48] http://www.eos-eu.com/EUfundedProjects/CRiSyS/tabid/303/Default.aspx last accessed 25 April 2015

[49] http://www.fp7-sec-help.eu/ last accessed 25 April 2015

[50] Note that the seemless integration of ACRIMAS results into DRIVER is not based on the structure of FP7 (cf. section 2.2.2.1), but was an accidental result of key-ACRIMAS-partners being also partners in DRIVER.

[51] ACRIMAS D7.3 „Contact database".

[52] Cf. section 2.2.1.

[53] http://www.demasst.eu/ last accessed 25 April 2015

[54] Adapted from SECURE-ED.

[55] DRIVER D13.2, p. 12.

[56] http://www.secur-ed.eu/ last accessed 25 April 2015

[57] The JRC platform has a specific role to develop a capacity for distributed experimentation..

[58] Cf. Also D13.2, chapter 5 "Subproject experimentation campaign 2 – SE2" and Annex I.

[59] http://driver-project.eu/ last accessed 25 April 2015

[60] DRIVER D13.2 „Milestone 1 Report", p. 12.

[61] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism:http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1401179579415&uri=CELEX:32013D1313 last accessed 25 April 2015

[62] SP2 and SP9 to coordinate on this.

[63] http://en.wikipedia.org/wiki/Innovation_system last accessed 25 April 2015

[64] Definition of the Oxford dictionary: A biological community of interacting organisms and their physical environment.

[65] One of the reasons why it is also difficult here to establish EU-level defence R&D co-operations or even procurement.

[66] Note that the analysis of further countries was impossible due to time and budget constraints in task 21.2.

Annexes

Disclaimer:

The information given in Annex I and II is for internal use and does not claim to be exhaustive. It will be updated during the project and can be regarded as work in progress.

4.1 Annex I: National military CD&E facilities

4.1.1 Germany

Point of Contact:

- **CD&E in the Planning Office of the Bundeswehr[66]**
- **CD&E in the Federal Office for equipment, information technology and Utilization Bundeswehr[67]**

4.1.1.1 General Description

The Ministry of Defence in Germany (BMVg) was restructured in April 2012. Two of the nine Departments, i.e. the departments "Planning Office" and "Federal Office for equipment, information technology of the Bundeswehr " **(BAAINBw) are the ministerial authorities directly related to CD&E process.**

The BAAINBw was founded on 01.10.2012 in Koblenz, after the dissolving of the "**Office of** Defence Technology and Procurement" (BWB) as well as the "F**ederal Office for Information Management and Information Technology of th**e Bundeswehr "(IT**-AmtBw) in September 2012.**

The BAAINBw is responsible for all actions for transformation, (Network Centric Warfare, CD&E, Modelling &Simulation, and R&T. It is supported by eleven service areas with eleven subordinate agencies. Two of service the areas are directly involved in the CD&E process: the service area P (Equipment Management and Strategy) and G (IT support). Additional there are two subordinate agencies: the "Wehrtechnische Dienststellen" WTD81 (Bundeswehr **Technology Centre for Information Technology and Electronics) and WTD91 (Bundeswehr Technical Centre for Weapons and Ammunition)**

The service area P, equipment management and strategy, is a key department. Here is the residence of the so-called "Equipment Location", where particular experiences of the military missions are integrated. Here is the interface to the planning authority formed, in which all new projects are initiated. There were strategic areas established, in terms of modern IT architectures or even topics such as cyber defines, research and technology or modelling and simulation. The team P1 monitors the implementation of the demands of the M&S and CD&E. In this context, at the beginning of 2008 the main activities in R&T for cross-sectional M&S were summarized in the SD VIntEL (System demonstrator Distributed Integrated Trial Landscape).

[66] http://www.planungsamt.bundeswehr.de/portal/a/plgabw/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9gpz0RCCVmFSSmplTmpeemodgx5voF2Q7KgIA2QI2eA!!/

[67] http://www.baainbw.de//portal/a/baain/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pMTEzDy9gqL8rNTsEr3klFT9gmxHRQBVgZcE/

From the international obligations implied claims, required system capabilities of the Simulation and Test Environment of the Bundeswehr (SuTBw) are derived. This project is in development and is a task of the "Centre for Information Technology of the Bundeswehr" (IT-ZentrumBw – service area G) located in Euskirchen. To this centre in Euskirchen is also appended the "Test and Analysis Centre" called which directly reports to BAAINBw. It emerged from the former Department 21 "System Test". Simulations for imaging and combination of virtual and physical reality belong to the main tasks of the Department TAZ. Here, the suitability of operational concepts and developed software is reviewed. The technical know-how on TAZ SuTBw was expanded and software tools for testing and quality management were introduced. Priority task are:

- The basic operation of the SuTBw infrastructure to networking of SuTBw locations at home and abroad, the coupling of real systems and platforms used there, both among themselves and with simulation systems in flexible trusted network associations
- Data recording and analysis system for the Bundeswehr common and standardized simulation and reporting forms
- Cloud Services: Unified Communications with Lync 2013 to NATO Secret, instant messaging and collaborative work, VoIP and video telephony, video conferencing
- PC-Cluster for Data Farming: experiment design, experiment execution, experiment analysis.

4.1.1.2 The SuTBW project

The SuTBw project was approved in 2005 by the Inspector General of the Bundeswehr and it was initiated on demand of a joint and centralized pool of cross-sectional systems, network infrastructure and technical services in support of M&S and Operations Research, which also requires a standing organisation, and another pool of fully trained experienced technical experts.

The SuTBw is geographically distributed nationwide. The simulation and test environment for the Bundeswehr is mainly a technical infrastructure, installed at various depot locations and simulation application of various types, but is mostly in military applications provided. On a SuTBw platform locally simulation models can be on the one hand developed and applied and on the other hand distributed over several test environment (SuT) locations, different HLA-based simulations and other applications in a cross-experimentation.

It uses several overarching Bundeswehr concepts (Network Enabled Capability, Communication and Information Systems, and Modelling & Simulation) and it is designed to support the accomplishments of the goals defined by NATO M&S Master Plan. The SuTBw community comprises about 45 organisations, commands and units. SuTBw operates exclusively RESTRICTED and SECRET networks based on SINA technology. SuTBw can establish simulation nets (DIS, HLA, and DIS/HLA), tactical nets and nets to facilitate

exchange of information between C2I systems and simulation systems. There are Constructive Simulation Systems specialized for Naval, Air, and Land joint scenarios. The Data Recording and Analysis Component contain applications dealing with monitoring, recording and analysis purposes. The different components communicate via gateways: standard gateway (DIS, HLA), gateways between simulation and Tactical Data Link networks and gateway between simulators and C2IS (Command, Control and Information Systems). A typical PC cluster for CD&E and Operation Research investigations is located at SuTBw in Euskirchen. Therefore several Data Farming applications are available on this Computer Farm. It can be triggered and operated from within any location in the Bundeswehr WAN and from the Internet through secure Secure Inter-Network Architecture Virtual Work stations. SuTBw contains four Operations Research (OR) support stations for support to ISAF operations. The OR software includes all necessary programs for daily work, like statistic software JMP, the General Algebraic Modelling System GAMS, etc.).

SuTBw disposes of collaboration systems for data and information exchange like MS Share Point, MS Exchange, MS Lync, or NATO Joint Exercise Management Module (JEMM), which can be used by all users accessing the Bundeswehr WAN.

The Test and Evaluation Centre (TAZ) uses the Microsoft suite with Window 7 clients, WINDOWS SERVER 2008 Rev2 and the 2010 System Centre Family. The migration to the next generation was planned for 2014.

4.1.1.3 VintEL system demonstrator

The System Demonstrator VintEL ("Verteilte Integrierte Erprobungs-Landschaft") contains **the main activities in the field of R&D for common modelling and simulations. It is an integrated test bed for a fast and effective evaluation of technical solutions in a realistic and operational environment. It is aiming at increasing the reliability and applicability of distributed simulations and strengthening the credibility of the simulation results.**

The concept for VIntEL is based on three pillars:

1) The architecture for coupling of the real, simulation and management systems, basic models and common services.

2) ABSEM (Agent based Sensor Shooter Modelling):

a) The basic models for the unification of time data from management, terrain, and objects with those of cross-sectional services.

b) Technical-Agent-based simulation with Data-Farming, which allows a variety of experimental runs.

3) Knowledge Management: it contains a collaboration tool in which all relevant data of the coupling simulation systems of the Bundeswehr are stored, a procedure model for the development of VIntEL test-bed and a service for initializing and versioning to ensure repeatability.

