Mediterranean practitioners' network & capacity building for effective response to emerging security challenges

MEDEA is a project that has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme **H2020-SEC-21-GM-2016-2017**, under grant agreement no **787111.**

Additional information about the project and the consortium can be found at www.medea-project.eu

D6.5 Mediterranean Research and Innovation Agenda v1

Contractual Delivery Date: 11/2019	**Actual Delivery Date**: 09/12/2019
Dissemination level: Public	**Version**: 1.0

Abstract

The Mediterranean Security Research and Innovation Agenda (MSRIA) lists common capabilities required by Mediterranean and Black Sea security practitioners to respond more effectively to current and emerging threats. MSRIA's current version is the first one out of four annual updates in total. The first MSRIA edition represents a subset of capability gaps resulted from practitioners' interactions inside the four developed Thematic Communities of Practitioners which formed the MEDEA practitioners' network. The objectives of MSRIA are (1) submit a series of recommendations to European Security and Defence technology leaders; (2) provide advisory services to practitioners; (3) communicate practitioner needs to National and EU Policy makers; (4) highlight current demands for interoperability and standardisation; and (5) promote integration of full technology, systems and services supply chains, by considering besides Technological, also Human-related, Organisational, and Regulatory framework conditions.

DISCLAIMER: This document contains material, which is the copyright of the **MEDEA** consortium members and the European Commission, and may not be reproduced or copied without permission, except as mandated by the European Commission grant agreement no. **787111** for reviewing and dissemination purposes.

Document Control - Revision History			
Issue	**Date**	**Comment**	**Author / Institution**
0.1	11-12-2018	First structure	ISDEFE
0.2	07-11-2019	Comments to the TOC	KEMEA
0.3	20-11-2019	Contribution	SATCEN
0.4	25-11-2019	Contribution	EPLFM
0.5	27-11-2019	Comments and review	EOS
0.6	29/11/2019	Structuring of Introduction and the MSRIA model	DGAP
0.6	02-12-2019	Contribution, comments, formatting	KEMEA ISDEFE
0.7	04-12-2019	Contributions in sections 3, 4 and section for TCP1. End to end review and finalisation of TCP2 and TCP4	KEMEA,
0.8	5/12/2019	Review and corrections	DGAP
0.9	6/12/2019	Contributions and conclusions	EOS
1.0	9/12/2019	Final review	ISDEFE, DGAP

Quality Control			
Issue	**Date**	**Comment**	**QA Responsible**
1.0	10/12/2019	Quality control of final version	ISDEFE

Statement of originality
This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

RELEASE APPROVAL			
Issue	**Date**	**Comment**	**QA Responsible**
0.1	09/12/2019	Final review	KEMEA
1.0	12/10/2019	Security scrutiny of the Deliverables	Security Committee

Executive summary

The Mediterranean Security and Research Agenda (MSRIA) is a living inclusive document that will be evolved in four annual editions. The first version is produced in 2019 and the final one will be delivered in 2022. The MSRIA objectives are:

I. Identify areas where security research and innovation is needed following a demand-driven, approach of gap & requirement formulation supported by practitioners.

II. Constitute a common position by Mediterranean and Black Sea security practitioners in with a view to emerging threats in the form of a Roadmap .

III. Submit recommendations for European Security & Defence technology investments both at the European and at the National level, in relation to respective funding mechanisms, and provide advisory services to Practitioners and Policymakers

IV. Explore needs for interoperability and standardisation, as well as dual-use synergies in R&D.

V. Promote integration of full technology, systems and services supply chains, by considering besides Technological, also Human-related, Organisational, and Regulatory framweork conditions (MEDEA THOR methodology for scenario building).

The current, first 2019 edition of MSRIA has collected capability gaps by the still in formation Thematic Communities of Practitioners (TCPs). As the editions of MSRIA will be reaching maturity year by year, MSRIA will assist the MEDEA Thematic Communities of Practitioners, as well as other practitioner's Networks by *Enable knowledge transfer* in the following three directions:

1. *Upstream* by communicating practitioners' required capabilities and requirements for regulatory and policy amendments using advanced analysis methods for assessing current and emerging threats.

2. D*ownstream* by communicating state-of-the-art solutions and innovative offering to address the identified by practitioner's capability gaps and facilitate the technology uptake in the security industry.

3. *Horizontally* by providing advisory and training services to practitioners from all four communities in the MEDEA network as well as with other practitioner's networks.

Table of Contents

Table of Figures

Table of Tables

Definitions and acronyms

Definitions

Concepts and terms used in this document and requiring a definition are included in the following Table 1:

Table 1: Definitions

Concept / Term	Definition
INTRA-perspective	MEDEA practitioners from the same discipline
TRANS-perspective	MEDEA practitioners from different disciplines
INTER-perspective	MEDEA practitioners who are based in EU and EU neighbouring countries radius
THOR	It is a four-dimension methodology model where for the: **Technological** dimension examines the concrete approaches and solutions that can be used; **Human** dimension studies human factors, behavioural aspects, privacy issues; **Organisational** dimension evaluates existing processes, procedures and policies within the organisations and examine interaction within their country and the region; and **Regulatory** dimension researches the provisioning law, existing standardisation and modus operandi of the involved entities
TCP	Competent practitioners will be engaged in discussions and collaboration on specific areas needing specific knowledge, training and expertise
CoP	In MEDEA these are groups of Practitioners who share a concern, a set of problems, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis

Acronyms

Acronyms used in this document and requiring a definition are included in the following Table 2.

Table 2: Acronyms

Acronym	Definition
BCP	Border Crossing Points
BGA	Border Guard Authorities
CoP	Community of Practitioners

CGF	Capability Gap Finding
EFCA	European Fisheries Control Agency
EMSA	European Maritime Safety Agency
EARTO	European Association of Research and technology Organisations
EC	European Commission
ENLETS	European Network of Law Enforcement Technology Services
EU	European Union
EU SatCen	European Union Satellite Centre
GIS	Geographic Information System
LEA	Law Enforcement Agencies
MSRIA	Mediterranean Security and Research Innovation Agenda
M&BS	Mediterranean and Black Sea
NGO	Non Governmental Organisations
PASR	Preparatory Action for Security Research
PCP	Pre Commercial Procurement
PPI	Public Procurement of Innovative solutions
RDI	Research and Development Initiatives
SIGINT	Signals Intelligence
SM	Social Media
STACCATO	STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities
TCP	Thematic Communities of Practitioners
TRL	Technology Readiness Level
WUI	Wildland–Urban Interface
WP	Work Package

References

Applicable documents

The following documents, of the exact issue shown, form part of this document to the extent specified herein. Applicable documents are those referenced in the Grant Agreement or approved by the Approval Authority. They are referenced in this document in the form [AD.X]:

Table 3: Applicable Documentation

Ref	Title	Version	Date
[AD.1]	GRANT AGREEMENT NUMBER — 787111 — MEDEA	1.0	15/05/2018

Reference documents

The following documents, although not part of this document, amplify or clarify its contents. Reference documents are those not applicable and referenced within this document. They are referenced in this document in the form [RD.X]:

Table 4: Reference Document

Ref	Title
[RD.6-1]	REGULATION (EU) No 377/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010
[RD.6-2]	Frontex Information Management. Available online at: https://frontex.europa.eu/intelligence/information-management/ Accessed on 19th Nov 2019.
[RD.6-3]	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624
[RD.6-4]	OBSERVER: Copernicus - Eyes on the EU’s external borders. Available at: https://www.copernicus.eu/en/observer-copernicus-eyes-on-EU-external-borders Accessed on 19th Nov 2019.

1 Introduction

1.1 MSRIA´s Vision

The Mediterranean Security and Research Innovation Agenda (MSRIA) constitutes one of the core activities of the MEDEA Practitioners' Network. In **strategic** terms, MSRIA will leverage capability-building activities performed in other relevant Networks of Practitioners, as well relevant Research & Innovation, and Coordination & Support Actions. This is taking place in the context of the DG HOME Community of Users events, as well as in dedicated inclusive conferences, such as the 1st Mediterranean Security Event in October 2019, which mobilised the support of fifty projects. Specifically, thirty-six (36) European R&D projects co-organised this joint initiative disseminating the results of their scientific work while fourteen (14) more security-related projects presented their objectives and achievements in the conference sessions of MSE2019[1]. The event was officially supported by the DG HOME of the European Commission (EC), the Community of Users (CoU) of Security Research, the European Association of Research and Technology Organisations (EARTO) and the European Network of Law Enforcement Technology Services (ENLETS).

In **formal** terms, MSRIA is a catalyst for key internal MEDEA objectives:

Obj1. Improve collaboration among institutions and actors from different disciplines using research and innovation as a catalyst for a) enhancing capabilities of practitioners through the use of technological innovations in their operations and b) enable the coordinated use of interconnected information systems. In this respect, linking particularly Obj1.2. "Strengthening operational capabilities of M&BS practitioners" with Obj1.3. "Development and Cooperation for Transnational Security Research - Exploitation of EU research and innovation outcomes in neighbouring/adjacent third countries."

