Journal of Research in Health Sciences
ISSN: 2228-7809 | https://jrhsjournal.com

Identifying and Prioritizing Clinical Care Capabilities in Regional Health Systems

Dr. K. Laurent[1], Dr. M. Petrov[2], Dr. S. Okoye[3]*

[1] Department of Clinical Pharmacology, University of Paris-Saclay, Paris, France
[2] Department of Neurology, Sechenov University, Moscow, Russia
[3] Department of Community Medicine, University of Ibadan, Ibadan, Nigeria

Abstract. Scenarios are frequently used within methods for planning and designing variations of the future security landscape. This paper presents the methodology applied to security scenarios used for the objectification of the security practitioners required capability ranking under the framework of MEDEA project. A process developed to determine the missing security capabilities– from the practitioner's operational point of view- is analysed. The approach for designing, building and analyzing a number of scenarios, developed by practitioners from a variety of security organisations operating in Mediterranean and Black sea countries is presented. The objective is to identify a list of regional security priorities that will be further processed by security experts and solution providers to develop a capability development roadmap regarding security challenges and threats in the Mediterranean and Black Sea region projected in the short, mid and long-term.

Keywords: THOR methodology, migration and asylum seekers, border management, fight against crime and terrorism, natural disasters, technological accidents, Mediterranean security research agenda, scenario, Horizon scanning, emerging threats.

1 Introduction

The countries located at the Southern and Southeastern Europe are neighboring to some of the most unstable regions in the world. The Mediterranean and Black Sea (M&BS) region — a crossroad between Europe, Africa and the Middle East — is experiencing the last decades an unprecedented regional security crisis. In the vicinity of the South and Eastern EU external borders, humanitarian, security and climate change challenges affect the life of a large number of vulnerable populations, which leads to regional instability. As a result, the number of migration and asylum seekers to Europe is continuously increasing with a significant impact to border controls and security resilience. Moreover the M&BS region experiences also increased organized crime activity and terrorism issues attributed to the return and relocation of foreign terrorist fighters to EU countries. From another viewpoint, the rapid social and economic development during the last decades have influenced rural and urban landscapes in the Mediterranean. Wildland-Urban Interface fires occur more and more often, while their severity and consequences are adding new dimensions to the current risk profile of these regions. As a result of the above, the security practitioners operating in the Mediterranean and

Black Sea countries are facing more threats than ever before. There is a strong demand for new capabilities in fighting against organised crime, in responding to natural disasters and technological accidents, in protecting large energy infrastructures of European interest, in managing a continuously increasing number of migrant and asylum seekers and in supervising the external European borders in a politically fragile and religiously rigid region. Scenarios of deliberate migration flow, which may lead to radicalization and extremism challenges combined with epidemic or pandemic crisis can't be considered unrealistic. In this context, MEDEA project[1], aims to develop a regional network of security practitioners that will be able, using a scenario-based approach, to identify and analyse the research priorities to develop the desired capabilities from the operational viewpoint. This paper presents the methodology that will assist the project members to achieve their research objectives.

2 The MEDEA Network of Practitioners

The MEDEA is a five-year Coordination and Support Action [1] (CSA) under the Horizon 2020 topic of SEC-21-GM-2016-2017 - Pan European Networks of practitioners and other actors in the field of security [2]. The MEDEA's scope is to establish and further develop a regional Network of Practitioners (NoP) engaged in security operations in the M&BS region to involve them in EU R&D activity. To accommodate the interest and facilitate the co-existence of practitioners from different countries with different operational interest, MEDEA NoP established the following four working groups organized as Thematic Communities of Practitioners (TCP) [3]:

TCP1: Managing of migration flows and asylum seekers
TCP2: Border management and surveillance
TCP3: Fight against cross border organised crime and terrorism and
TCP4: Natural hazards and technological accidents.