This project will be closed in 2015. Results and Experiences are supposed flow into the SuTBw process.

4.1.1.4 Links of the CD&E process to other departments

The Centre for Information Technology and Electronics (WTD 81) reports to the BAAINBw. It processes over all branches of the armed forces and systems issues of information technology. The tasks of the WTD 81 is divided into the testing and analysis of systems and equipment, R&T in selected research and technology fields as well as the professional technical input to projects in BAAINBw. The thesis topics are: information transmission and processing, information retrieval, and electronics. The "Centre for In**teroperability, Network Centric Warfare** and Simulation" (ZINS) is operating since March 2013. T**he "ZINS" is ideally suited for the execution of technical experiments, CD&E studies and subsequent presentation of the site investigations. The WTD81 is located in Greding (Bavaria).**

The WTD 91 (Bundeswehr Technical Centre 91) is located in Meppen and deals with the implementation of numerical simulations, such as the calculation on trajectories, taking into account weather data, etc. The focus of activities is the networking of simulators, real components and management systems based on standardized interfaces (High Level Architecture HLA).

The ministerial department "Planning Office" of BMVg contains four departments. The department four (IV) "Scientific support and interoperability" is divided in ten sub **departments. Two of these departments address directly the CD&E process:**

- "Department concept development, CD&E"
- **This department reviews the concepts with different experiments, for example, under laboratory conditions or in use. Number, type and scope of the experiments align themselves to the size and complexity of the CD&E project. For the experimental verification of several concepts scenarios for participants are to be developed to capture all facets of the experimental setup. The findings from the experiments are directly flowing back into the concept development. The scheduler Office of the Bundeswehr has two staff officers through a direct connection to the American Joint Staff in Suffolk (Virginia)**
- "Department experiment development and experimental procedure for CD&E"
- **This Department also supports the general education of the CD&E method and developed technical papers and publications. In experiments, the department controls and monitors the methods used by other services of the Bundeswehr. CD&E studies and concept ideas regarding a possible implementation and verification are evaluated in advance by experimental verification. The knowledge gained from the experiments conducted is evaluated by analysts of division IV of the Planning Office with independent scientific methods. They make recommendations for further actions.)**

4.1.1.5 Learning from SuTBw experience

Based on the SuTBw network architecture the Air Manoeuvre Tactical Leadership Training (AMTLT) was set-up. Various flight and fight simulators, Computer General Forces (CGF), the current Army C2IS and the "Serious Gaming Software" Virtual Battlespace 2 (CBS2) are utilized in distributed simulation. The "Air mission Commander" pilot course conducted in **2011 showed that the set-up allows the full mission training in complex scenarios without the need of real life flight operations.**

Another Training conducted in 2011 was Joint Air Defence Synthetic Training (JADSynT), which was designed to prove the Concept of Federated & Virtualized Training for Joint Air Defence and to evaluate the utility of new SuTBw components. Virtual missions were successfully conducted and SuTBw provided an infrastructure up to NATO SECRET with network entry points at several locations in Germany and the USA. SuTBw provides tools and permanent network services including OR Cells and reach back elements in Germany. The OR Cells uses one of the four Research Support Stations which belongs to SuTBw. These stations have high end performance IT hardware components and a wide spectrum of software package for analysis, like the statistic software JMP, the General Algebraic Modelling System (GAMS), Arena, Eclipse, MS Office Suite, Mind Manager and Share Point 2010 for communications between OR personal in theatre and back to Germany.

The user community of SuTBw is growing fast and there is a high demand for Network & Simulation Support of Joint Training & Exercises and pre-development workups. That means it is an increased need for secure network support and an increased complexity of supported activities across all services.

4.1.1.6 Requirements for the Architecture of the Test-Bed

The main general requirements are:

- **Reliability of the simulation results**
- **Reusability of simulation systems**

Other general requirements are:

- **Performance**
- **Scalability**
- **Components implemented in different languages can be joined to the architecture**
- **Components can be distributed spatially**
- **The existence of an error management**
- **Operations can be conducted asynchronously**
- **Components have an interface for the initialization of data**

Special requirements:

- A service to deliver environmental data of any kind (like GOIS)
- A communication of effects service (CES)
- A weapon effects service (WES)

The ability of these services to be called by other services should be provided.

Simple said the architecture contains a set of services and a set of real systems which are connected through various nets to the set of simulation systems.

- The application dependent services are e.g. data collecting, storage and analysis, modelling the environment and modelling physical processes. Technical services are dealing with the interconnection between the systems.
- The set of real systems contains model coupling and Commando and Control (C2) simulations.
- The simulation system maps a piece of reality onto a model.

A series of experiments was conducted to prove the applicability of the reference architecture, which used following components:

1. Simulation Systems:
    - Constructive simulation Agent-Based Sensor.Effector Modelling (EADS) and PABST (IABG)
    - Virtual vehicle simulations GeneSys and GenPlatSim (both IABG)
    - Virtual target simulation dome at WTD81 in Greding
2. Services
    - Geo-referenced environment service GOIS (IABG)
    - Communication services KESS (Thales)
    - Weapon effects service WES (IABG)
    - GEPARD proxy (gateway between anti-air-tank GEPARD an High Level Architecture (HLA) Simulation)
    - Recce-proxy (gateway between MIP DEM and HLA)
    - C2SimProxy (gateway between Multilateral Interoperability Programme Digital Elevation Model and HLA)
3. Busses
    - Simulation bus: HLA with MÄK RTI v3.x or PITCH pRTI[68] v3.x
    - Service bus: HTTP/SOAP
    - Data bus: XML over TCP7IP for synthetic environment and STANAG 4609 for video data
    - Tactical bus: MIP DEM
4. Real Systems:

[68] RTI that support all HLA versions (Pitch RTI)

- Anti-air tank: GEPARD (German anti-air tank).
- Reconnaissance systems: AMFIS (evaluation of UAV data)
- C2-system: FIS-H (C2-system of the German Army)

The conducted experiments showed that several constructive and simulation systems have to be adapted to the use of services and that the services could be reused across the experiments. Moreover, it was established that it is very useful for some specific experiments to reuse the whole architecture.

4.1.1.7 Learning from VIntEL experience

Distributed Integrated Testing Environment is for DRIVER a central aspect. Distributed Simulation experiments have high complexity on both the technical and at the organisational level. The experience gained with VIntEL especially the technical implementation, the analysis support and best-practice guides are relevant for DRIVER. VIntEL and also DRIVER allows to bring together technical and special experts in order to assure a continuous and consistent top down flow of information (regarding new scenarios, new concepts of operations and corresponding requirements) and bottom up flow of information (regarding restrictions, environmental conditions and alignment of solutions).

The first VIntEL experiment took place in October 2004. The Simulation System was built of several virtual platform simulators and real systems aiming to investigate the performance of unmanned reconnaissance vehicles in atypical experiment. The System was distributed over four locations. Only in six weeks the systems were bound together using the PSISA[69] middleware to create HLA interfaces. Two different Run Time Infrastructure (GERTICO and DMSO) were used and a subset of Real-time Platform-level Reference Federation Object Model (RPR FOM). The middleware PSISA played a key role for the quick generation of the VIntEL [Neugebauer –An Env].

The basic concept of DS VIntEL contains four sub concepts: Architecture, Organisation, Procedure Model, and Information Management [Fig. 1]

Procedure VEVA 2

The procedure model for the use of VIntEL architecture (VEVA 2.0) was developed at the University of the Bundeswehr Munich. It includes both theoretical and practical experience in building distributed simulations [Alexander Laux]. The model VEVA 2.0 has the claim of universality, and thus the applicability is not restricted to VIntEL. The theoretical foundations are mainly the "Distributed Interactive Simulation" (DIS) standard, "The Guide to Model **Documentation "(LMD), the" Distributed Simulation Engineering and Execution Process "(DSEEP) and VEVA. Practical experiences have been found in the use**

[69] Proposed Standard Interface for Simulation Applications

of VEVA and served as input to VEVA 2.0.