Obj2. Define Mediterranean and Black Sea regional security priorities, amalgamated in an annually updated **Mediterranean Security Research and Innovation Agenda**, using a scenario-based visioning method for considering alternative future threats and high impact scenarios, comparing them, analysing how they might occur at the mid to the long-term scenarios and how effective and efficient responses may by devised. Key in this respect is particularly the link between Obj2.2. "Provide a unified Mediterranean contribution to the National and EU Policy Makers on Upcoming Challenges to European Security" and

Obj3. Build a scenario driven technology roadmap that a) Identifies common needs of relevant actors across the region and b) explores the use of innovative tools such as PCP, PPI, etc. to take advantage of economies of scale and reduce time to market, and c) capitalize on previous research and innovation activities.

The MSRIA has two characteristics:

[1] https://mse2019.kemea-research.gr/press-release-mediterranean-security-event-2019/

- It is a **living and adaptive document**, that provides stakeholder-sensitive recommendations for R&D and policy actions in its four consecutive editions throughout the project.
- Second, MSRIA is a **circular strategic tool** within MEDEA: On the one hand, it is an **end** of the Practitioners' activities within the four Thematic Communities of Practitioners (TCPs), but at the same time, also a **means to strengthen practitioners' engagement and networking**, by providing a tangible incentive for all actors with security-related mandate from the public and private sector to join in MEDEA in the course of its 5-year activity.

In the course of MEDEA network members and other practitioners engage into a scenario-based assessment of present, emerging & future threats with the objective of being prepared to early anticipate them and being better prepared to effectively respond, with the introduction of new and innovative concepts and capabilities and/or interfaces to existing capabilities. The scenarios will examine **interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields and also make extensive use of the role of the space provided information**. The Technology Assessment Process will be carried out under the Technology evaluation and prioritization for each TCP. Those aspects will be eventually reflected in the agenda each of the four MSRIA editions will propose. A flow model visually summarizing the working of the MEDEA leading to MSRIA is featured for that reason below:

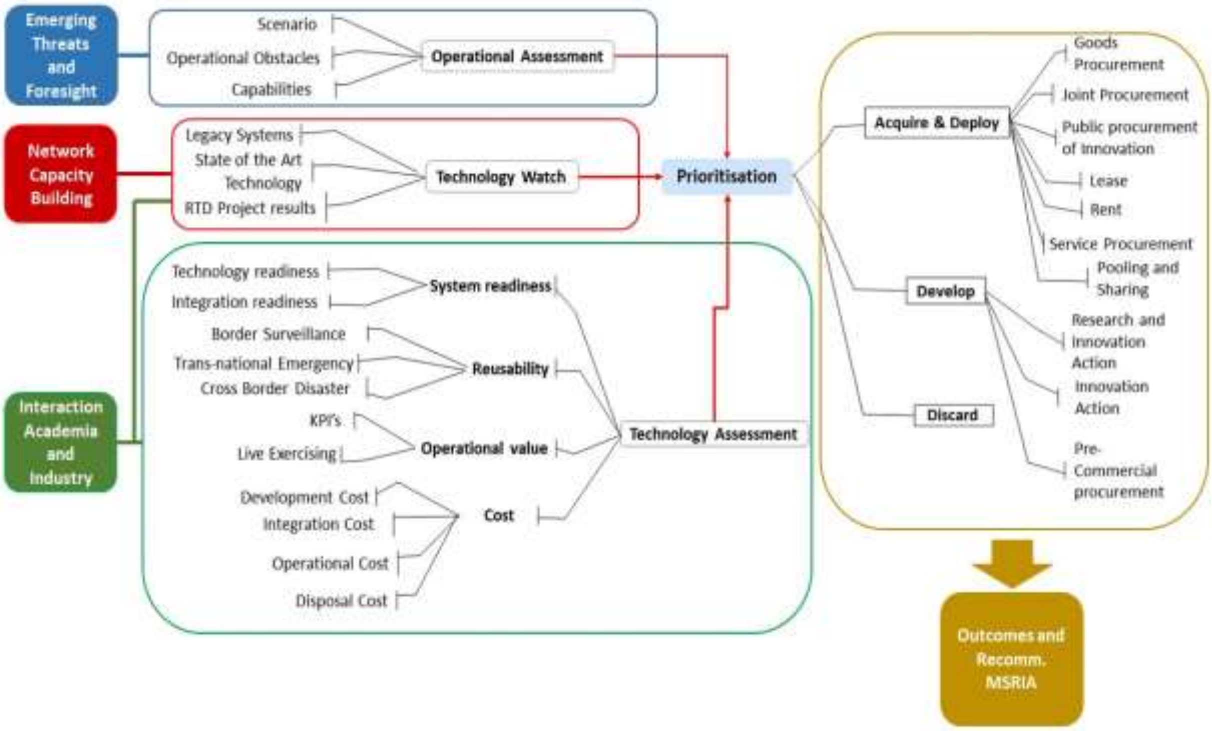


Figure 1: MEDEA TCP activities leading to MSRIA

It is important to stress at this point, that this flow encompasses the whole value-chain of capability building and will enable a demand-driven definition of requirements, as well as a make the uptake of innovative technological and non-technological solutions by end users more probable and more sustainable. The four annual editions of MSRIA are set **to impact on the Mediterranean and Black Sea security provision ecosystem via following actions**:

- Introducing to and familiarizing practitioners with the state of the science capabilities and/or interfaces to existing ones, that will have a noteworthy impact on the operational capacity of their organizations.
- Strengthening collaboration – exchange of best practices, on how to be engaged in security research and innovation actions and on the uptake of the research and innovation outcomes on the daily operations.
- Thorough assessment and anticipatory governance of common threats across the Mediterranean and the Black Sea, which is critical for the long-term planning thus societies more resilient to emerging security challenges. This includes how common threats across the Mediterranean or cross-border ones may be triggered, evolved, magnified / cascaded into disastrous events and engage in targeted exchange of ideas and discussions, and how the unintended negative impacts of these scenarios could be minimised or even avoided
- Establishment of common scenarios database, which can be used as the basis for national risk assessment by respective national organizations
- Simplification of administrative burden, through proposals for coordinated, integrated and long-term approach between EU funded programmes (e.g. H2020, ISF, the upcoming Horizon Europe Programme) and national security R&D programmes, also maximizing European added-value based upon the synergetic uptake of results and common funding evaluation procedures.

The MSRIA is part of MEDEA's WP 6 which is responsible for ensuring the transfer insights to the right target addressees. This process, which acknowledges the different logics, time-frames, interests, and capacities of all involved security stakeholders, helps turn findings and insights out of the practitioner-led scenarios into Actionable Knowledge, which should be useful, usable and factually used by policy makers, and security providers.

The adjustment and evolution of the THOR assessment template consolidates awareness of Technological, Human, Organisational, and Regulatory enablers and constraints in the concrete, threat-specific contexts of the respective CoPs. This approach is expected to avoid unusable blueprinting, and lead to reliable and valid prioritizations of scenarios in a demand-driven, stakeholder-sensitive way. Such a procedure is bound to raise effectiveness, transferability, and sustainability of security solutions.

A key approach followed thereby by the MEDEA consortium is **Co-Creation**: This is the stakeholder-inclusive definition, generation, and implementation of knowledge through all involved stages of the project. At the same time, this approach, since it is not an academic top-down implementation of ready-made models, comes together with certain delays in the constitution and workings of each of the four TCPs. For that reason, the maturity of the agendas recommended to each of the TCPs respectively, may vary depending on the ripeness stage of the scenario elaboration and THOR assessments performed with each of the TCPs.

Nevertheless, as the editions of MSRIA will be reaching maturity year by year, MSRIA will enable **knowledge transfer**:

1. *Upstream* by communicating practitioners' required capabilities and requirements for regulatory and policy amendments using advanced analysis methods for assessing current and emerging threats.
2. D*ownstream* by communicating state-of-the-art solutions and innovative offering to address the identified by practitioner's capability gaps and facilitate the technology uptake in the security industry.
3. *Horizontally* by providing advisory and training services to practitioners from all four communities in the MEDEA network as well as with other practitioner's networks.

Specifically, the positioning of MSRIA (Task 6.4) within the overall architecture of MEDEA is explained below:

The MSRIA editions are cross-linked with specific other MEDEA Tasks, such as the **THOR elaboration tasks** (2.2, 3.2, 4.2, and 5.2) which will provide substantial insights about gaps and requirements, as well as with the transfer-related tasks within each TCP. Furthermore, MSRIA is directly connected with Task 6.3 (**Advisory services to practitioners for innovation procurement)** and Task 6.5 (**Recommendation to Policy Makers).**

At network-building level, MSRIA is connected with Task 1.3 (**Fostering Capacity-building in Thematic Communities of Practice**), Task 6.2 (**Enhancing practitioners' involvement to RDI**), and with Task 7.4 (**Interaction with other networks**). At a ripe stage toward the end of MEDEA, the ambition is to valorise recommendations from MSRIA into capability-building in practice, by putting together a **Med Regional network of security research infrastructures** (Task 6.7).

1.2 MSRIA´s steps

In order to achieve its goals, MEDEA developed a general-purpose multi-factor prioritization technique that will pinpoint the short, medium- and long-term priorities as far as technology development is concerned, taking as a baseline the scenarios developed by the different TCPs. Starting from operational scenarios, that will be analysed by practitioners with the assistance of researchers aiming to bring together the technical, operational, legal, human and financial aspects, all of which will contribute to the development of MSRIA. Three different distinct steps will be performed.