The TCPs were stuffed initially with consortium members, based on their operational and professional experience and knowledge in relation to the subject of the TCPs. These groups were extended then including First Responders, Border Guards, Firemen, Police Officers, Civil Protection and Emergency teams, Humanitarian/social workers, Army officers, policy makers and advisers participating as experts and peers in the project activity. The aim is to identify, in a professional community setting, existing barriers and capability gaps that prevent security practitioners to respond effectively to a series of regional and common security threats. The findings and conclusions from all four TCPs will be analysed in context of MEDEA activity using a four-dimensional analysis known as THOR (Technology, Human, Organisational, Regulatory) as explained later in this paper.

MEDEA network has a layered structure with the project partners (consortium) at the core, the practitioners (TCPs) in the middle, the associated experts and R&D providers as third layer and the decision and policy makers who are placed at the external layer. All these groups form the MEDEA regional network. The challenge of MEDEA

[1] Mediterranean practitioners' network capacity building for effective response to emerging security challenges

consortium is to trace the capability radius that link these layers starting from the center of the structure to reach the external layer.

The external layer is where the findings of the TCPs and the results of the THOR analysis will be reported, by publishing them in the Mediterranean and Black sea Security Research and Innovation Agenda (MSRIA).

3 MEDEA methodology building blocks

There are three main building blocks defined in MEDEA methodology, which are used to define challenges, identify capability gaps and elaborate potential solutions in relation to each of the four TCPs. These are: (1) a scenario development block where security practitioners from the M&BS region will first develop at organisational level and then jointly elaborate with other stakeholders from their TCP operational scenarios that will be used to identify their needs for enhanced or new operational capabilities; (2) an impact analysis block for the needed capabilities. A four-dimensional analysis will examine the impact of the requested capabilities with respect to the Technology, the Human, the Organisational and the Regulatory dimension. Based on the findings from the impact analysis, (3) the practitioners will arrange their expectations in three horizons while at the same time they will document and objectify their priorities to acquire the respective capabilities in three distinct time horizons: short term, mid-term and long term.

The gap analysis process, which MEDEA adopted, is structured in four consecutive steps from the problem definition, to scenario, multidimensional analysis and strategy development (Figure 1).

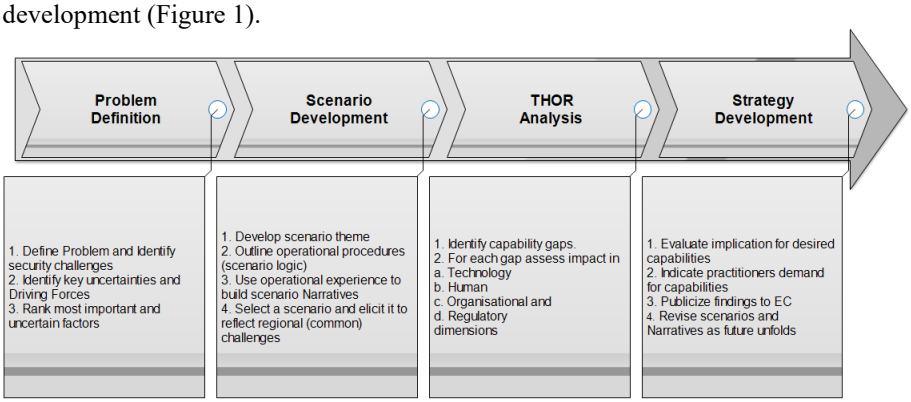

Fig. 1. MEDEA scenario development, impact analysis and recommendations process

4 Problem definition and scenario based approach

Taking as starting point the scenario definition given by Carrol (1999) where "[…] scenarios are stories about people and their activities" [4], MEDEA defines scenarios as operational cases concerning security practitioners, their activities and their duties. Scenarios are used by many security institutions for a variety of purposes (planning, exercises, operations etc.). As example, the US Defence Modelling and Simulation