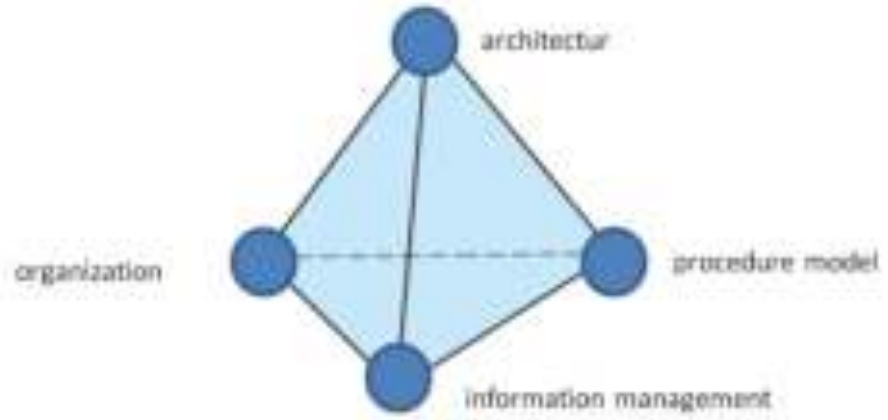

Fig.1 Classification of the process model as one of four functional sub concepts of SD VIntEL basic concept

From interoperability criteria an actual checklist is derived. These criteria have to be identified, structured and integrated in the VEVA.

The first phase of VEVA 2.o is the "Goal Definition" and has to specify the objectives of the **simulation environments. That means also the resource assessment, frame conditions; work on scenarios, quality requirements, planning of experiments.**

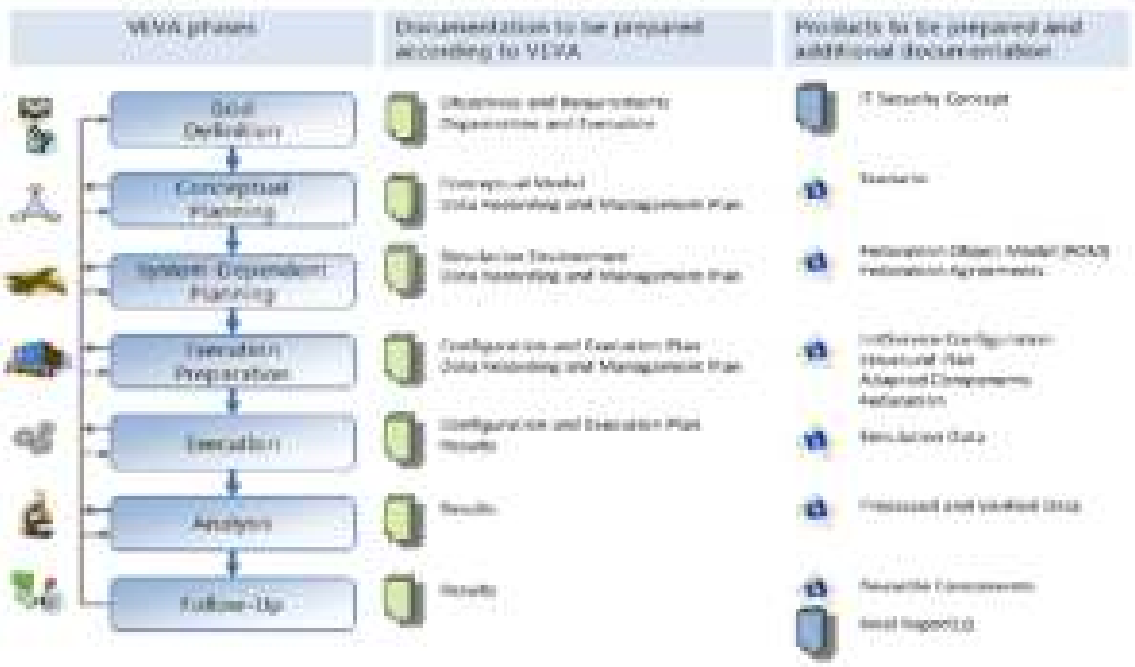

Fig.2 Phases, Documentation and Products of VEVA 2.0 (VIntEL)[70]

[70] NATO RTO-MP-MSG-087: How to ensure fair fight in LVC Simulatio: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDYQFjAD&url=http%3A%2F%2Fwww.ibrarian.net%2Fnavon%2Fpaper%2FHow_to_Ensure_Fair_Fight_in_LVC_Simulations.pdf%3Fpaperid%3D19011781&ei=BFbHVNvMEMmrU4ecgWg&usg=AFQjCNHBQyXfiZugD1JcaLRcU75bVO3mVQ&bvm=bv.84349003,d.d24

The second phase is the conceptual planning. First of all a capability analysis will be performed considering the capability requirements, the communication and interactional relationships.

In Phase 3 ("System-Dependent Planning") the actual simulation systems have to be selected **and the data exchange model has to be developed. A feasibility check follows to carry out an explicit Verification and Validation, focusing on fire fight effects. The implementation analysis will then specify which objects/capability would be implemented as services or real system or simulation system. The timing analysis will develop a timing model for the system to be investigated.**

The "Execution Preparation" (phase 4) deals with setting up the simulation environment and **integrating all participating systems, identifying possible problems and sorting them out before executing the simulation environment**

During the Simulation execution phase (5) all simulation runs are monitored and possible problems recorded.

The Analysis (phase 6) provides an activity "plausibility check" which is dedicated to **analysing the simulation results to find out whether the data are suitable for analysis and interpretation.**

In the last phase "follow up" the problems documented and the possible solutions are to be **documented. The body of knowledge regarding the identified problem at the Phase 1 will be generated or updated.**

4.1.2 The Netherlands

4.1.2.1 General Description

Concept Development & Experimentation

The basis of CD&E is stimulating creativity and innovation by experiencing new ideas and concepts. Thinking and doing are combined in an interactive process with experts and the customer. This creates a change in mind-set, as well as insights. By using results from brainstorm sessions, evaluations and experiments, a widely supported concept is developed which describes a solution for the problem at hand. By capturing the insights in a *concept document*, a robust framework for the final solution is created. Due to this procedure, the quality of the final solution is often much higher. Furthermore, the requirement of acquisitions for new functionalities can sometimes disappears and changes in organisations can become more effective. The concept document is very important during the implementation of the final solution.

Advanced Concept Development & Experimentation Environment

Testing new technologies and concepts by the Department of Defence in a real/live environment is extremely costly: it requires deployment of lots of personnel and material. TNO therefore developed 'TNO ACE' (Advanced Concept Development & Experimentation **Environment), a virtual world in which methodological experiments can be performed with, for example, new weapon systems. This can save the Department of Defence a lot of time and money.**

Components and facilities

TNO ACE offers a variety of rooms on different TNO locations. The rooms vary from application specific environments to generic environments that are expandable with powerful simulation and analysis tools. The TNO ACE rooms can be linked together via a (voice / video / data) network. This also includes the possibility to link to the Public Internet, Dutch defence networks, and NATO networks. Some of the rooms are accredited for working with classified (NATO Secret) data.

Fig. 3 Generic TNO ACE room

TNO ACE tools include:

- collaboration tools,
- constructive and virtual simulators,
- simulation infrastructure tools,
- tactical data links,
- Command & Control systems (sound, video, simulation data) recording tools,
- simulation data analysis tools,
- 2D/3D simulation data visualization tools,
- terrain databases.

4.1.2.2 Examples

Over the years TNO has supported the Dutch MoD and NATO in numerous experiments utilizing the TNO ACE facilities and components. Examples range from brainstorm sessions for the exploration of new concepts, to fully fledged distributed Computer Assisted Exercises (CAX).

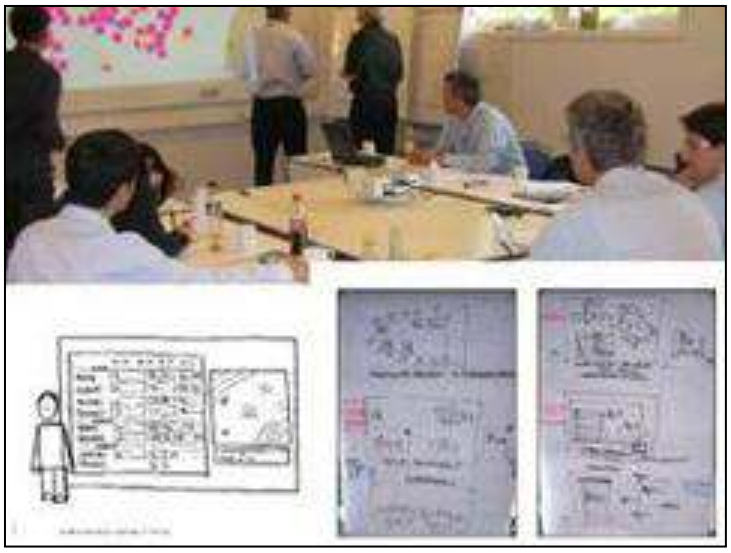

Fig. 4 Brainstorming to explore concepts

Fig. 5 Evaluation of new concepts in exercises with the use of simulation

4.1.2.3 Relevance for DRIVER

The TNO ACE design, workflows and hands-on experience can be used in designing the DRIVER Test bed architecture and required services.