Step-1: Operational assessment,

Step-2: Technology watch and assessment and

Step-3: Prioritisation.

1.2.1 Step-1: Operational Assessment

The Operational Assessment will be carried out as part of the scenario definition for each TCP. This process will identify, which of the submitted scenarios are the more relevant and which sections or entries should be further elaborated to reflect the practitioner's operational capabilities. The operational assessment will rely on the knowledge and background of the authorities and practitioners acting as project partners, as well as from the inputs delivered by other collaborating stakeholders. This process will rely strongly on the characterization of the context, the identification of the operational obstacles faced by the end-users and the categorization of the capabilities required for the successful achievement of the operational objectives. As part of this process, and in order to articulate the Scenario driven based approach proposed by MEDEA, it is of paramount importance to establish a parallelism between the capabilities required to conduct successful operations in each scenario, and the features of such scenarios. A common capability taxonomy should be jointly agreed among the TCP members and it should be a valuable tool in order to derive homogeneous results from the operational assessment.

1.2.2 Step-2: Technology watch and assessment

Based on the work performed in step-1, technology-watch activities should provide inputs to all the processes but mainly to the Technology Assessment. The Technology Assessment Process will be carried out under the Technology evaluation and prioritization for each TCP. It will reveal the benefits and disadvantages associated to the availability of certain technology or to the lack of it, respectively. The quantification of the value of certain technology can be based on different value models like the: The Technology Readiness Assessment (TRL), the Reusability and Extensibility Assessment, the Operational Assessment and the Cost Assessment. The outcomes and findings from Step-2 shall periodically feed the Mediterranean Security Research Innovation Agenda, thus showing the priorities of the practitioners with respect to the short, mid and long-term research.

1.2.3 Step-3 Prioritization

The objective of this step is to sort out a list of candidate technologies, methods and techniques following a semi-quantitative analysis scheme. This list will define the priorities for the adoption or further development of such technologies according to the risk levels perceived by the users' community and other stakeholders. The risk levels will be determined by a number of factors, all relevant to support the decision process for the definition of innovation priorities. These factors will be identified and quantified in terms of the three horizons, and they shall include, among others, the operational context, the technical features of the technologies, their maturity levels, their operational relevance, their reusability and extensibility and their cost.

1.3 MSRIA´s approach

The MSRIA editions, depending on the maturity of the results delivered by each of the four TCPs, aim at presenting a dynamic, annually updated **TCP-specific R&I Roadmap** for action. The MSRIA Roadmap will present the Research & innovation Agenda as a set of recommended actions taking into account the key addressed stakeholder groups **(WHO)**, the envisioned value-added or purpose the innovative intervention is expected to fulfil **(WHAT FOR)**, the THOR-elaborated R&D recommendation, which may encompass technological, human-oriented, organisational, or regulatory innovation needs in the form of specific requirements **(HOW)**, as well as the temporal frame(s) for planning **(WHEN)**.

The results in each TCP MSRIA roadmap, provided that they have reached a satisfactory degree of maturity, will be able to propose a **prioritised agenda** out of the **mapped options.** However, even the THOR-elaborated aspects of R&D needs, and the gaps analyses are included in the first editions of the MSRIA, since they build the basis for a roadmap.

1.4 Development Process

Figure 2 explains the MSRIA Development process, which aim at defining first Practitioners' needs; then identifying related capability and organizational gaps; and concluding the exercise by providing them concrete solutions (technology innovation).

Needs
Gaps
Solutions

Figure 2: MSRIA Development cycle

Next figure (Figure 3) goes more into detail concerning the MSRIA Development process, by concretely defining where and how these inputs are collected from (MEDEA Partners and Stakeholders). The result of practitioners' interactions will enable TCP members to develop and co-create the key elements required for THOR analysis. The Capability Gap Findings that will be the outcome of the scenario analysis, in each one of the THOR dimensions, will be further decomposed and formed the Technology, Human, Organisational and Regulatory attributes.

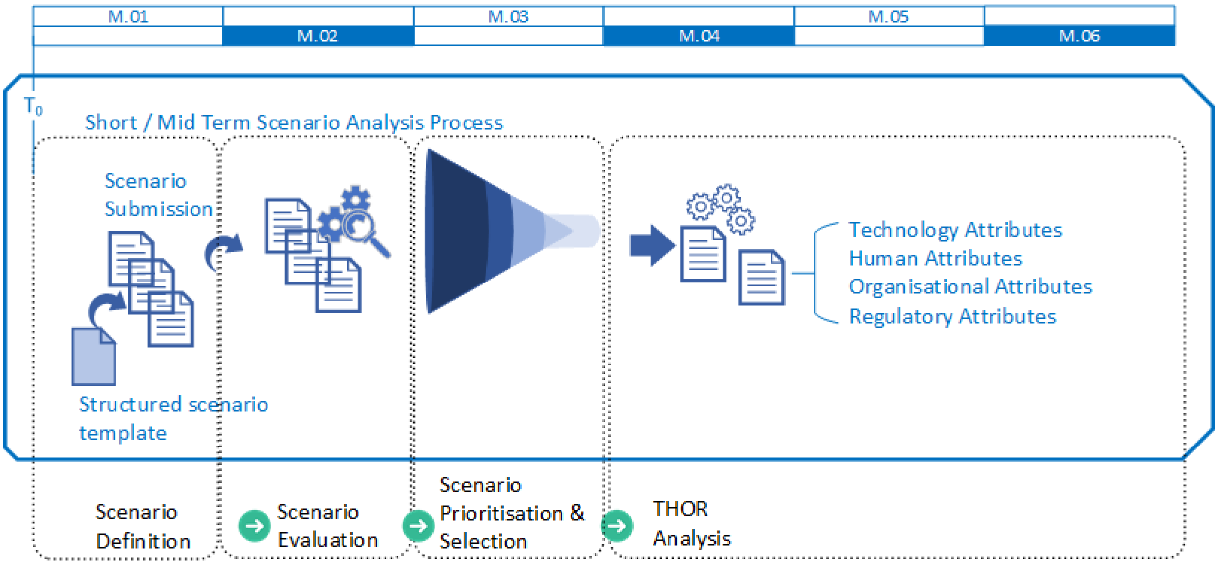


Figure 3: Scenario prioritisation to THOR analysis

TCP are formed by competent practitioners that are engaged in discussions and collaborated in specific areas requiring specific knowledge, training and expertise. These TCP will define user requirements, which will be shared with both Industry and Research Organisations that will promote related Security Research Priority which will be at the basis of the MSRIA, a scheme can be shown in Figure 4.

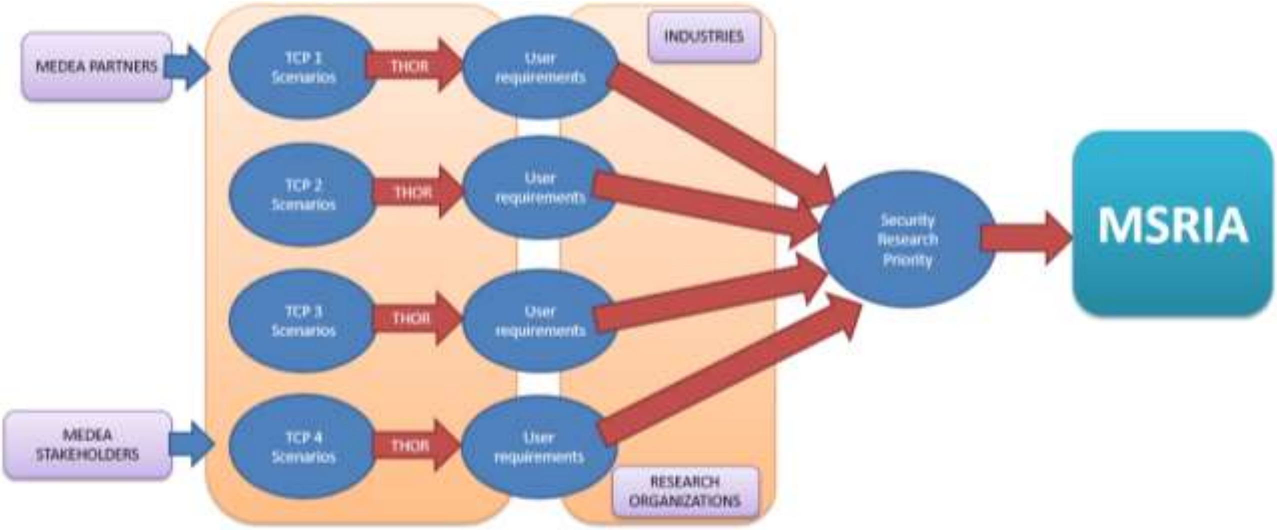


Figure 4: MSRIA Development process

1.5 Taxonomy

In order to have a useful common language tool not only for the MEDEA consortium but also for interfacing with end users, we are going to use the STACCATO taxonomy.