Office (DMSO) uses scenarios to establish "An initial set of conditions and timeline of significant events imposed on trainees or systems to achieve exercise objectives". To address the needs of identifying operational gaps in the capabilities of security practitioners, MEDEA adopted the relative approach of Whitworth et al [5] who considers scenario as "a representation of the state, and present actions, of a set of animate and/or inanimate objects, so as to permit the exploration of, or reasoning about, their future state and the events that lead to it.". This approach is applied to reconstruct past security incidents properly. As such, MEDEA scenarios can assist practitioners, from different security organisations, to describe new incidents related to similar threats that may occur modified somehow. The approach used is aligned to the works of Rigland and Schwart (1998) [6] and Van der Heijden (2002) [7] who demonstrated how scenarios can be used as a planning instrument for strategic foresight. In MEDEA, practitioners use scenarios as a mean to describe potential future situations that are attributed to present circumstances. A repository of scenarios corresponding to interesting and important security cases related to the topics of the four TCPs of MEDEA has been created. The developed scenarios can be used to predict a probable situation evolvement without using a straightforward projection of the current conditions. On the contrary, scenarios might have as a starting point a present situation, and they can be evolved and transformed using the practitioners tacit knowledge to foresee possible outcomes very different and irrelevant to the present situations, based on operational experience and expertise.

4.1 A Systems Approach to Scenarios

In order to determine the descriptive fields that should be considered in a specific scenario, information from a number of real cases or relative scenarios developed by practitioners in context of past EU funded projects is analysed. This material is organized in a list of distinct "scenario instances", which take the form of individual sections in the scenario design. The basic principles in scenario structure are the following: Each scenario has an introductory section where contextual information is provided regarding an envisaged event type. A setting of the socio-economic and political context using eventually references from past cases. Information concerning the threat or risk and the specific challenge considered, the likelihood of the scenario (or its specific instance), the expected impact, the purpose of the analysis and the interested countries are determined in the introductory section. Succeeding sections accommodate specific information concerning instances of the scenario. This information includes entries for the initial conditions, the place, site, incident type, stakeholders involved and the scenario storyline (sequence, duration/pace, facts, actions/injects). The sections may refer to any stage of crisis or disaster management i.e. Prevention, Mitigation, Preparedness and Early warning, Response and Recovery [8].

Thus, in MEDEA, scenarios are stories developed by practitioners, highlighting challenges to meet their operational objectives against virtual operational cases related to current or new security threats. Using scenario as an analysis tool the practitioners cooperate with the R&D community to identify missing capabilities to address relevant artificial incidents. This approach allows the MEDEA network to become a research-practice interface, able to provide focused and documented recommendations to relevant decision and policy makers for specific research topics.

Apart from the structure, the scenarios in MEDEA have characteristic elements. They include or presuppose a setting (typically a location in M&BS region) and additional setting elements like the number of ir respective organisational objectives and operational mandates. Each practitioner organization typically has its own goals or objectives. These are the operational mandates that the practitioner should achieve under challenging circumstances of the setting. Every scenario involves at least one practitioner organization and at least one operational objective. The elaborated scenarios will most likely include more than one practitioner organisation or country.

Scenarios have also a plot; they include sequences of facts/injects and actions. These refer to things that practitioners involved in the scenario can do, things that happen to them, changes in the circumstances of the setting, and so forth. Particular actions and events can facilitate, obstruct, or be irrelevant to given goals. Notably, actions and events can often change the goals — even the defining goal — of a scenario. Scenarios and the elements of scenario-based design rationale can be generalised and abstracted using theories of human behaviour, enabling the cumulation and development of knowledge attained in the course of design.

4.2 Scenario Planning and Horizon Scanning

In [9] Rowe et al, quoting the works of [10] and [6], defines Scenario Planning (SP) as a "collaborative process to envision alternative future environments, articulate their implications, test the logic of long term plans, strategies and policies". In this approach, a single scenario gives a deterministic view of the future - whereas multiple scenarios depict a number of prospects and deepen the focus, expression and understanding of possible changes and developments. As such, by considering multiple possible scenarios, recognition is given to the indeterminate and emergent nature of the future, in contrast to forecasting-based approaches of the future, which often simply extrapolate on the basis of present situation and past trends.