4.1.2.4 Practical issues

The TNO ACE facilities and components are in principle available for DRIVER experiments. Depending on the experiment, the layout of the ACE rooms can be adjusted to the needs of the experiment. Also components can be configured to the needs of the experiment.

Furthermore, it is possible to install operational systems in the ACE rooms, that can be connected to a DRIVER exercise VPN.

What could be the added value for the facility of hosting DRIVER experiments?

TNO ACE is designed to host CD&E events in the military domain. Experience and lessons learned in designing tools that support brainstorm sessions and creating Live, Virtual Constructive distributed environments over secure communication lines can be very beneficial for hosting or participating in DRIVER experiments. The existing infrastructure and the availability of personnel skilled to operate the TNO ACE facility can support DRIVER experiments efficiently and effectively.

4.1.3 France

Point of Contact

- *Tata Consultancy Services France (TCS)*[71]

4.1.3.1 General Description

The French CD&E mechanisms for defence are orchestrated through different organisations of the Ministry of Defence into a coherent approach.

We only insist in this chapter on (i) the Joint level and (ii) the LTO, and we then focus on (iii) CD&E process and a rapid survey of (iv) some available tools.

The Joint Forces Centre for Concept Development, Doctrine and Experimentation (CICDE - Centre Interarmées de Concepts, de Doctrines et d'Expérimentations) – created in 2005 – is installed on the site of the Military School in Paris. Its role is to design joint forces concepts and doctrine development, in a spirit of creativity and reactivity, with use of experimentation as soon as necessary. The CICDE represents a strategic and influential hub and a key player in the general evolution process. It is part of the transformation network in company with allied centres (ACT, US JFCOM, DCDC,…).

Used when a quick solution to an urgent operational requirement is needed or when the issue dealt with is complex, the "experimentation" or "CD&E" approach results in **recommendations relative to the different support structures, concepts and doctrines, as well as equipment, education and training. Experimentations are conducted within a national or international context: operations, exercises, battle-labs, technical and operational laboratories, etc.**

The Technical-Operational Laboratory (LTO - Laboratoire Technico-Opérationnel) is co-piloted by the DGA (Direction Générale de l'Armement **- the French procurement agency and Army operational research centre) and the Etat-Major des Armées (EMA). It contributes to support decision of definition of future weapon systems implying (technical, operational and economic) choices. For that purpose, it allows to perform experimentations which regroup personnel from Forces, Program or Capability managers, technical experts and possibly industrials (when necessary). The objective is then to study in a cooperative way needs, constraints, technical possibilities, organisations, tactics, techniques and procedures, and concepts of operations /of employment / of use of future military capabilities and of the weapon systems which are part of it. After collective discussions and reflexions, candidate options are tested using resources of modelling & simulation, including Serious Games, before been experimented through hybrid frameworks mixing simulation and real systems.**

[71] **http://www.tcs.com/worldwide/europe/locations/france/Pages/default.aspx**

The CD&E process deployed by the LTO is the following:

- **Sharing experience: What are the real requirements? This first phase must provide answers to that question. The working method is simple. It involves developing these** requirements fully by sharing all parties' experience and technical and military **expertise. Computer-assisted brainstorming and creativity sessions (workgroup laboratory) are organised for that purpose.**
- **Formalising the requirement: Next, the requirement is specified. It is formalised by describing it in greater detail and providing specific information on potential technical solutions. At this stage, the main task is to provide large organisational or system architecture models.**
- **Analysing the options: Do the options address the initial requirement? Ti answer this question, these options must be tested in simplified simulations based on actual use, using table-top or role-playing games.**
- **Verifying performance: the major technical-operational options for the future are determined. Their overall performance must now be verified. Capability simulations that take physical phenomena and behaviour into account on a macroscopic scale** will reveal the future system's potential performance.
- Testing against planned use: The future system's performance has been verified. **However, technical performance is not the only consideration. The next step is to confirm that its concepts of use will be appropriate for future military users. The future system must be able to be implemented simply, quickly and efficiently. The concept and the technical solutions must thus be tested in concrete scenarios of use. This is done by using technical-operational simulation tools or representative demonstrators.**
- **Experimenting with man in the loop: This last phase involves real-world testing of the solution(s) in the field. This means obtaining feedback before the product even exists. The process thus involves conducting full-scale experiments that combine the virtual world and the real world by combining demonstrators and military exercises in the field.**

The French MoD tools supporting CD&E can be declined put in relation with the type of simulation / experimentation which is targeted:

- *live simulation* **(real systems exploited by real operators). This encompasses individual simulators and collective ones supporting experimentation and interconnecting dedicated devices (ex: CENTAC/CENTAURE or CENZUB/SIMULZUB)**
- *constructive simulation* **(simulated systems are exploited by simulated or real operators). Mainly concerns simulation for Command & Control systems (wargames are part of it) (ex: JANUS or SCIPIO).**

- *virtual simulation* **(simulated systems are exploited by real operators – ex : OPOSIA), and** *embedded simulation* **(training simulators embedded in real equipment of systems) which are not illustrated here.**

In the focus of simulation for experimentation, the Ministry of Defence has developed different assets, among which are the following (from the DGA or the French Army):

- **the Combat Training Centre (CENTAC -** Centre d'entraînement au combat) located in **Mailly-le-Camp, is dedicated to train and control Army forces (SGTIA - units combining all operational functions) to manoeuvre and tactical reflexion. During 4 days, soldiers fight against a real manoeuvring adversary. Objective is to provide instantaneous evaluation of the level of the trainee units in mastering their tools, methods, doctrine and capacities in situation of stress. CENTAC uses simulation for weapons effects and performs coordination and analysis through a centralised information system (CENTAURE).**
- **the Urban Operations Training Centre (CENZUB -** Centre d'entraînement aux actions **en zone urbaine) consist in a complete instrumentation of the combat village of Joffrecourt. Supervision and control is guaranteed by the centralized system CERBERE (Centre d'entraînement en zone bâtie et de restitution des engagements).**
- **JANUS France (French version of the US platoon-to-brigade level combat simulation) can simulate operational functionality of all types. The interactions between systems as well as the impact of the battlefield environment on acquisition and engagement are represented at a high level of fidelity. Janus performs interactive (actual, real-time interplay between the personnel who perform the command decisions and the simulated units and systems they control), six-sided (up to six friendly and/or enemy forces can be represented), closed (the sides/forces in a scenario do not have perfect knowledge of other sides/forces), stochastic, ground combat simulation. The forces are simultaneously directed and controlled by a set of players or gamers for each side who only have knowledge of enemy units that are in direct observation by one or more of their subordinate units. Additional intelligence from other sources may be available if the appropriate C3 nets are represented. Janus is played on a computer-generated digitized terrain map. Currently, Janus is used extensively for military training, combat development and analysis, and operational test and exercise driving applications. The Saumur Military Schools Simulation Centre allows to train up to 400 simultaneous trainees. JANUS France allowed a simulation exercise in case of flood in Maine-et-Loire (France) dedicated to definition of procedures (evacuation,** commonality of resources from Department and Cities…) to integrate in the flood **rescue disposal.**
- **SCIPIO is the first national training tool for HQs. The SCIPIO requirement originates in a major advanced study launched by the French MoD at the turn of the century to explore available technologies for Army distributed training to combat operations on**

the digitized battlespace, and its impact on doctrine. The requirement then evolved to a full command training capability. SCIPIO emphasizes the reduction of preparation and training resources, prepares Army units to the use of command & control information systems, and introduces advanced simulation software agents, such as decision models to animate subordinated tactical units, offering faithful replication of tactical decision-making and manoeuvre for companies and below. These agents follow doctrine and develop automated situational awareness in their synthetic environment (terrain, enemy, mission and resources). Initially designed for conventional, high intensity warfare, SCIPIO today encompasses new operational requirements, such as operations other than war and asymmetric warfare in complex, mostly urban, environments, and provides a full scope of combined, digitised Army operations over the current peace-crisis-war continuum.

Most of these assets (as well as a lot of others more dedicated to constructive and virtual simulation) are interconnected through a specific network using a dedicated technical M&S infrastructure: ITCS (ITCS - Infrastructure Technique Commune dédiée à la Simulation pour l'acquisition).