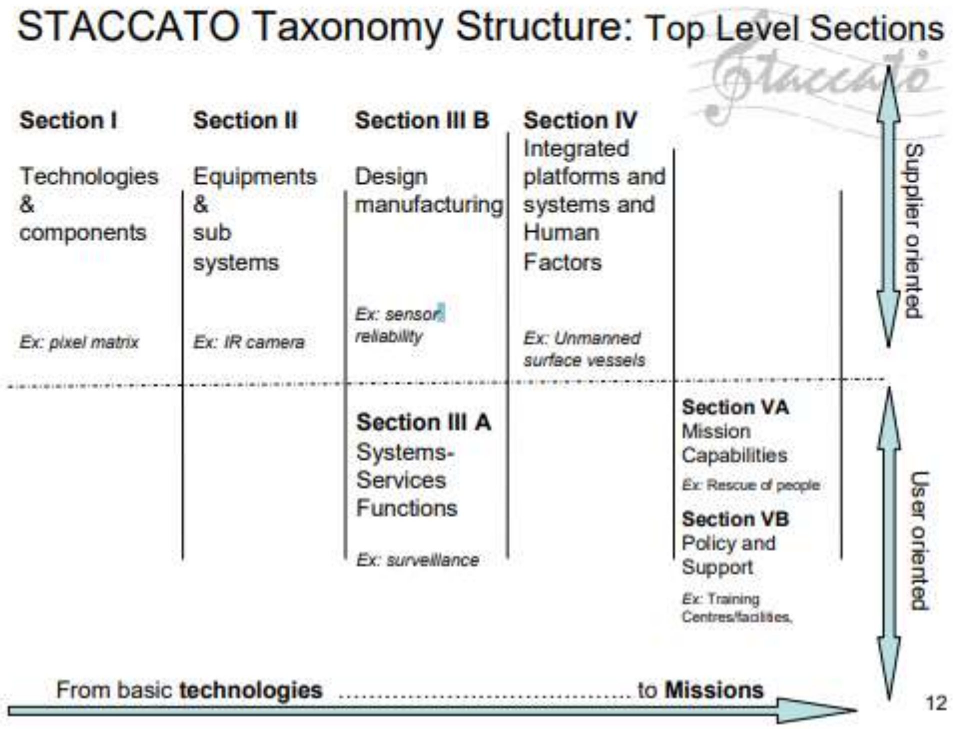
STACCATO stands for STAkeholders platform for supply Chain mapping, market condition Analysis and Technologies Opportunities. STACCATO was a European funded Preparatory Action for Security Research (PASR). With the view to map the competences of the supply chain and to establish a multi-sector stakeholder platform, STACCATO involved End Users, Government agencies, Think Thanks, Research Institutes, Academia and Industry; with a specific attention to SMEs and competences in new Member States.[2]

MEDEA builds on STACCATO main conclusions, and specifically on the seven-top level/sections of STACCATO Security taxonomy:

- (I) Technologies and Components
- (II) equipment and Sub Systems
- (IIIA) Systems-Services Functions
- (IIIB) Design-Manufacturing
- (IV) Integrated Platforms and Systems and Human Factors
- (VA) Missions Capabilities
- (VB) Policy and Support

The need is to have entries which can be used by the representatives of suppliers to indicate their capabilities and users to identify their needs.

[2] For more information on STACCATO, please refer to the “Main Conclusions and Recommendations on the European Security Equipment Market (ESEM) AND Executive Summary of the Final Study Report” available here: https://www.iai.it/sites/default/files/staccato_final-report-executive-summary.pdf



STACCATO Taxonomy Structure: Top Level Sections

Section I
Technologies & components
Ex: pixel matrix

Section II
Equipments & sub systems
Ex: IR camera

Section III B
Design manufacturing
Ex: sensor reliability

Section IV
Integrated platforms and systems and Human Factors
Ex: Unmanned surface vessels

Section III A
Systems-Services Functions
Ex: surveillance

Section VA
Mission Capabilities
Ex: Rescue of people

Section VB
Policy and Support
Ex: Training Centres/facilities.

Supplier oriented

User oriented

From basic technologies .... to Missions

12

Figure 5: Applied taxonomy

1.5.1 Dimensions of Gaps and Needs

In order to make a traceable Agenda, the propose scheme is a table where every solution/challenge has entries of:

- **ID:** Identification Code of the Solution/Challenge
- **Solution/Challenge:** Name of the Solution/Challenge
- **Description:** Brief description of the Solution/Challenge
- **Thematic:** (TCP1, TCP2, TCP3, TCP4)
- **Priority:** Per each thematic a number of priorities should be defining.
- **Capability:** Each priority should have a number of capabilities
- **Need:** The need that the solution/challenge should solve.
- **Gap:** Difference with the actual state of the art
- **Domain:** Operational domain (sea, land, air, cyberspace)
- **Scenario:** Identification of the scenario that is the source (could be more than one)
- **Term:** Expected time to achieve the capability
- **TRL:** Technology Readiness Level of the technology (if apply)

1.5.1.1 Example

ID	Solution	Description	Thematic	Priority	Capability	Need	Gap	Domain	Scenario	Term	TRL
	New radio communication system with fault tolerance for long distance	Development a new radio communication system with fault tolerance to use in sea and land surveillance operations.	TCP2	Earth Observation, Radio spectrum management, positioning, information management, communication system ….) Communication systems.	Improve the communication systems to send alerts and ensure the correct reception.	Avoid the loose of alerts for problems in the communication.	Actual radio satellite communications do not have redundancy system in every place.	Sea (In land operation there are more option to have redundancy in the communications 3G, 4G, Wi-Fi, radio stations…).	TCP2_scenario_3	Mid Term	1-3

Table 5: Example of solution identification and classification

2 Thematic Communities of Practitioners

The Mediterranean and Black Sea network of practitioners is composed of four Thematic Communities of Practice (TCP). As defined in previous sections, TCPs are communities in which competent practitioners are engage into discussions aiming to **collaborate on specific areas such as common needs required to respond to current and emerging threats, training and demand for new expertise.** The formation of the four TCP listed below is attributed to regional security concerns. These **security concerns** are:

1. Management of migration flows and Asylum seekers;
2. Border management and surveillance;
3. Cross border organized crime and terrorism;
4. Natural hazards and technological accidents.

The four formed TCPs are the following:

- TCP1, is the M&BS community of practice established from practitioners responding to migration flows and the registration of asylum applicants,
- TCP2 is made from organisations tasked to maintain security along the borders, both land and maritime,
- TCP3 is formed from practitioners responding to threats related to fight against (organized) crime, terrorism, radicalization, return of foreign fighters and lastly,
- TCP4 whose members are practitioners responsible for preparedness and response to physical disasters, technological accidents and Natech accidents.

The following sections are presenting the initial findings across all four communities of practice.

3 TCP1 Management of migration flows and Asylum seekers

3.1 Introduction

The objective of TCP1 (community of practitioners with interest in the phenomena of migration and involved in the asylum procedures) is to foresee the activities performed by the TCP on the topic of prevention and management of migration flows. According to UNHCR, world is in the midst of a forced migration crisis, and it is expected the situation to get worse. Based on the annual Global Trends Study from the United Nations Refugee Agency[3], more than 68 million people were forcibly displaced cross the world at the end of 2017. The Mediterranean and Black Sea (M&BS) region has been in the center of this crisis given its proximity to conflict areas and the persistent economic disparity between the EU and many countries of origin. The management of the refugee crisis will be of high priority in the EU in the forthcoming years due to the continuation of the phenomenon but also due to new challenges emerging from the registration and asylum processing to integration into the societal dynamics and productive economy (relocation).

The TCP on "Management of Migration Flows and Asylum seekers" approaches the issue of migration from both technical and social point of views, thus discovering understanding the factors driving migrants/refugees/ asylum seekers to relocate to another country from their country of origin. It is concerned with the assessment of scenarios and pertinent THOR components relevant to the migration flows in the M&BS countries.

The submitted scenarios are focused on the management of migration flows and asylum seekers and investigate the challenges related to the provision of humanitarian assistance, (electronic) recording of migrants along with their needs and requirements, establishment of efficient safe and secure reception centers, integration and asylum process, relocation placing equal emphasis on the human, societal and organizational as well as the technological dimension.

Emphasis will be also given to the preventative strategies that can be adopted for the management of migrants prior to their movement in the reception countries. Additionally, there will be an approach towards the interoperability of information system between national systems and EU ones. The work of the TCP will be performed by practitioners whose daily duties is to handle the Mediterranean refugee crisis, as well as by Civil Society Organizations in the field.

3.2 Threats, risks, challenges, Priorities and the way forward

The following threats, risks and capability gaps could be taken under consideration and constitute a priority of research where it is possible based on the scenarios that will be provided for this TCP:

[3] https://www.unhcr.org/news/stories/2018/6/5b222c494/forced-displacement-record-685-million.html

- Social Media analysis for trend revealing on migration flows and statistical tools for in-depth analysis
- Prior information on procedures. Examine if SM analysis and other applications could lead in facilitating the migration movements and the final expectations of the migrants
- Examine if the use of technology solutions such as drones, patrols, thermal cameras, SIGINT, satellite monitoring can be used as preventive mechanism
- Assess if direct aid to the countries of origin can alleviate the migratory pressures
- Examine the problems with bilateral, multilateral and EU-level agreements for the safe return and readmission of irregularly entering or staying migrants and failed asylum seekers

In the coming months the analysis of the above scenarios will lead to identification of capability gap findings which will be further processes as stated in section 1.2 “MSRIA´s steps”.