The first French white paper on Defence and National Security issued after the end of Cold War cites that "there is a need to develop a "horizon-scanning" approach by the Government, in universities and in defence and security circles, in order to anticipate emerging risks and threats, opportunities for French and European interests, and to guide preventive policies and assets in a timely fashion"[12].

The use of Horizon Scanning (HS) approach in MEDEA is intended to develop a practitioner's organisation capability for identifying subtle security changes, allowing relevant organisations to cultivate a high awareness and understanding of their needs for future capabilities, leading to a quick and effective response to contextual changes and new threats (unexpected events) as per the work of Miles and Saritas [11]. Practitioners claim the true value of SP and HS lies in enhancing the 'cognitive agility' of planners by extending long-term thinking and exploring future developments.

5 The origins and the evolution of THOR Methodology

The MEDEA project has adopted an comprehensive approach, which is widely known as THOR (Technology-Human-Organizational-Regulatory) to analyze the capability gaps and the relative solutions that the network of practitioners considers. The THOR

methodology [10] had been originally introduced by the FP7 CAMINO[2] project [11], a project aiming to provide a realistic roadmap for improving resilience against cybercrime and cyber terrorism. Four dimensions of analysis have been defined, the combination of which can efficiently enhance resilience against cybercrime. These dimensions concerns Technical and Human issues inter-related with Organisational and Regulatory aspects. The work performed in CAMINO resulted to a number of resilience topics. Each topic was related to high priority (core) activities that were addressed in the CAMINO Roadmap. Each one of these topics was assigned to one of the four (THOR) dimensions and each topic was further divided into objectives. For every objective short-term, mid-term and long-term goals "milestones" were defined.

The THOR methodology was further elaborated in two recent EU H2020 funded projects (INSPEC[2]T [12] and TRILLION [13]), both within the FCT-14-2014[3] – Topic 2: Enhancing cooperation between law enforcement agencies and citizens. The work performed in INSPEC[2]T project revealed that a topic might be related to more than one dimension of analysis [14]. That is, an objective or solution, which is a subset of a topic, can be assigned to more than one dimension. For instance, a specific technical solution might require a legal amendment (Regulatory dimension), while most likely its introduction might necessitate acquisitions of specific skills (Human dimension).

The concept of "objective", used in the aforementioned two FCT-14 projects, is perceived in MEDEA as "identified gaps". The objectives are classified in short-, mid- and long-term time horizons while every objective is prioritised over the others [15]. As an example, a technical solution nowadays can be preferred over other (short time frame), while in the mid and long term its impact might be less severe, therefore other solutions might be prioritized.

Following the relative outcome of CAMINO, INSPEC[2]T and TRILLION projects, the THOR methodology is considered as a concrete framework to analyze the missing capabilities that practitioners need to prevent, mitigate and respond to various security-related challenges.

5.1 The MEDEA approach to identify missing capabilities

A key-objective of the MEDEA project is to identify the gaps in the capabilities of the security practitioners in the Mediterranean and Black Sea region to address current challenges and emerging threats. These findings will be organized to define a Mediterranean Security Research and Innovation Agenda (MSRIA), which may feed relevant future security programs or policies in E.U. The use of THOR methodology has been adopted for the needs of MEDEA project and the MSRIA scope in order to formulate a "footprint" of needed practitioners' capabilities. The methodology will be applied to a number of selected scenarios.

Initially the topics of interest are defined by the core of the MEDEA network, which is formed by the project consortium partners and organized in four focused, thematic working groups related to a. migration and asylum, b. border security, c. organized crime and terrorism and d. natural and technological hazards. These groups are open

[2] https://cordis.europa.eu/project/id/607406/pl

[3] FCT-14-2014 - Ethical/Societal Dimension Topic 2: Enhancing cooperation between law enforcement agencies and citizens - Community policing

and ensure the communication of the project with the diverse communities of practitioners while supporting the growth of the MEDEA network with new members. In the MEDEA jargon the groups are named Thematic Communities of Practitioners (TCPs). Scenarios related to the topics of interest are first developed by practitioners and submitted to the TCPs, using a structured template. A number of these basic scenarios is selected then for further processing, based on community decisions. There are two iterations in elaborating the scenarios. In the first, the practitioners co-create a set of scenario cases considering short term needs (threats currently experienced or likely to occur within the next three years). In the second iteration, a new set of scenarios will be developed concerning the same topic of interest for mid-term security threats (that most likely will appear within the next decade).