4.1.3.2 Relevance for DRIVER

Over the fact that a possibility may exist to use some of the above mentioned assets (to be negotiated case by case), the DRIVER Project may benefit from this huge amount of experience in the field of CD&E in terms of expertise, know-how, skill and information regarding such domains as:

- **methodology,**
- **methods,**
- **specification of experimentation testbed** (services…) – **through experience from DGA / ITCS**
- **implementation technology for hybrid experimentation**
- **return on experience, business rules and best practices in experimentation.**

4.1.4 Poland (ITTI)

Point of Contact:

- **National Defense University, Warsaw, Poland**[72]
- **E-Technology and Business Poland (ITTI)**[73]

4.1.4.1 General Description

In what follows, the capabilities dealing with planning, organizing, and conducting experiments connected with military and non-military threats are described. It should be emphasized that the systems described in this elaboration are not only fully operational, but above all are exploited during exercises and trainings. This concerns both a didactic process with students as well as services provided for governmental and nongovernmental organisations.

The National Defence University (NDU) permanently carries educational and research activities and this fact can be the main obstacle to fulfil some of requests of the DRIVER projects. Thus, it is crucial to determine in advance the terms and range of all DRIVER actions involving NDU with its local coordinator. Due to a specific role played by NDU, every test and experiment should be in accordance with the University schedule. Nevertheless, NDU is willing to take an active part in this extraordinarily interesting project because it is not only the largest CM European project, but mainly because the profile of NDU activities is strictly connected with the subject of DRIVER.

ITTI's main contact at NDU:

Andrzej GLEN, Associate Professor, Vice Rector for Science and Research

4.1.4.2 Part I – FACILITIES

4.1.4.2.1 War Gaming and Simulation Centre (WG&SC)

War Gaming and Simulation Center (WG&SC) is located at the National Defense University (NDU). Shortly speaking, the WG&SC provides facilities and equipment needed to conduct computer assisted exercises (CAX). The Center cooperates with both university faculties, but its service for the Polish Armed Forces is crucial. Furthermore, its cooperation with the NATO members is of significance as well.

The overall goal is to train military leaders and his/her staff on the levels of brigade, division, corps, and operational command. This is done in most cases by CAX's on one or more levels,

[72] **http://www.studies-in-poland.pl/s/2333/57926-Studies-in-Poland/466-National-Defence-University-in-Warsaw.htm**
[73] **http://www.itti.com.pl/english/about.html**

with one or more parties. CAXs are used to maintain readiness, providing a flexible method for training commanders at all levels of warfare. As with any exercise, a CAX must have specific objectives, be properly planned in advance, and be executed in a controlled environment. CAX realistically simulates the capabilities and limitations of armaments, people, and environment. It is excellent for exercising tactics, techniques, and procedures for units. CAX is a mix of simulation systems that places the commanders and staff in an operationally realistic environment in order to not only execute decision making, but also practice operations and coordination between headquarters. Dynamic aggregation and disaggregation of units during the game is allowed in CAX, so different echelons can be trained by users.

The main tasks of the WG&SC are as follows:

- organising pre-exercise training events, conferences, courses for operators;
- planning and technical support expertise;
- operational analysis for the participants;
- new command ideas research;
- modelling and simulation development;
- defining of training objectives;
- design of an exercise to meet the training objectives;
- developing scenarios that will lead the training audience toward accomplishing of objectives;
- maintaining and managing simulation systems, IT equipment, communication networks, and databases.

The remaining tasks of the Centre cover:

- compiling the catalogue of threats;
- collecting information about CM sources;
- building databases of crises management sources;
- building scenarios for exercises;
- providing trainings and exercises (experiments) with CM teams (at different levels);
- launching of the CM procedures (during training and exercises);
- monitoring of potential threats during exercises (experiments);
- collecting important data for an afterwards exercise analysis;
- presenting collected data at different levels of details;
- providing analysis of what happened during exercises (experiments);
- implementation of new tasks (procedures) in the field of CM and critical infrastructure protection during trainings and exercises (to find optimal solutions).

WG&SC lab technical design

Facility's scheme

The Center infrastructure consists of 37 rooms used for CAXs. 400 players can be supported in one shift. There are 5 floors and a basement in the building. The ground and 1st floors are designed mostly for offices of the staff. The remaining 3 floors include war gaming and exercise control areas. On each floor there are war gaming halls, briefing rooms, and working rooms; see Figure 1.

Fig. 6 WG&SC lab design

Stationary and distributed CAX are distinguished. They differ by the choice of location for the elements and an important factor is a location of the low commander (LOCON) units. Common to both kinds of CAX are (i) the central location of control and directory staff (DISTAFF), mainly at the WG&SC and (ii) that the exercising command posts (CPs) have no access to the simulation.

Figure 2 below shows an organization of a stationary corps level CAX, training on two levels of command in an one party exercise. Except from the player units, these are the CPs on division and brigade level, all other elements like DISTAFF with exercise controller (EXCON), high level commander (HICON), WHITE CELL, opposite force (OPFOR), EVALUATION and the units of LOCON, are located within the centre.

Fig. 7 Stationary CAX

A schema of a distributed CAX is shown on Figure 3. The trained CPs as well as the LOCON units are located in the field. Connecting two or more simulations, so that they pass information to each other and interact with each other, leads to a distributed simulation. However, distributed does not necessarily mean that the simulations must be separated by large distances. Two different levels of abstraction are possible for distributed simulation implementations. For example, Joint Theater Level Simulation (JTLS) as a highly aggregated level model and *Joint Conflict and Tactical Simulation* (JCATS) as a high resolution model running at different geographic locations in a distributed manner. The major challenges of this kind of exercises deal with an overall exercise control: what is happening in various simulations? how can it be combined into a single view?

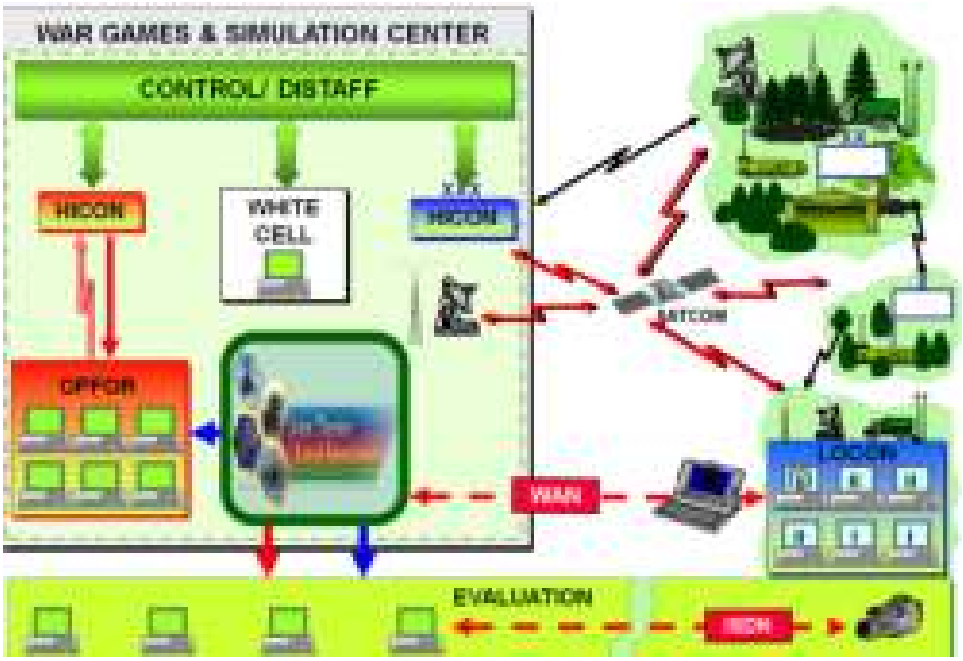

Fig. 8 Distributed CAX

Equipment specification

- over 200 PC's;
- 70 laptops;
- 9 servers;
- 25 network printers;
- multifunctional printers;
- 1 graphical station.