4 TCP2: Border management and surveillance

4.1 Introduction

The Thematic Community of Practitioners (TCP2) is focused on the following topics:

- Border control
- Search and Rescue during maritime border surveillance operations
- Risk analysis
- Interagency cooperation
- Cooperation with third countries
- Schengen quality control mechanism
- Entry Exit System
- Border surveillance technologies
- Information Sharing
- Earth Observation

The first work carried out by TCP2, was focused on land borders. To facilitate and assist the TCP analysis synergies and collaboration with other European project (EWISA) were sought to identify capability gaps in land border surveillance, and more specifically in detecting illegal crossing activities.

4.2 Threats, risks and challenges

Europe, due to its geographical, geopolitical and economic situation in the world, has many threats and risk related to its frontiers. In addition, the Mediterranean and Black Sea region is specially affected by the migrant pressure from African countries and Middle East. The huge quantity of people trying to get into Europe, using different way (airports, crossing land borders, sea borders) is a challenge to the authorities.

A classification of threats, risk and challenge can be done taking in consideration the kind of frontier, but for all the frontiers the main challenges are:

- Detection of illegal migrants
- Detection of illicit goods
- Sharing the information between European authorities

Under these main challenges presented above there is a great number of small challenges like:

- Accommodate the ever-increasing flow of cargo and people crossing the external borders of the EU, without undue delay or with minimal intrusion, employing affordable technical and human resources.
- In maritime borders it is an important challenge to distinguish regular activities from illegal.
- The challenge of cooperation between authorities and other organizations (humanitarian) in the case of search and rescue operations.
- The control and detection of false documents.

- Detection of people carrying infectious diseases.
- Control of overstayers.
- Detect and track small boats and to distinguish them as possible threats.
- Detect illicit activities under the cover of regular shipping activity.

4.3 Capabilities and Gaps

The analysis of the second workshop for maritime border surveillance is ongoing. Here below the findings from the land border focused activities are presented, and the capabilities gaps of Earth Observation, based on the experience from Satcen.

Land Border

- **Community of trusted partners**
- **Advance return process**
- **Advance fraudulent detection**
- **Pan European database**
- **Advance CEAS**
- **Advance Risk Analysis process need to better define which risk analysis**
- **Promote EU MS – Third countries cooperation**
- **Advance cooperation between practitioners across EU MS**
- **Common operations across EU MS**
- **Security solution standardisation and certification**
- **Develop a standardised ecosystem for security solutions**
- **Support of legacy / deployed solutions**
- **Identify and remove illegal context in the internet**
- **Find counter measures to safeguard intelligence about practitioners' assets and resources deployed**
- **Promote lessons learned culture**
- **Advance technology adoption**
- **Early detection in difficult/challenging landscapes / weather conditions**
- **Advance detection capabilities**
- **Advance Common Prefrontier Intelligence picture**
- **Advance border crossing preventive mechanisms**
- **Advance border crossing detection mechanisms**
- **Advance return process**
- **Develop special forces (rapid deployment teams)**

Earth Observation and Border surveillance

- **Service timeliness**
- **Service quality**
- **Service awareness, Skills and acceptance**

Figure 6: Findings from the land border workshop activities

4.3.1 Land Borders: Capabilities-gaps

There are 24 in total (up to the current analysis phase) capability gap findings. These are the following.

Community of trusted partners	
CGF id	**Description**
2.CGF.1	Lack of an Independent authority e.g. Observatory (on a National and/or European level) with a clear mandate and mission to monitor NGO operations and other private (profit) organisations and ensure their operations are conducted within the frameworks of EU and national legislation. Organisation who are not comply with EU rules should be asked to comply, otherwise they should be registered in an exclusion list and restrict access to EU/National funding, facilities and products (information sharing)

Advance return process	
CGF id	**Description**
2.CGF.2	Improve existing process and procedures with EU third countries and EU MS for return processes in the case of non-eligibility for asylum. The improve should be driven by EU principles and should consider all EU MS instead of transferring back and forth in the EU the non-successful applicants.

Advance fraudulent detection	
CGF id	**Description**
2.CGF.3	Improve current capabilities related to detection of falsified (fraudulent) documents. Practitioners should be equipped with the right tools and training to detect also falsified multimedia material which is often supplied as evidence.

Promote EU MS – Third countries cooperation	
CGF id	**Description**
2.CGF.8	Use of intelligence is one part of the problem. You can utilise OSINT, SIGINT, HUMINT, IMINT (open source, signal, human and imaginary) sources but without cooperation with 3rd countries you cannot raise an alert/readiness level at the other side of the borders to prevent/suppress the threats.

Advance Risk Analysis process	
CGF id	**Description**
2.CGF.7	Initiative to develop common risk analysis tools and offer training to practitioners who will be using those. Common tools and methods are required to produce risk analysis across all EU MS. Risk analysis should be performed in all three levels. Local, National and Regional. Training of how the practitioners shall use these tools should be offered. The tools should provide • at local level - awareness so the practitioners will be briefed beforehand what they will most likely encounter; • at national level Risk Analysis will allow better utilisation of operational forces; • at regional level will assist the collaboration of EU MS in M&BS region Artificial Intelligence should be used. BGA need to train their practitioners to use the same risk analysis tools and have similar risk scales across M&BS countries and a common terminology for risk

Pan European database	
CGF id	**Description**
2.CGF.4	Having a system of systems (interconnection of databases) where practitioners from all EU MS have access. However, this necessitates a unique identification of all applicants. The system shall also include fields for tattoos and wounds as they recorded in the first EU MS. Other fields shall include results from mental examinations or age detection results.
2.CGF.5	Records for medical/mental diagnosis are not accessible from all EU MS states authorities

Advance cooperation between practitioners across EU MS	
CGF id	**Description**
2.CGF.9	Before asking and seek cooperation between EU MS and 3rd (neighbouring) countries you need to ensure cooperation is achieved across EU MS.

	Further to (explore synergies and cooperation across EU MS) you can define a doctrine of cooperation. As such the use of means currently not used near the borders (e.g. drones) can be enforced in the outside EU borders if it is accepted as an EU practice

Common operations across EU MS	
CGF id	**Description**
2.CGF.10	Lack of advanced cooperation schemes / exchange programs (e.g. border guard practitioners exchange program across EU MS at outside borders) between EU and 3rd countries, that will shape and promote the legal, operational, training and logistical framework for joint activities and cooperation on a daily basis (e.g. patrolling)

Security solution standardisation and certification	
CGF id	**Description**
2.CGF.11	Lack of commonly accepted technology standards (e.g. military) for the security ecosystem. Currently the security solutions are standardised as stand-alone systems, but not standardised / certified for deployment and interworking with existing systems.

Develop a standardised ecosystem for security solutions	
CGF id	**Description**
2.CGF.12	Open/common interconnection interfaces for systems and solutions that will be deployed in the borders. Further to 2.CGF.11 an approach is required to interconnect (with minimum effort) solutions from different vendors and ensure interworking between different subsystems (e.g. common analytics from various day and night cameras and interworking with deployed radars and vibration / proximity sensors)

Support of legacy / deployed solutions	
CGF id	**Description**
2.CGF.13	Backwards compatibility of new security solutions with command and control systems. If possible, interworking of new systems with existing deployed equipment

Identify and remove illegal context in the internet	
CGF id	**Description**
2.CGF.14	Technology should assist the detection of content in the web which supports/promote illegal activities. Upon identification of inappropriate context, the context should be removed, or access should be blocked.

Find counter measures to safeguard intelligence about practitioners' assets and resources deployed	
CGF id	**Description**
2.CGF.15	Practitioners would like to minimize and/or eliminate risks related to perpetrators and adversaries collecting information about deployed systems and resources and use more sophisticated methods for prevention and detection of illegal activities.

Promote lessons learned culture	
CGF id	**Description**
2.CGF.16	Use systems to log/archived records of decisions and use de-briefings to highlight wrong calls. Use lessons learned for awareness and training of practitioners (analysis teams). Lessons learn from past incidents will assist the analysis tasks.

Advance technology adoption	
CGF id	**Description**
2.CGF.17	Amend regulatory framework for all new technology solutions and push for technology adoption in practitioner's organisations.

Early detection in difficult/challenging landscapes / weather conditions	
CGF id	**Description**
2.CGF.18	Technology solutions to provide detection in forest areas are needed taking into account the terrain characteristics and the lack of power sources.

Advance detection capabilities	
CGF id	**Description**
2.CGF.19	Advanced analytics (video, data) are required for detection and awareness of individuals who are detected near the borders. This capability is being complemented by cooperation between EU MS and third countries (2.CGF.2).

Advance Common Prefrontier Intelligence picture	
CGF id	**Description**
2.CGF.20	A solution that will offer the desired prefrontier intelligence picture for various border types is required. This involves intelligence from land border, maritime borders and intelligence sharing among practitioners from different discipline organisation in the same country (initial) and subsequent cooperation between multidiscipline organisations across the borders (from different EU MS)

Advance border crossing preventive mechanisms	
CGF id	**Description**
2.CGF.21	Better preventive mechanisms are needed along the borders. Legislation and procedures between EU and third countries should be adapted.