In the course of the MEDEA project, the network members and associated expert practitioners will engage into a scenario-based assessment of capability gaps, to address present (0 to 3 years) and emerging (3 to 10 years) threats. This will allow to be timely prepared to mitigate these threats and to respond effectively, acquiring new and improved capabilities. Having identified and documented the present and the emerging gaps in the capabilities of the practitioners, the MEDEA core group will engage in discussion with industry, academia and research communities to share their findings and identify potential solutions and priotitize future research needs in MSRIA.

To develop the short-term scenarios, the practitioners use their operational experience to outline their needs, using the scenario structured template, attributed to current and potential challenges that might become security threats within the next three years. For the mid-term horizon, the practitioners shall use both their operational experience and their tacit knowledge to outline situations that might evolve to security challenges in the near future. Based on practitioners' experience and security concerns, worst case scenarios for the considered time period (next 3 to 10 years) are also considered. An example related to the migration issue is the case of deliberate flow of migrants into Europe through the south and eastern borders due to geopolitical conflicts. In such case security practitioners in the M&BS region will need to cope with an unprecedented situation, which can eventually be combined with a pandemic.

MEDEA aims to gather the direct feedback from practitioners to define security risks and the need to develop the appropriate solutions, using the European R&D capacity. However, considering the need to identify challenges and threats in the long-term, which is ten or more years from now, the contribution of the practitioners might be limited. To this purpose, HS techniques will be utilised to elaborate relative foresight scenarios. Interaction with academia, technology pioneers and policy makers will be used by the core group to elaborate relevant security capacity building approaches and define new capabilities that may mitigate such risks.

5.2 Application of MEDEA SP and HS approaches

When a scenario is created, it is stored in the MEDEA's collaboration workspace, which is accommodated in a secure platform, maintained by the project. Invitations are promptly sent to members of the respective TCP of the network to inform them on the new scenario and ask them to elaborate its content and review it online. At the same time a virtual presentation to TCP members is scheduled by the scenario creator. The members of the network can ask information and clarifications on the context of the

scenario or highlight solutions, already in place, that may fulfil relative mission objectives, propose modifications and recommend variations or additions. At a later stage, the interested practitioners may co-define an operational scene, which will host a number of different scenarios. By doing this, a number of different and divert scenario cases is developed using a formalized theater of operations where all threats will be studied and analysed during an interactive workshop session.

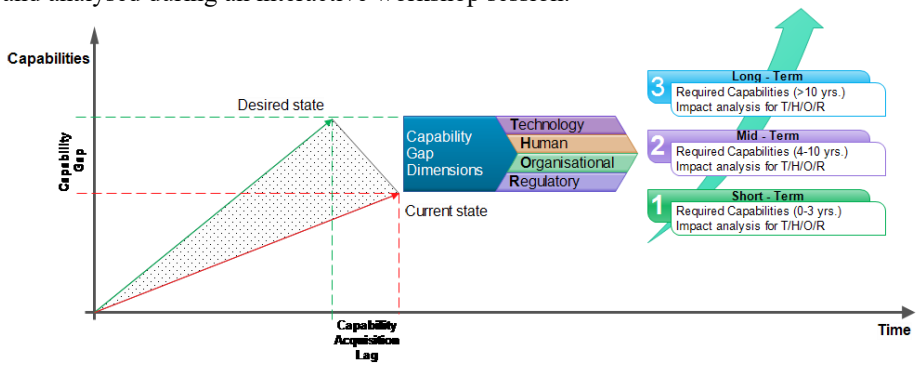

Figure 2: Practitioner's capability gap identification and analysis process.