Software specification

- JTLS 4.1.7 – The Joint Theater Level Simulation (JTLS®) is an interactive, internet-enabled simulation that models multi-sided air, ground, and naval civil-military operations with logistical, Special Operation Force (SOF), and intelligence support. Moreover, it can also model crisis situations;
- JEMM 2.7 – Joint Exercise Management Module is a module used to prepare major events and incidents and steer the execution phase of an exercise towards its goals. It also collects data for After Action Review (AAR). For each incident the response and factoring parameters are selected, e.g., aircraft loses, time, and number of combat air patrol missions. JEMM collects and sends this data to the analysis module. Moreover, the module provides an interfaces for EXCON staff to enter the observations on the reactions of training audience to each incident. These records are then analysed for the AAR;

- IGeoSit – The Interim Geo-Spatial Intelligence Tool, is a situational awareness tool developed by NATO Communications and Information Agency (NCIA) and used widely within NATO. IGeoSIT consists of a web-enabled Java server client and a central server, running Apache and Tomcat. IGeoSIT servers respond similarly as ArcGIS, and other GIS servers, to WMS requests. It contains requests for data layers, opacity, and different base maps. IGeoSIT clients are used by analysts and operators to geospatially reference events or perform terrain analysis;
- ArcGIS 10.2, PGO2014 are geographic information systems for capturing, storing, checking, and displaying data related to positions on Earth's surface. ArcGIS and PGO2014 can show many different kinds of data on one map. This enables people to more easily see, analyse, and understand patterns and relationships;
- Oracle 11g – Oracle Database is an object-relational database management system;
- Edius 7.0 is versatile real time editing software – 4K, 3D, HD, SD and almost any format from 24x24 to 4Kx2K, all on the same timeline, even in nested sequences, all in real time. It is a tool to broadcast news, news magazine content and studio programs, as well as corporate, documentary, and 4K theatrical productions;
- LimeSurvey is an open source tool for online surveys;
- Cent OS is a server operating system;
- Microsoft Windows 7 is an operating system.

4.1.4.2.2 CBRN defence Training Centre

Description

CBRN Laboratory is an integral part of the CBRN Defense Training Centre. The main purpose of the Laboratory is to provide facility capable to host trainings and experiments events related to modelling and simulation of chemical, biological, radiological, and nuclear (CBRN) hazards. The Lab is focused on education and training of military personnel, however, civilian audience is also welcomed. In reference to the national approach on CBRN warning and reporting, the trainings and experiments organized in the Lab are related to binding both issues to enhance cooperation and provide common understanding of CBRN hazards' **complexity. The Lab staff introduced an innovative approach to crisis situation management. A strong point of the platform behind it is the combination of JTLS software results provided by War Gaming and Simulation Centre with HPAC and BEAM software outputs which are owned by the Lab.**

Concept development depends of composition (assignment) of a given training audience or requesting authority needs. A training/experimentation platform (hardware and software) is provided to conduct individual or team trainings followed by exercises to test and evaluate personnel and/or procedures. Final results are to confirm or deny correctness of existing solutions and (possibly) propose ways of improvements to be introduced in the Polish Armed Forces or civilian institutions.

An example of an experiment is the case study of CBRN release involving the first responders and military support to face terrorist attack during a mass event like UEFA European Football Championships. The aim is to check consistency of procedures, detection capability, command and control, equipment compatibility, decontamination efficiency, communication and services interoperability. Specific methods, metrics and performance indicators are adjusted to an audience and are set by an experiment control staff. Supporting tools belong to CBRN M&S and information management categories.

The offered scope of events cover CBRN releases resulting from:

- **CBRN incidents (in accordance with NATO ATP-45);**
- **chemical, biological, nuclear facilities;**
- **CBRN weapons;**
- **missile interception with chemical/biological payload.**

Expected outcomes may be related to:

- **information flow;**
- **warning and reporting effectiveness;**
- **CM after major/local CBRN incidents;**
- **human medical effects;**
- **toxicity levels;**
- **contaminated areas;**
- **population exposure;**

- hazard areas and evacuation planning;
- casualties estimation.

Achieved results of experiments may help to better understand the complexity of CBRN hazards and required combined efforts of military and civilian services to mitigate their effects on military operations and population. Additionally, they may result in CM plans review and adjustment.

CBRN Lab technical design

Laboratory's scheme

Figure 4: CBRN Lab.

Equipment specification

- 15x PC: Dell Optiplex 9010 MT with 2 monitors: Dell P1913 & NEC PA241W;
- 2x graphic stations Dell Precision T7600 with 2 monitors: NEC PA241W & NEC PA271W;
- 3x 55 inches monitors Samsung PE55C (one with touch capability);
- 3x projectors NEC P420X;
- 2x printers KYOCERA FS-2100DN;
- 1 plotter EPSON SC-T7000;
- 1 multifunctional device KYOCERA TaskAlfa 3050ci;
- 1 server Dell PowerEdge T620.

Software specification

- server: Microsoft Windows Server Small Business Standard;
- PCs: Windows 7 professional;
- expert software: HPAC 4.04 (DTRA/OPTIMETRICS) and BEAM 3.0 (POL MOD).

CBRN Lab utilization for DRIVER purposes would bring the proper understanding of CBRN risks to community to identify gaps in existing response systems. The obstacle could be the lack of standing evaluation parameters which depend on experiment/training requesting authority. An essential issue is a clear goal to be achieved helping the staff to design experiment and evaluate its result effectively.

4.1.4.3 Part II – EXPERIENCE

National Defense University contains two faculties, namely Management and Command Faculty and National Security Faculty, and at each of them there are experts having an extensive experience related to various CM-related issues, both in military and civil domains. The experience originates essentially from the two main activities at the University, i.e., education and research. To fulfill the mission of the University, which is to prepare military and civilians to evaluate and solve strategic dilemmas connected with national and international security challenges and threats through educational and multi-disciplinary research programs, NDU participates actively in the works over the following issues:

- National Security System;
- integrated system to create CM plans;
- new informatics technologies;
- interactive training psyhosymulator for Police;
- methodology of risk estimation for CM system in Poland;
- tools for assessing an effectiveness of the solutions for internal security.

The educational and scientific activities at NDU are focused on preparing a theoretical basis and developing CM knowledge, organizing and functioning of a national CM system, and on using armed forces and units in a context of challenges, chances, and risks to security of Poland. It is clear that the activities within education and research are closely linked, for some solutions developed at NDU (or with cooperation of its employees) were kindled by the needs resulting from the educational activities, and – needless to say – the solutions available at NDU are extensively used during courses, training, exercises, and experiments organized by the University.

The educational activities of the University are concerned mostly with courses, trainings, exercises, and experiments organized regularly for the students of NDU, but also upon request from external (often civilian) entities. The aim of the courses is to acquire knowledge, skills, and mould predispositions of their participants to prevent and respond to crisis situations, train rational functioning during a given situation, eliminate its effects and to prepare a national and local administration to manage people in a case of a thread.

Research and development activities at NDU are focused on introducing new solutions to deal with crisis situations. An important part in elaboration of new solutions is played by a

cooperation between NDU and TELDAT, a Polish business entity which has been present on the market for almost eighteen years. It is a leading constructor and producer of the world's most innovative data communication solutions. The company has been involved in research and development, design, production, implementation and maintenance (including remote supervision) of specialized electronic, data communication, IT, telecommunication and alarm systems and devices dedicated mostly to security, national defense, and CM. Its products (both hardware and software) and services (research, development, implementation, and maintenance) have been successfully used and tested during multiple national and international exercises, and exploited in real military missions.

One of the outcomes of the cooperation between NDU and TELDAT is Network Centric Data Communication Platform JASMINE. It's a unique system of systems in the areas of command support and communication in armed forces as well as control and communication, e.g., in the CM structures. JASMINE platform is a large collection of mutually consistent products of TELDAT, on the basis of which one can build an integrated information systems fulfilling actual needs. JASMINE has many specialized systems, subsystems, devices, and software, most of which can also be used autonomously. JASMINE belongs to a group of C4ISR systems (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), and has already proved its usefulness during multiple national and international activities, including exercises organized under the NATO's umbrella.

The Crisis management JASMINE Laboratory at NDU is equipped with such devices as:

- servers;
- computers;
- routers;
- switches;
- simulation environment using HLA;
- mobile vehicle with telecommunication infrastructure;
- virtualization tools;
- automatic testing tools;
- radio stations;
- satellite devices.

In the Laboratory a lot of new concepts were developed and a number of innovative solutions were implemented in real tools and components.

Other solutions exploited at NDU include, e.g.,

- GAMBLER – a simulation system used in planning and conducting research and experiments utilizing models containing and selected fragments of reality. Usage of the simulator is particularly valuable in the planning of the use of the air force and air defence system. With its help the strengths and weaknesses of developed courses of action can be identified and a better solution can be chosen. The essence of the use of GAMBLER is to

reduce the uncertainty areas, which is achieved by executing an experiment scenario which reflects real and anticipated operational tactical situation;

- TOPAZ – Artillery Fire Control System – a complex communication and information artillery fire command and control system. TOPAZ suite includes necessary hardware and software for all command posts within the field of an artillery battalion. The information is exchanged in digital mode in a multi-node radio network.