Advance border crossing detection mechanisms	
CGF id	**Description**
2.CGF.22	Advanced detection and surveillance methods are required for “difficult” terrain (forest, mountain) areas. Solutions should address the challenges of power availability in these areas and provide solutions for their connectivity with command and control centres

Advance return process	
CGF id	**Description**
2.CGF.23	More sophisticated detection methods are required to prevent smuggling to normal Border Crossing Points (BCP) and along borders in general.

Develop special forces (rapid deployment teams)	
CGF id	**Description**
2.CGF.24	Development of Rapid deployment teams with certain capabilities and skills (translators, social workers, medical staff) to offset organizational limitation of the public sector.

4.3.2 Earth Observation and Border surveillance: Current capabilities and gaps

The European Commission relies on entrusted competent entities, in order to implement Copernicus, the Earth Observation programme of EU [RD.6-1], and particularly its service component. The Delegation Agreement between FRONTEX and the European Commission on the Implementation of the Border Surveillance Component of the Copernicus Security Service, was signed on the 10th of November 2015. The agreement entitles FRONTEX to act as the single and central point for the acquisition, fusion and delivery of these services. FRONTEX delivers these services in cooperation with several partners, including the European Maritime Safety Agency (EMSA), the EU Satellite Centre (EU SatCen), the European Fisheries Control Agency (EFCA), and other commercial partners [RD.6-2].

FRONTEX and the National Coordinated Centres (NCCs) established in the Member States as the backbone of EUROSUR, can request satellite-based services, which cover a large range of needs spanning from operational monitoring of activity in the border to strategic analysis and mapping. As reported in Observer [RD.6-3] FRONTEX currently delivers through EUROSUR a set of Border Surveillance services in the framework of the Copernicus programme. These services cover various operational needs to improve situational awareness, support strategic allocation of resources, perform proactive analysis to detect patterns of potential interest on satellite imagery etc.

The **value** that the Earth Observation services can offer depends on:

i) **timeliness** of service,

ii) **quality** of service,

iii) service **awareness** of the persons using it,

iv) basic **skills** to understand the limitations and opportunities offered,

v) institutional **acceptance**.

The **timeliness** of service delivery depends on several factors, including: i) satellite orbit, ii) ground station visibility, iii) cloud conditions (for optical images), iv) automation of image processing chains, v) imagery analysis requires manual work, vi) dissemination channels, vii) organisational procedures.

The **quality** of service delivery depends on factors relevant to: i) spatial resolution of the imagery, ii) consistency of observations, iii) image analysis skills, iv) endurance of observation, v) the nature of activity to be observed and its manifestation during observation window of opportunity, vi) observation frequency.

Service **awareness** is important to penetrate institutional structures and reach practitioners in the Member States. Awareness sessions and workshops are necessary to build awareness on the services. This is currently tackled under Commission´s user uptake actions. In addition, basic **skills** can be obtained by organising training sessions. These processes will boost institutional **acceptance**, as more practitioners become aware of the capabilities and use them in their work.

As noticed above the value, timeliness and quality of service delivery cannot be solely tackled by technological means, as organisational procedures need to be streamlined to enable effective dissemination. Moreover, the institutions involved in service delivery are required to perform actions to improve service awareness, while users are also required to communicate requirements and use cases, which can assist in service evolution. It is through these interactions that services will be extended to cover current capability gaps.

Service timeliness	
CGF id	**Description**
2.CGF.25	Gaps on the satellite imagery acquisition side: Need for integrated solutions to deliver images in real-time manner (Technology). Need for short cut-off times (i.e. from request to satellite image acquisition).
2.CGF.26	Gaps on the analysis side: Need to standardise and automate IMINT extraction (Technology).
2.CGF.27	Gaps on the dissemination side: Need for system-to-system approaches to avoid red tape (Technology, Organisation).
2.CGF.28	Gaps on the organisation procedures: Need to modernise procedures and workflows to account for new technological developments, allowing system-to-system tasking, delivery and dissemination (Technology, Organisation).

Service quality	
CGF id	**Description**
2.CGF.29	Gaps on the payloads and platform side: Need to improve the spatial resolution of satellite optical cameras and the area covered per observation (Technology).
2.CGF.30	Gaps on the endurance side: More persistent systems are required to enable longer endurance over border areas (Technology).
2.CGF.31	Gaps on the understanding of the observable features/events: Higher revisit capabilities are required (Technology).
2.CGF.32	Night observation capabilities from space are required, due to the fact that relevant activity usually takes place outside of current observation windows (Technology).
2.CGF.33	Better interaction between producer and user/requestor is required. Trust needs to be established to enable proper exchange of information, which

	will lead to more relevant and better-informed IMINT reports (Human, Organisation).

Service awareness, Skills and acceptance	
CGF id	**Description**
2.CGF.34	Gaps on current education curricula: Currently Earth Observation is regarded a high technological asset, regarded by many practitioners as far from their real tasks (Human).
2.CGF.35	Limited knowledge of the available (through EUROSUR) IMINT services is accompanied by reluctance to task the services and profit from them (Human, Organisation).
2.CGF.36	Service acceptance is connected with success cases, which prove the value that can be delivered (Human, Organisation).

4.4 Identified Solutions and Challenges

TCP2 activities are ongoing. As such not all findings were consolidated at this time, so the activities to identify potential solutions to fulfil those Capability Gaps and perform requirement analysis for short/mid and long-term Horizons did not start.

4.5 Priorities

Similarly, the activities for this task have not started. The activities to prioritise the identified solutions and challenges can only start when the “identified solutions task” develops results.

4.6 Conclusions and the way forward

TCP members in the coming months will include the findings form the Maritime surveillance workshop. The consolidates list of capability gaps for both land and maritime borders will be shaped in the next 18M. During this time, an initial list of potential solutions will be considered.

5 TCP3: Cross border organized crime and terrorism

5.1 Introduction

The general objective of this community of practitioners is to analyse the existent threats in the field of fight against cross border crime and terrorism. As described in sections 1 and 2, the identification of practitioners capability gaps will be performed using the scenario-driven approach, where over the last two months, community members are contributing in order to get the most relevant conclusions in assessing future and emerging threats and definition of the regional security priorities. In order to do so, each scenario is being taken through, the following steps:

- **Identification and analysis of the current state** in the specific field of this work package. By using a scenario-based visioning method, the emerging and future threats are being evaluated. Within the scenarios, they are being evaluated: modus operandi, routes, stakeholders involved, risk evaluation (probability and impact), profile of the criminal groups, profile of the victims etc.
- **Identify the gaps of the existent law enforcement architecture**, which are exploited by the organised crime groups in order to accomplish their criminal activities. Within the scenarios, they are being analysed the benefits and impediments regarding security procedures, technical infrastructure and cooperation mechanisms in place.
- **Identify the desired future state and the needs of the law enforcement agencies**, which can raise the effectiveness of the strategies in combating cross border crime and terrorism. As an expected outcome of the analysis of each scenario, recommendations and conclusions are being elaborated regarding the issues that had to be foreseen, mistakes that could be prevented and challenges that have to be addressed.

The specific objectives of this community are the following:

Obj.4-1 Elaboration of relevant scenarios in the field of fight against cross border crime and terrorism and going them through all the required stages of the analysis, in order to generate knowledge: definition, evaluation, prioritization, analysis, interaction between project partners, generating conclusions.

Obj.4-2 Applying the THOR impact assessment template for the selected scenario, with its for dimensions: Technological, Human, Organisational, and Regulatory. For each one of dimensions, relevant applicable topics will be identified.

Obj.4-3 Organise one table top exercise between practitioners, regarding the selected scenario, in order ensure an in-depth analysis of the criminal activities and of the measures which can be taken by the law enforcement agencies. Dedicated analysis techniques will be applied, using dedicated analysis software: link analysis, event charting, flow analysis, GIS representations.

Obj.4-4 Ensure the transfer of knowledge, by elaborating recommendations and reporting the outcomes.

5.2 Threats, risks, challenges, Priorities and the way forward

Until now seven scenarios were developed, and the TCP is working on their elaboration. The scenarios developed considered the following threats:

1. New forms of terrorism - Online Radicalization;
2. Smuggling of illicit drugs – Smuggling of heroin from Turkey to countries from West Europe;
3. Smuggling of illicit drugs - Smuggling of cocaine by carriers;
4. Smuggling of illicit goods - Nuclear Material Trafficking;
5. Smuggling of illicit goods - Illicit usage of drones in smuggling drugs and firearms;
6. Detection of fraudulent documents;
7. Drug trafficking scenario, elaborated in collaboration with I-LEAD

In the coming months the analysis of the above scenarios will lead to identification of capability gap findings which will be further processes as stated in section 1.2 “MSRIA´s steps”.

6 TCP4: Natural hazards and technological accidents

6.1 Introduction

The fourth Thematic Community of Practitioners (TCP4) is focusing on natural hazards (wildfires, floods, earthquakes, tsunamis) and natech, i.e. natural hazard-triggered technological accidents.

The first cycle of work, started in May 2019, was focused on identifying capability gaps in wildfires, and more specifically in fire management in the specific context of wildland-urban interface. Consequently, the results presented by TCP4 in this first issue of the MSRIA only cover this area.

6.2 Threats, risks and challenges

The Mediterranean and Black Sea region has been the most vulnerable European region to a wide range of natural disasters.