The scenario templates host a special section where the maximum impact is defined for the societal, economic, reputation or environment aspect. However, the use of taxonomies for the scenario scene and the categorisation of threats might also be convenient for a more comprehensive examination of practitioner needs. It is up to the practitioner communities (TCPs) to select the scenarios of their interest. Scenarios developed for the needs of other EU funded security projects are considered as well, further developed and possibly adapted to match the peculiarities of the M&BS security topics. From the developed scenarios, the most comprehensive and complementary ones are selected to be further examined in proper practitioner's capability analysis workshops.

Following the scenario selection, physical interactions, preferable in TCP Capability Gaps Workshops are taking place. A preferred audience for the workshop, apart of the MEDEA members and invited subject matter security experts, are members (practitioners) from other practitioners' network and / or members from other EU funded projects with profound interest in the workshop's objectives. During the Capability Gaps Workshops, audio and video material is used to visualize the scenario and to trigger the interest and feedback of the participants. The practitioners are confronted to respond to a number of security issues and challenges relevant to the envisaged scenario. Initially, the practitioners outline the currently existing capabilities, which are able to respond to the challenges under analysis and then they are indicating (to the best of their knowledge and operational experience) the needed capabilities that will enable their organisations to become more effective. At the final workshop stage, the practitioners will confirm and rank the identified capability gaps and outlined a timeline for acquiring these capabilities and incorporate them in their organisations. This is illustrated in Figure 2.

The preliminary outcomes of the workshops are identification and prioritisation by practitioners of capability gaps on existing systems and procedures, and requirements for additional functionalities. Specific emphasis is placed on the interoperability of information systems and the use of existing EU databases. The output of the scenario

analysis, following the Capability Gaps Workshops, take the form of practitioners' related "user requirements", which are further processed and organized to be conveyed to academia and industry at the next stage.

5.3 THOR methodology in context of MEDEA

The outcomes of the Capability Gaps Workshops (a priority list of missing capabilities), is further processed by the core group of MEDEA (project consortium). The capability gap findings are pre-processed according to the four THOR dimensions by the core group of MEDEA. For each capability gap, the THOR methodology is applied based on the following:

For the **Technology** dimension, practitioners examine a variety of already developed solutions as well as developing ones and assess their adequacy to address the envisaged gap. The MEDEA practitioner's network aims to short list and prioritise the missing technical capabilities, which are (1) currently needed or (2) desired in the mid and long-term by security practitioners.

The **Human** dimension corresponds to the analysis of the practitioner's capabilities (both current and desired), in regards to possible new skills and training required to suppress new and emerging threats. Eventual social implications, which may follow the introduction of new capabilities will be examined under this dimension as well.

The **Organisational** dimension studies the re-organisation of procedures and operational activity that can improve response to current and resilience to emerging and future threats. Further to an organisation's reform, the organizational analysis covers the impact collaboration and corporate culture may have to the operational performance and suggest standardisation of procedures between different practitioners' entities or across neighbouring Member States of E.U.

Lastly the **Regulatory** dimension seeks to identify gaps in institutional, policy and legal frameworks that may influence the capability to respond to current and new security challenges. Besides, there is in many cases a need for common policies and adoption of unified regulations across all EU MS.

After the conclusion of THOR analysis there can be cases where addressing capability gaps might require more than one dimensional component (attribute). The impact of each dimension to an envisaged capability is described by a relative attribute. Solutions to address an identified gap can be related to more dimensions. As an example, a capability gap might be attributed to two technological and one regulatory dimension. i.e. the performance of Electronic Support Measures (ESM) sensors might need to become more stable (technology maturity) and might necessitate interworking with legacy command and control solutions (open /standardised interfaces). However, their usage for example might not be regulated in some EU MS despite their proven operational advantage they offer to practitioners.

MEDEA has created a database of attributes (as shown in **Error! Reference source not found.**) where the dimensions of each capability gaps are compared to.