The employees of NDU have a comprehensive experience with experimentation in the military domain. As already mentioned, they participate actively in various activities devoted to the CM-related education and innovative solutions development. Each of these areas of involvement requires an extensive knowledge, expertise, experience, and innovative oriented, broad look at the CM issues. The University constantly carries on a comprehensive collaboration, on the one hand, with solution developers (e.g., TELDAT), and, on the other hand, with possible end-users of CM solutions (e.g., Polish Armed Forces). As a consequence, employees of NDU have developed plenty of solutions/upgrades for Military Decision Making Process (MDMP). The facilities available at the University are exploited extensively to arrive at valuable solutions; appropriate methods, metrics, and performance indicators are defined each time to ensure that the final product satisfies the highest standards.

Generally speaking, the specialists at NDU have knowledge, experience, and expertise to:

- develop and implement concepts;
- perform experiments;
- evaluate results;
- carry research;
- provide measurement methodology.

As main obstacles which DRIVER can face, the employees of NDU mentioned different law regulations in different countries. Moreover, they also pointed out that, according to their knowledge and experience, several valuable solutions extensively used on a regional level in Europe are not prepared to be utilized by persons not familiar with a given local language. This observation is related to another fact indicated by the experts at NDU, namely that a successful experiment requires good management which cannot be achieved without proper communication between partners.

Contact information

War Gaming and Simulation Center

Experimentation and technical staff:

Col. Grzegorz KOTT, PhD, Eng., e-mail: g.kott@aon.edu.pl

LtC. Jacek STEMPIEŃ, PhD, Eng., e**-mail: j.stempien@aon.edu.pl**

LtC. Krzysztof ŻWIREK, PhD, Eng., e**-mail: k.zwirek@aon.edu.pl**

CBRN Defence Training Centre

Experimentation and technical staff:

LtC. Adam BAGNIEWSKI, MSc, Eng., e-mail: a.bagniewski@aon.edu.pl

LtC. Mariusz MŁYNARCZYK, PhD, Eng., e**-mail: m.mlynarczyk@aon.edu.pl**

Management and Command Faculty

Col. Stanisław KOWALKOWSKI, Prof., e**-mail: s.kowalkowski@aon.edu.pl**

National Security Faculty

Col. Dariusz MAJCHRZAK, PhD, Eng., e-mail: d.majchrzak@aon.edu.pl

4.2 Annex II: DRIVER partner resources

4.2.1 Crisis test rooms

4.2.1.1 Wielkopolska Voivodeship Office, Security and Crisis management Department, Poznań, Poland (ITTI)

4.2.1.1.1 General Description

The Security and Crisis management Department of the Wielkopolska Voivodeship Office is responsible for all kinds of crisis situations whose outreach extends the areal of a single city or borough. To be more specific, the scope of the activities covers such issues as:

- **civil defence,**
- **security of mass events,**
- **national emergency medical services,**
- **emergency call centre,**
- **crisis related communication,**
- **flood control and protection,**
- **nuclear energy legislation.**

The employees of the Department are:

- **predicting and evaluating possible and present threats,**
- **recommending to the Voivode actions to take,**
- **reviewing and recommending changes of the voivodeship crisis management plans,**
- **circulating among society information concerning threats,**
- **responsible for training its staff and ensuring smooth cooperation among various services.**

With respect to the emergency call center (phone no. 112), the main duties of the Department staff are to: (i) identify whether there is any threat and if so, then of what kind, (ii) gather all relevant information such as personal data of the person who calls, detailed coordinates (address) of the event, (iii) work out possibly comprehensive situational awareness, (iv) inform appropriate emergency services and provide them with all necessary information, (v) give guidance and instructions to the contact person (and other witnesses), which includes also physiological and first-aid medical support.

4.2.1.1.2 Relevance for DRIVER:

The facility:

- **can be used in experiments, trainings, and exercises,**

- is governed by crisis management experts having an extensive experience in dealing with crisis situations as well as in organizing corresponding exercises and trainings,
- can be exploited for training crisis management and creating situational awareness at all echelons,
- comprises components and solutions which can be utilized for DRIVER integrated test bed,
- can be used to simulate crisis room operations and to use crisis management systems in a real like environment,
- includes information sharing channels to coordinate operations and to work out a clear understanding of the mission area,
- provides various internal/external communication networks.

Fig. 9 Facilities of the Security and Crisis Management department, Poznan Poland(ITTI)

4.2.1.2 Municipal Office of Poznań, **Security and Crisis management Department**, Poznań, **Poland (ITTI)**

4.2.1.2.1 General Description

The Security and Crisis management Department of the Municipal Office in Poznań is to **support** the Mayor of Poznań in the decision making process during crisis situations by **gathering all relevant data as well as performing analyses and simulations concerning the crisis situation which occurred. The responsibilities of the Department include coordination in hazard situations of joint efforts of police, health care, emergency medical service, firefighters, municipal police, public transportation, health and veterinary inspections, drinking water suppliers, gasworks, etc. The main activities of the Department are concerned with:**

- **an ensurance of a twenty-four-hour long flow of information for the needs of the crisis management, e.g., by 24/7 emergency call service,**
- **a management of the so called SWOA system developed to detect, warn, and alert** inhabitants of Poznań,
- **a cooperation with crisis management centers or other public administration units and institutions,**
- **a cooperation with institutions responsible for an environment monitoring,**
- **a cooperation with units undertaking rescue, search, and humanitarian actions,**
- **a documentation of all actions undertaken by the Department,**
- **a constant monitoring of threats related to the national defense,**
- **an organisation of trainings and exercises for various services to ensure their proper cooperation in the case of a crisis event.**

4.2.1.2.2 Relevance for DRIVER

The facility:

- **can be used in experiments, trainings, and exercises,**
- **is governed by crisis management experts having an extensive experience in dealing with crisis situations as well as in organizing corresponding exercises and trainings,**
- **can be exploited for training crisis management and creating situational awareness at all echelons,**
- **comprises components and solutions which can be utilized for DRIVER integrated test bed,**
- **can be used to simulate crisis room operations and to use crisis management systems in a real like environment,**

- includes information sharing channels to coordinate operations and to work out a clear understanding of the mission area,
- provides various internal/external communication networks.

Fig.10 Facilities of the Security and Crisis Management Department of the Municipal Office in Poznan, Poland

4.2.1.3 The Main School of Fire Service, Faculty of Civil Safety Engineering, Warsaw, Poland (ITTI)

4.2.1.3.1 General Description

The Main School of Fire Service (MSFS) is an academic facility of state services subordinate to the Minister of Internal Affairs. It educates the firefighters of the State Fire Service, officers of other services and guards, subordinate to the Minister of the Internal Affairs. MSFS also trains civilians. At the same time, MSFS also enjoys the status of organisational unit of the State Fire Service operating on the basis of the Act on the State Fire Service of 24 August 1991. According to the act, the School provides cadet officers with the opportunity to serve as trainees in the School Rescue and Firefighting Unit. The School's mission is to train the most highly qualified staff in the following areas: natural disasters and social threats

assessment, as well as life, health, property, and other values protection against those hazards. MSFS also aims at focusing on patriotic values, dedication to public service and respect for discipline in work and duties. The employees of the School have an extensive experience in organizing trainings and exercises focused on crisis management concerned with practically all kinds of crisis situations; often the School organizes such activities at the request of companies, administrative units, or particular groups of end-users. (For further details see: https://www.sgsp.edu.pl/)

4.2.1.3.2 Relevance for DRIVER

The facility:

- can be used in experiments, trainings, and exercises,
- is governed by crisis management experts having an extensive experience in dealing with crisis situations as well as in organizing corresponding exercises and trainings,
- can be exploited for training crisis management and creating situational awareness at all echelons,
- comprises components and solutions which can be utilized for DRIVER integrated test bed,
- can be used to simulate crisis room operations and to use crisis management systems in a real like environment,
- includes information sharing channels to coordinate operations and to work out a clear understanding of the mission area,
- provides various internal/external communication networks.