Indeed, compared to the rest of Europe, the Mediterranean basin is especially exposed to flash-floods, which are amongst the costliest and deadliest natural disasters especially in an area where population growth is particularly dynamic.[4]

Earthquakes and forest fires, and according to IPCC reports the most likely to experience the highest impacts of climate change under any examined scenario.

Tsunamis are also a concern in the Mediterranean region. They can occur in European waters due to earthquakes caused by the African Plate drifting northwards underneath the Eurasian Plate. While 10% of all tsunamis worldwide occur in this region, on average, one disastrous tsunami takes place in the Mediterranean region every century. “The possible scale of a tsunami in the Mediterranean is quite comparable with the catastrophic event of December 26, 2004 in the Indian Ocean. Earthquakes in the Mediterranean region can reach a magnitude of 7.5 to 8, and accordingly wave heights of five to six metres are within the realms of possibility”[5].

Recent related disasters show an exponentially increasing trend (as processed EM-DAT evidence shows). Enhanced measures need to be drafted and implemented at a local, national and regional level to stabilize the impacts of disasters, such as contingency plans, risk barriers and security and safety policies implementation, thus collectively strengthening resilience of Mediterranean societies.

[4] G. , E. Borga, L. Marco, M. Carmen, . Maouche et al., Mediterranean extreme floods and flash floods (Sub-chapter 1.3.4) In Allenvi (Ed.) The Mediterranean Region under Climate Change. A Scientific Update, pp.133-144, 2016.

[5] Dr. Jörn Lauterjung from the GFZ, https://www.eskp.de/en/natural-hazards/tsunami-risk-in-the-mediterranean-sea-935107/

In addition, as a consequence to the increase of natural hazards, the cascading effects on industrial facilities are now thoroughly examined as the development by the Joint Research Center of a database specifically dedicated to the mapping of “natech” events shows.

Thus far, the community of TCP4 worked on seven scenarios, that are representative of the priorities identified in this field.

Five scenario concern pure natural hazards :

- wildland urban interface fires (2), and a wildfire crossing a border (1);
- Mediterranean event, flash flood (1);
- Earthquake (1).

While the two remaining scenarios are focused on natech events:

- Tsunami in Crete with industrial cascading effects (1).
- Earthquake in Turkey with hazmat impact (1).

As explained above, only wildland urban interface fires area has been thoroughly investigated in this first cycle.

6.3 Capabilities and Gaps

6.3.1 Overview of identified capability gaps in Wildland-Urban Interface Fire Management

The capability gaps presented below are derived from the wildland urban interface fire management workshop initiated by MEDEA project and co-organized with FIRE-IN[6], WUI-View [7]and HEIMDALL [8]projects as part of the Mediterranean Security Event 2019 that took place in Crete (GR) between 28 and 30/10/2019.

The figure below (7) depicts the ten (10) capability gaps that were identified and discussed during the workshop, plotted over the four strategic pillars of the European Civil Protection.

[6] https://cordis.europa.eu/project/rcn/209950/en

[7] 2018 Call - ECHO (Agreement Nº ECHO/2018/826522)

[8] https://cordis.europa.eu/project/rcn/210221/factsheet/en

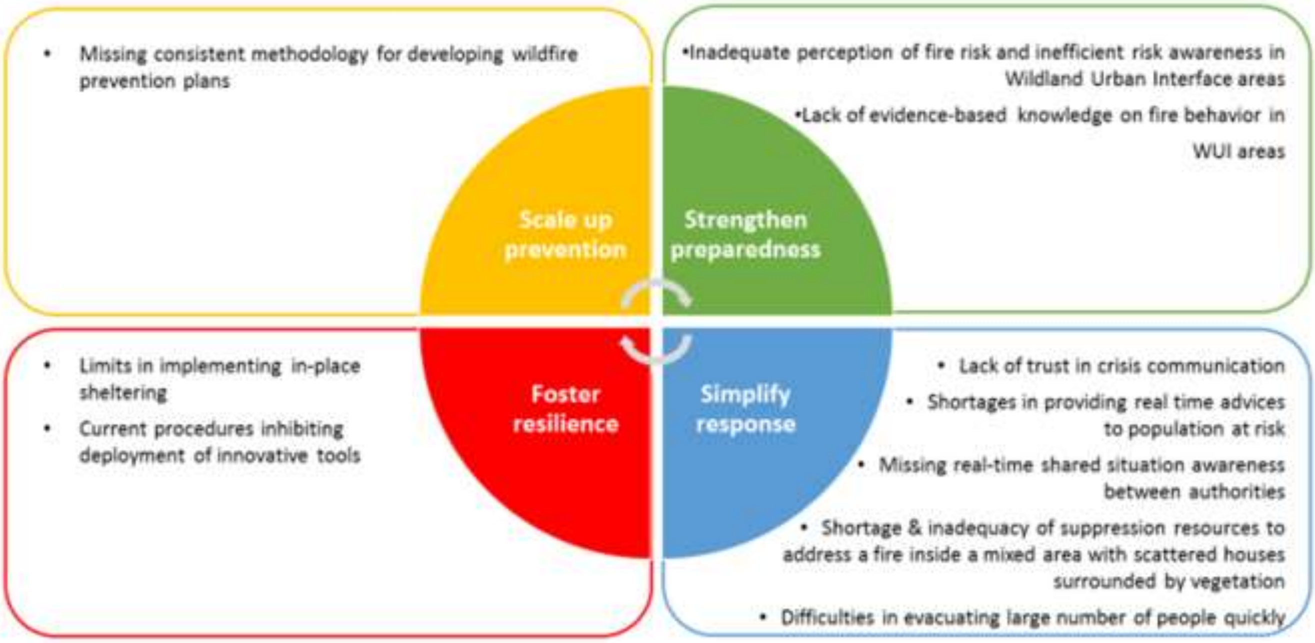

Missing consistent methodology for developing wildfire prevention plans
•Inadequate perception of fire risk and inefficient risk awareness in Wildland Urban Interface areas
•Lack of evidence-based knowledge on fire behavior in WUI areas
Scale up prevention
Strengthen preparedness
Foster resilience
Simplify response
Limits in implementing in-place sheltering
Current procedures inhibiting deployment of innovative tools
Lack of trust in crisis communication
Shortages in providing real time advices to population at risk
Missing real-time shared situation awareness between authorities
Shortage & inadequacy of suppression resources to address a fire inside a mixed area with scattered houses surrounded by vegetation
Difficulties in evacuating large number of people quickly

Figure 7: Capability Gap findings from WUI fire scenario analysis

6.3.2 Detailed capability-gaps and associated challenges

This section presents the ten capability gaps in more details, with associated sub-challenges and proposals for potential solutions, as discussed during the workshop.

Inadequate perception of fire risk and inefficient risk awareness in Wildland Urban Interface areas	
CGF id	**Description**
4.CGF.1	Lack of security culture: wildfire risk prevention isn't integrated in the mindset and lifestyle of the citizens living in the WUI. Tourists and visitors of fire-prone areas are more vulnerable than other groups, since they have limited knowledge of the area and the local risks. Neither perception nor ownership of fire risk: most citizens remain inactive even if they are informed of the fire risk. Systematic risk communication and organized citizen awareness campaigns are missing for WUI areas.
Proposals and potential solutions	✓ **Awareness raising** programs at community level based on social sciences, avoiding one-size-fits-all approach, adapted to various groups and to community specificities.

	✓ Continuous **education and training** of groups of citizens in WUI areas based on carefully designed material (printed, video, tv …). ✓ Creation of **active groups** (volunteers with uniform and equipment). ✓ Organize community of practice based on joint education, training and **exercises** of multi-stakeholders' groups (including the citizens). ✓ Share citizens' memories and experience of **past events** and integrate lessons learned from past WUI fires in the risk culture**.** ✓ Use local community elements (schools, local opinion leaders, touristic companies, campsite owners) to scatter a security culture. ✓ Suitable risk communication for **tourists and visitors**, (consider language barrier) regarding local risks as part of security culture. ✓ Fire safety and security programs and exercises for **schoolchildren.** **Meteorological risk-based preparedness** organization (simple rules for alerting local communities and increase citizen readiness level).

Missing consistent methodology for developing wildfire prevention plans	
CGF id	**Description**
4.CGF.2	Stakeholders (operational services, local authorities, and homeowners/residents) elaborate prevention plans individually.
Proposals and potential solutions	✓ **Standardization** of a methodology. ✓ **Impact-based fire risk analysis** for wildfire prevention planning. ✓ Involvement of **local** professionals and residents in fire prevention.

Lack of trust in the crisis communication	
CGF id	**Description**
4.CGF.3	People don't know where to get reliable information.

Proposals and potential solutions	✓ Identification of the trustworthy authority. ✓ Control over disinformation and spreading of fake news (VOST support). ✓ Take advantage of social media.