Table 1. MEDEA attributes database for each THOR dimension

Attributes class and number	T - Dimension	H - Dimension	O-Dimension	R-Dimension
Interoperability	3	2	2	2
Dual use and Misuse	1	1	2	2
Migration and asylum seeking	2	3	2	2
Early Warning and Situational Awareness	2	1	3	3
Cross border crime and terrorism	2	2	0	2
Natural Hazards & Technological Accidents	1	3	2	0
Soft Skills	2	4	7	2
Standardisation Issues	4	1	2	2
Uncertainties (Local, National, Regional)	3	3	2	8
Other Security stakeholders	1	1	1	1

The database (of the THOR attributes) is open and linked to the contribution of MEDEA members participating in THOR analysis workshops. for the attributes listed above and will help the researchers and the practitioners to co-develop a list of recommendations for the Mediterranean Security Research and Innovation Agenda (MSRIA). New attributes defined during the THOR analysis workshops are recorded and considered in future analysis cycles.

6 Prioritisation of practitioners' capabilities in three horizons

THOR workshops with relevant practitioners' representatives are organized then to analyze and prioritize missing capabilities (gaps). Prioritisation is based on implementation time and impact criteria. The European dimension, beyond the M&BS regional interest, of the identified capability gaps will also play a role in defining the priority and urgency to invest research effort to address them.

Following the identification and documentation of the attributes, every attribute is prioritized against each of the THOR dimensions. This is done by the practitioners using a number of prioritisation techniques, e.g. either a five level Likert scale or the MoSCoW (Must have, Should have, Could have, and Won't have) method. Each prioritisation technique possesses certain advantages. The preferred method is decided as soon as the capability gap attributes are adequately described. Because of the particular nature of the Regulatory dimension, there are attributes that might be related to legal, ethical and regulatory issues. In such case, the 1 to N (Likert scale) quantification approach might not be suitable. Thus, a weight of 0 or 1 corresponding to impact and no impact is utilised instead. The practitioners involved in the TCP workshops are asked

to respond to questionnaires that assist MEDEA project to prioritise the need for capabilities in the short, mid and long-term. It is anticipated that the need for developing solutions to fulfil the identified capability gaps will vary over time.

Radar plot will be utilised to highlight the importance (impact) of every attribute including information for the three time-horizons i.e. 1) Short-term (0-3 years), 2) mid-term (3-10 years) and 3) long term (10+ years). The plot chart uses the data of the 1-N Likert / MoSCoW quantification exercise, in order to visualize the priority needs to fulfill the capability gaps.

Apart of the identification and prioritisation of capability gaps, their initial prioritisation to qualify for further analysis using the THOR methodology, the attributes resulted and their prioritisation, the MEDEA partners should also consider the solution development perspective. The desired attributes should be verified if they are available or will be delivered as part of a solution. If the needed capabilities are part of an available solution, the consortium should approach solution providers to arrange for a proof of concept demonstrations for the required capabilities. If the desired capabilities are not covered by existing industry portfolios, a design, development and testing cycle is required, which will delay the introduction of new solutions. As such, the time to deliver and acquire solutions to fulfil the identified capability gaps should be considered in the MEDEA recommendations to the MSRIA.

7 Conclusions and next steps

This paper presents the methodology utilised by MEDEA project to identify, prioritise and analyse missing capabilities to address current security challenges and emerging threats in the M&BS region. However, the proposed approach can be applied universally.

Scenarios developed by practitioners combined with a horizon-scanning approach are used to document a list of a. desired capabilities linked to current/existing threats, which will most likely encountered in the next three years (short term); b. capabilities that will be needed to address emerging threats foreseen to challenge security in the next 3 to 10 years (mid-term), according to the practitioners' operational experience ; and c. capabilities to address improbable future threats that can't be excluded to appear beyond the 10-year horizon (long term). To be successful with the long-term planning, practitioners experienced in the operational and strategic planning should interact with the research community and solution providers to identify capabilities that might be required beyond a decade from nowadays.