Fig 11 Facilities of the Faculty of Civil Safety Engineering of the Main School Fire Service; Earssaw, Poland

4.2.1.4 Crisis Information Centre, Space Research Centre, Warsaw, Poland (ITTI)

4.2.1.4.1 General Description

The activities of the Crisis Information Centre (CIC) are aimed at an effective use (by developing, testing, evaluating, and also training of potential end-users) of space applications for international security, civil protection, and humanitarian operations. CIC focuses its attention particularly on those solutions originating from the satellite technology which are already available, but are not yet commonly used by potential end-users involved in rescue and crisis management. Moreover, the centre is responsible of maintaining a portal for a geospatial information exchange. The activities of CIC cover:

- **support of the crisis management institutions and companies dealing with a usage of the geospatial and satellite information,**
- **utilization of the technical possibilities originating from the geospatial information,**
- **geo information support of Polish NGO outside Poland,**
- **evaluation of new technological solutions,**
- **development of new methods and tools (particularly satellite-based) for crisis and rescue management.**

CIC organizes ground experiments based on prior prepared scenarios, often taking place at the military training grounds (e.g., in Żagań, Poland). In those experiments such tools as **satellite-based communication, monitoring, and localization as well as geo maps, unmanned shuttles, or contamination sensors are often involved. The Centre cooperates closely with the National Headquarters of the State Fire Service of Poland, and for the exercises inside uses mostly facilities of the Main School of Fire Service (own facilities of CIC are at present under construction). CIC has experience in an international cooperation, e.g., at the end of 2014 it will organize exercises dealing with mountain flooding in Georgia focused on optimalization of cooperation between various services. Moreover, head of the Space Research Centre, Jakub Ryzenko, coordinated Polish EU Presidency activities related to use of space applications for civil protection and in May-July 2010 he led a 6-week emergency effort, providing an effective satellite support for crisis management operations during large-scale floods in Poland.**

4.2.1.4.2 Relevance for DRIVER

<u>The facility:</u>

- **can be used in experiments, trainings, and exercises,**
- **is governed by persons having an experience in dealing with selected crisis situations as well as in organizing corresponding exercises and trainings,**

- is focused particularly on implementation of innovative technologies to crisis management,
- can be exploited for training crisis management and creating situational awareness at all echelons,
- comprises components and solutions which can be utilized for DRIVER integrated test bed,
- can be used to simulate crisis room operations and to use crisis management systems in a real like environment,
- includes information sharing channels to coordinate operations and to work out a clear understanding of the mission area,
- provides various internal/external communication networks.

Fig. 12 Experiments organized by the Space Research Centre of the Crisis Information Centre, Warsaw, Poland

4.2.2 Physical test/exercise facilities

4.2.2.1 EDSP 13: the fire department training school of Bouches-du-Rhône (France) (Pole)

Webpage, Point of Contact:

http://www.sdis13.fr/haut/menu_principal/nos_missions/l_ecole_departementale

Built in 2012 in Velaux (France), the new training schools of the Bouches-du-Rhône fire department (SDIS 13) is dedicated to the initial and continue training of fire-fighters for urban fire, CBRN activities, and forest fire.

4.2.2.1.1 General Description

- **6 000 m2 of various environment & buildings are available to deploy and test several technologies, as RPAS, robots, crisis management tactical systems, fire simulation software, health technologies, vision systems, new materials for thermal protection, chemical additives for fire fighting.**
- **Fire use is allowed. Artificial forest fire is available (gaz use) to evaluate the thermal constraint on material (closes, vehicle).**
- **Very high rank medical service is also available to welcome and study physiological effects studies**
- **The training school** hasn't be built to host experiments. But, as a training center, **the operational environment is close to the reality. It is in consequence important to anticipate the agenda as far as possible to check the site availability and freeze the period of experiment.**

Fig. 13 Training Facilities MSB

4.2.2.1.2 Relevance for DRIVER

- **Different types of experiments could be hosted at the EDSP 13:**
  - **For SP3:**
    - **Table-top exercises on Resilience mechanisms and procedures with several entities in charge of the crisis management, including political makers and police.**

        - Dissemination event on the DRIVER resilience approach, with medium and large European cities urban planers.
    - For SP4:
        - DRIVER Scenarii workshop with international experts. It could indeed very interesting to organize a general brainstorming on the 3 scenarii (flood & pandemia ; ice storm & electricity failure ; Mediterranean tsunami & add-on hazards) by merging ideas, suggestions, exchanges. It could be a very good imput to start precise scenariii organisation. International thematic experts could be merged in 3 sub group, with end-users DRIVER partners as animators.

- Different scenario could be done in EDSP 13:
    - Urban search and Rescue, including CBRN hazards
    - Forest fire monitoring by using RPAS
    - Forest fire fighting simulation (ground & aerial)
    - Resilience table top exercize
    - DRIVER scenarii brainstorming with international experts

4.2.2.1.3 Practical issues

- EDSP 13 need to pre-plan the DRIVER experiments at least 6 month before. 1 year is better.
- Logistics: all the EDSP 13 has been built to welcome hundreds of people. A large DRIVER consortium could work, eat and sleep on site. Sevaral meetings rooms are also available, such as plenary conference room.
- Additional costs involved: Pole RISQUES will rent the EDSP 13 premises and facilities. Consortium could have to pay for lunch, hotel. EDSP 13 could also arrange transportation.

4.2.2.1.4 What could be the added value for the facility of hosting DRIVER experiments

- It is crucial to think about experimentation as something really different than a demonstration. The DRIVER project could be for EDSP 13 a huge opportunity to introduce a scientific approach (objectives, methodologies, indicators, evaluation, lesson learned, dissemination). Globally, DRIVER could be the R&D framework of the EDSP 13, and in consequence highlight gaps, requirements and strategies for the next years investments.
- Pole RISQUES has the objective to use the DRIVER opportunities to build in France (at least) a crisis management test-bed network, including shared protocols, economics models and dissemination activities, to merge private and public

efforts in the same way. EDSP 13 will be one of the pillars of those networking efforts.

4.2.3 Relevant products

Webpage, Point of Contact:

http://arxiv.org/ftp/arxiv/papers/0903/0903.2543.pdf

4.2.3.1 PROCeed (ITTI)

4.2.3.1.1 General Description

PROCeed is a computer system which supports preparations for decision making in simulated situations. It allows to create and run various kinds of simulation applications for the needs of training as interactive decision-making games as well as can be utilized as a tool box for the 'what if' analysis. Exploiting simulation techniques allows an exact **mapping of an actual course of a given crisis situation, by taking into account all necessary roles, decisions, phenomena, physical objects, or elements of an environment. By observing dynamically changing simulated situation, a user of the system can make decisions which influence its further development and behaviour of other users. Crisis situations included in PROCeed concern, e.g., flooding and epidemic. The system can be accessed from various locations. Target group: everybody interested in training to cope with crisis situations.**

4.2.3.1.2 Relevance for DRIVER:

Supports decision making process, creates situational awareness in crises situations, enhances understanding of dynamics of crisis events, and allows to analyse consequences of the decisions made.

For further details see the flyers of PROCeed.

4.2.3.2 LIMA2 (ITTI)

4.2.3.2.1 General Description

LIMA2 is a methodology based software tool that supports collecting, analysis, and exploitation of experiences gathered during in-field missions. LIMA2 was originally developed for analysing lessons learned during patrol duties of small military units, however it can be as well used for any activity that follows the classic 3-stages schema: planning, execution (in CM response), and post mission analysis (in CM recovery). Target group: Planners and managers of crisis management operations.

4.2.3.2.2 Relevance for DRIVER

Demonstrates complexity and difficulty related to incorporating lessons learned in military as well as other operations and provides a clear insight into lessons learned circle.

4.2.3.3 BESECURE (ITTI)

4.2.3.3.1 General Description

BESECURE (Best practice Enhancers for SEcurity in Urban Regions) is a software tool based on collection and analyses of best practices within the area of urban security through case studies in eight selected urban areas throughout Europe. By building a comprehensive set of indicators for urban security, along with best practices from different urban areas, important facts about the state of security in urban regions including such factors as social makeup, economic state, crime numbers, and public perception of security became apparent. Based on this knowledge, BESECURE developed towards a creation of a resource database that supports local policy makers to assess the impact of their practices and improve their decision making. BESECURE is composed of three platforms, namely:

- **Inspirational Platform, which supports policy makers in accessing knowledge about interventions and practices for urban policy,**
- **Policy Support Platform, which is to guide policy makers through several steps in building an evidence base for their urban security decisions,**
- **Urban Data Platform, which is to support policy makers to make more and better use of (urban) data in their policy making process.**

Target group: local urban policy makers.

4.2.3.3.2 Relevance for DRIVER

Creates situational awareness and sheds light on mutual dependences between various hazards in inhabited areas.

For further details see the flyers of BESECURE or the website http://www.besecure-project.eu/.