Shortages in providing real time advices to population at risk (crisis communication)	
CGF id	**Description**
4.CGF.4	People do not receive, understand or follow recommendations.
Proposals and potential solutions	✓ Massive alert procedures and capability to reach out to people in degraded conditions (reverse 112). ✓ Capability to precisely identify people to warn (warning messages need to be accurately location based otherwise the population discard these alerts as unsolicited messages). ✓ Early warning solutions and risk communication methodologies. ✓ Adaptation of communication means and messages to specific groups' needs (elderly, children, tourists, disabled people…). ✓ Take into account language issue for tourists. ✓ Role of municipalities through preparation and activation of municipal crisis plans

Missing real-time shared situation awareness between the authorities involved in firefighting.	
CGF id	**Description**
4.CGF.5	Lack of communication, cooperation and information-sharing culture between different authorities. No interoperability of systems across organisations. Plans are shared between agencies but not integrated. Missing culture and infrastructure to share Common Operational Picture (COP) during the incident (e.g. fire growth, weather conditions, road blockages etc.) between involved services.

	Missing of a jointly accepted methodology for Risk Assessment & Resources Analysis.
Proposals and potential solutions	✓ Development of common procedures. ✓ Real time imagery shared among services. ✓ Robust data transfer system. ✓ Common Operational Picture (COP) solutions.

Lack of evidence-based knowledge on fire behaviour in WUI areas	
CGF id	**Description**
4.CGF.6	Difficulty to accurately anticipate the fire development and the cascading effects. Heterogeneity of the conditions in the Wildland Urban Interface, notably concerning fuel types (buildings, gardens and natural vegetation) and quantity. Scattered presence of numerous people in an actively burning area Lack of risk assessment models adapted to WUI and new fire behaviour.
Proposals and potential solutions	✓ Development of new knowledge on fire behaviour in WUI areas (addressing both wide-area firefighting and people safety). ✓ Adaptation of risk assessment models to WUI and changing fire behaviour. ✓ Development of fire propagation models able to accommodate specific type of fuel (ornamental vegetation, hedges, buildings) and the heterogeneity of conditions at small scale.

Shortage and inadequacy of fire-suppression resources to address a fire inside a mixed area with scattered houses surrounded by vegetation	
CGF id	**Description**
4.CGF.7	No specific knowledge exists concerning wildfire management in WUI, which is a very difficult and non-homogeneous environment (including human presence).

	Missing geographic information on people and buildings in need to be protected during fire. Challenges in WUI-firefighting training of fire-fighters. No specific firefighting means, either terrestrial or aerial, suited for intervention in the WUI exist.
Proposals and potential solutions	✓ WUI-specific training of fire-fighters, volunteers and residents. ✓ Specific risk indexes for WUI areas. Define exposure and vulnerability of WUI areas (develop WUI fragility curves to wildfire). ✓ Specifications for vehicles and equipment to be used in WUI fire suppression efforts. ✓ Identification of specific risk and protection (example of gas tanks) for first responders.

Difficulties in evacuating large number of people in a small amount of time while preventing that people get trapped while trying to escape	
CGF id	**Description**
4.CGF.8	Formal guidelines and evacuation plans do not exist for WUI settlements. Evacuation concept may be misused and eventually create wrong impression on reducing fire impact.
Proposals and potential solutions	✓ Decision support solutions for fire safety choosing between evacuation and sheltering (evacuation risk assessment, demographics characteristics, availability of resources, coordination with Police). ✓ Integrated and documented evacuation plans (adaptable to time period, real time traffic situation, including pre-identification of safe places, and installation of road signs). ✓ European guidelines for developing local evacuation plans. ✓ Elaboration and improvement of our understanding on the evacuation potential and capabilities in case of wildfire in WUI areas, notably by developing evacuation modelling.

Limits in implementing in-place sheltering	
CGF id	**Description**
4.CGF.9	Misconceptions concerning the use of houses as shelters. No specific guidelines exist for home-protection in WUI areas. No building standards in vulnerable WUI environments. People do not feel safe in their houses surrounded by fire.
Proposals and potential solutions	✓ Improve shelters environment: vegetation and other fuel storage control around houses. ✓ Development of a European building code (materials) for fire resistant and resilient building structures in WUI areas. ✓ Standard self-protection guidelines and recommendations for homes (passive self-protection systems) & homeowners at WUI. ✓ Performance comparison between evacuation and sheltering.

The current procedures inhibit deployment of innovative tools	
CGF id	**Description**
4.CGF.10	Mismatch between established procedures and capabilities enabled by innovative solutions.
Proposals and potential solutions	✓ Adaptation of procedures to benefit from possibilities offered by new technologies.

6.4 Identified Solutions and Challenges

This phase has not yet started in TCP4.

6.5 Priorities

This phase has not yet started in TCP4.

6.6 Next steps

TCP members in the next 18 months will finalise their analysis from the WUI fire workshop. Existing solutions will be considered by TCP members with the assistance of practitioners.

7 Conclusions

The first 2019 edition of the MSRIA reflects the state-of-play of the outcomes from the threat scenarios and the respective gap analyses performed by the different Thematic Communities of Practitioners.

The current document aims at introducing the rationale behind the MSRIA. The MSRIA is part of MEDEA's WP 6, responsible for ensuring the transfer insights to the right target addressees. This process, which acknowledges the different logics, time-frames, interests, and capacities of all involved security stakeholders, helps turn findings and insights out of the practitioner-led scenarios into Actionable Knowledge, which should be useful, usable and factually used by policy makers, and security providers. MSRIA will leverage capability-building activities performed in other relevant Networks of Practitioners, as well relevant Research & Innovation, and Coordination & Support Actions.

MSRIA delivers on MEDEA's core objectives, which are the following ones: improve the collaboration among institutions and actors from different disciplines; define the Mediterranean and Black Sea regional security priorities; build what is referred as scenario-driven technology roadmap.

The MSRIA is a living and adaptive document, that will be updated throughout the life of this project in its four consecutive editions, by aiming at providing stakeholders sensitive recommendations not only for the R&D community, but also in terms of future policy actions.

This document aims, also, to explain how the MSRIA can be considered as a circular strategic tool within MEDEA. MSRIA should not be considered as an end of the TCPs activities, but also a tool that will strengthen their engagement and their role in future networking. MSRIA is a tangible incentive for all relevant actors in the security-related mandate, both from the public as well as the private sector, to join the activities in the course of the project activities.

MSRIA is the product of MEDEA network members and external invited or associated practitioners engaging in scenario-based assessment of present, emerging and future threats with the objective of being prepared to adopt a proactive mind-set to effectively respond to introduce new and innovative concepts and capabilities. This process will be carried out under the Technology evaluation and prioritization for each TCP.

It is clear that a main concept behind the MSRIA is Co-Creation. This is the stakeholder-inclusive definition, generation, and implementation of knowledge through all involved stages of the project. At the same time, this approach, since it is not an academic top-down implementation of ready-made models, comes together with certain delays in the constitution and workings of each of the four TCPs. For this reason, the maturity of the agendas recommended to each of the TCPs respectively, may vary depending on the ripeness stage of the scenario elaboration and THOR assessments performed with each of the TCPs.

The results in each TCP MSRIA roadmap, provided that they have reached a satisfactory degree of maturity, will be able to propose a **prioritised agenda** out of the **mapped options.** However, even the THOR-elaborated aspects of R&D needs, and the gaps analyses are included in the first editions of the MSRIA, since they build the basis for a roadmap.

The Mediterranean and Black Sea network of practitioners is composed of four TCPs. As defined in previous sections, TCPs are communities in which competent practitioners are engage into discussions aiming to collaborate on specific areas such as common needs required to respond to current and emerging threats, training and demand for new expertise. The formation of the four TCPs listed below is attributed to regional security concerns, as explained below:

Table 6: Applicable Documentation

TCP #	Focus/Security concern	Profile of the Practitioners engaged
TCP1	Management of migration flows and Asylum seekers	M&BS community of practice established from practitioners responding to migration flows and the registration of asylum applicants,
TCP2	Border management and surveillance	Organizations tasked to maintain security along the borders, both land and maritime.
TCP3	Cross border organized crime and terrorism	Practitioners responding to threats related to fight against (organized) crime, terrorism, radicalization, return of foreign fighters
TCP4	Natural hazards and technological accidents	Practitioners responsible for preparedness and response to physical disasters, technological accident and natech accident.

The main outcomes are from TCP2 and TCP4. For these TCPs some workshops have been carried out, and they seem to be the best way to get the information from the practitioners.

In the current moment of the project only capability gap analysis has been developed and the results are:

- TCP1 has defined the main scenarios where they will be focused on the next months to identify gaps.
- TCP2 has defined 36 capability gaps, 24 in the land border subtopic, and 12 in Earth Observation.
- In TCP3 seven scenarios has been developed.
- In TCP4 10 capability gaps have been formulated in Wildland-Urban Interface Fire Management in TCP4.

As a briefing from TCP2 we can say the main needs are in the interoperability between countries and organizations involved in the land border management. Sharing databases, information, connectivity between different technologies are at the same level than the need to have new technology for an early and more accuracy detection.

In TCP4 the main needs detected for wildland urban interface fire management are related to the quality of the information, and the needs to share it, not only between authorities but with the population.

The information sharing it seems to be one the most important capabilities for all the TCPs.

The next step is to analyse the capability gaps detected using the THOR methodology in order to find the attributes in the four dimensions (Technological, Human, Organisational and Regulatory) and process to their prioritisation. These actions will be concluded for all four TCPs in the 2nd edition of the MSRIA (by M30) as far as the short-term scenario horizon is concerned.