MEDEA project utilizes Scenario Planning and Horizon scanning approaches as well as Capability Gaps and THOR analysis workshops to identify and analyse the missing and desired capabilities. This is organized in close cooperation between practitioners, experts and researchers to define concrete user requirements, which are conveyed to the R&D community as well as to relevant policy and decision makers. Interaction with Academia/Research and Industry is planned in the form of open call for ideas, Research Development and Industry days, conferences and Proof of concept demonstration activities aimed to bring together the solution provider and the end users. These planned interactions will assist the formed TCPs to proceed with solution selection that will be trialed and demonstrated to practitioners. The Desired, Foreseen and

Expected Capabilities, as well as their prioritisation and the results of the THOR analysis will be documented in the Mediterranean Security Research and Innovation Agenda (MSRIA).

At the end of 2019, in month 18 of the project, MEDEA members have released the first version of the MSRIA. There will be four versions of the MSRIA with the final one scheduled to be delivered in 2023. More interactions in each TCP, cross TCP activities and joint events like the Mediterranean Security Event 2019 are planned to bring together security practitioners across EU MS and enable them to interact with representatives from Academia/Research and Industry, policy makers and other security stakeholders.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787111. The support is gratefully acknowledged. The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

References

[1] [Online]. Available: https://www.medea-project.eu/. [Accessed 29 11 2019].

[2] [Online]. Available: https://cordis.europa.eu/programme/rcn/701794/en. [Accessed 30 11 2019].

[3] E. Wenger, "Communities of practice: A brief introduction," 2011.

[4] J. Carrol, "Five reasons for scenario-based design," in *32nd Annual Hawaii International Conference on Systems Sciences*, 1999.

[5] I. R. e. a. Whitworth, "How do we know that a scenario is 'appropriate'," in *11th International Command and Control Technology Symposium, , UK.* ., Cambridge, 2006.

[6] G. Ringland and P. Préfacier Schwart, Scenario planning: managing for the future, John Wiley & Sons, 1998.

[7] K. Van der Heijden, R. Bradfield and G. Burt, The sixth sense: Accelerating organizational learning with scenarios, John Wiley & Sons, 2002.

[8] D. Coppola, Introduction to international disaster management., Elsevier, 2006.

[9] E. Rowe, G. Wright and J. Derbyshire, "Enhancing horizon scanning by utilizing pre-developed scenarios: Analysis of current practice and

specification of a process improvement to aid the identification of important ‘weak signals," *Technological Forecasting and Social Change,* vol. 125, pp. 224-235, 2017 .

[10] F. O'Brien, M. Meadows and M. Murt, Creating and using scenarios: exploring alternative possible futures and their impact on strategic decisions. Supporting Strategy: Frameworks, Methods and Models, Chichester: John Wiley, 2007.

[11] N. Sarkozy, The French White Paper on defence and national security, Odile Jacob Publishing Corp, 2008.

[12] I. Miles and O. Saritas, "The depth of the horizon: searching, scanning and widening horizons," *Foresight,* vol. 14, no. 6, pp. 530-545, 2012.

[13] M. e. a. Choras, "Comprehensive approach to increase cyber security and resilience," in *10th International Conference on Availability, Reliability and Security*, 2015.

[14] [Online]. Available: https://cordis.europa.eu/project/rcn/185485/factsheet/en. [Accessed 03 08 2019].

[15] [Online]. Available: https://cordis.europa.eu/project/rcn/194895/factsheet/en. [Accessed 25 11 2019].

[16] [Online]. Available: https://cordis.europa.eu/project/rcn/194841/factsheet/en. [Accessed 10 11 2019].

[17] G. Leventakis and G. Kokkinis, "Developing and Assessing Next Generation Community Policing Social Networks with THOR Methodology," in *Community-Oriented Policing and Technological Innovations*, 2018.

[18] C. Patrikakis, A. Konstantas, D. Kogias and M. Chor, "TRILLION project approach on scenarios definition for citizen security services.," in *International Journal of Electronic Governance*, 2017.