Combining security scenarios development, capability gap identification and THOR Analysis in the MEDEA Networks of Practitioners.

George Kokkinis[*], Genny Dimitrakopoulou[*], Freideriki Makri[*]

[*] KEMEA, Center for Security Studies

Abstract- The THOR methodology is the most essential building block in a chain that aspires to influence the development of security solutions and produce meaningful recommendations to policy and decision makers. Initially, in order to identify operational capability gaps that security practitioners face, specific working scenarios are formulated and developed, exposing an array of possible threats and responses. Then, analysing these scenarios with different categories and ranks of security practitioners offers a well-rounded, comprehensive insight into the needs that should be fulfilled and the operational capabilities to be developed or complemented. This detailed detection and documentation of capabilities serves as an impact analysis that offers the canvas that will be used to pinpoint and categorise individual attributes that touch upon the THOR methodology's four dimensions: the Technological, the Human, the Organisational, and the Regulatory dimension. Based on the produced findings, a strategy shall be outlined so that practitioners are able to weigh-in on the cross-over between gaps and urgencies and prioritise the fulfilment of their needs. A crucial element of the THOR methodology -and the purpose of this paper – is to demonstrate how each capability gap interacts with the THOR dimensions, revealing the interconnection of deficits. Understanding the ad hoc interplay of the four THOR dimensions is crucial to optimally grasp the challenges that need to be overcome. For instance, there are attributes that appear at first sight technological, nevertheless the sole adoption of a pertinent technological solution would not address core issues and deficits, if professional development (human-related dimension) or acquisition of expertise (organisational-related dimension), and/or a supportive legal framework (regulatory dimension) are not in place beforehand. THOR methodology assists practitioners to carefully identify their capability needs, prioritise them, by utilizing their operational experience. The application of a multiple-dimensional approach in a field as vast as security, considers expertise and experience by various security stakeholders - their positions and specialties notwithstanding. This, in turn, generates ideas and solutions of practical value, aimed at addressing existing and emerging threats alike.

Index Terms- THOR Methodology, Scenario development, End User requirements, Security projects, Capability gaps, Technology acceptance, Policy recommendations

I. INTRODUCTION TO MEDEA APPROACH

The Mediterranean and Black Sea region has neighbouring countries that are experiencing security issues like the political uprisings in Egypt, Tunisia, and Libya, the wars in Syria and Ukraine to name but a few. The future security of the region depends upon a cooperative and collective ability to understand and shape conditions to counter traditional and emerging threats like the hybrid threats, economic and energy coercion, disruption of governance, disinformation campaigns, and paramilitary threats. As a result, the ongoing 'migration crises and the increasing security 'pressure' experienced at the EU external borders, mostly in the Mediterranean and Black Sea regions is a result of existing migration and border management practices. In addition, the expansion of cross-border crime, asymmetric globalisation, and information and communications technology (ICT) created new opportunities for transnational organised crime groups (OCGs) to develop and expand, exploiting novel technological methods and regulatory loopholes, thus leaving Law Enforcement Agencies (LEAs) one step behind. Aside the political and social economic factors, the region is the most vulnerable European region to earthquakes, flash floods and forest fires. The frequency, speed and magnitude of natural disaster risks are expected to be acerbated in the region due to climate change.

[1] DOI: 10.5281/zenodo.10003812 / Book chapter

Under this spectrum, innovative methodologies are being explored and employed so as to render LEAs better equipped to tackle challenges, unforeseen events, and emerging threats in a prompt and swift manner, often by anticipating and foreseeing risks, other than merely addressing them when they occur. The aim of this paper is to introduce the methodology used by the MEDEA network of Practitioners (NOP) as a method to better identify, analyse, and address the needs of security practitioners. It is argued that the implementation of this methodology can offer a better understanding of the multi-dimensional nature of the practitioners' capability gaps that comes from the interplay of the four THOR dimensions.

THOR's four dimensions include Technical and Human issues inter-related with Organisational and Regulatory aspects. In more detail, the Technology dimension focuses on new technologies and studies their capacity to address current capability gaps. The Human dimension analyses the practitioners' capabilities in regards of new skills and training requirements needed to suppress new and emerging threats. The Organisational dimensions studies the re-organisation needed to respond to emerging and future threats. Finally, the Regulatory dimension is related to the necessity of standardisation, the identification of gaps in legislative and policy framework in light of the new security era challenges, and the need for common policies.

There are five main building blocks described in the MEDEA methodology (Figure 1). These are:

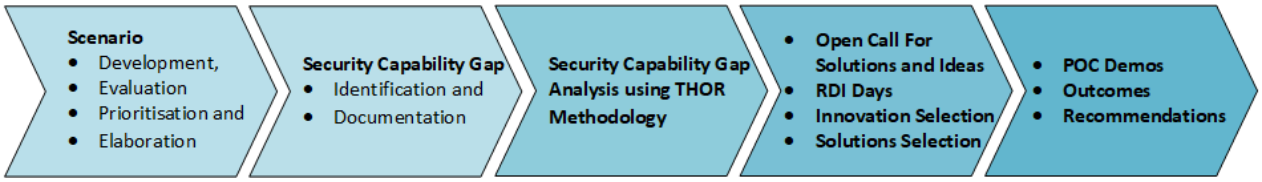

Figure 1: MEDEA scenario development, Capability Gap formulation and recommendations process

1. A **Scenario** development block where security practitioners will first develop at organisational level, a set of security scenarios. Next at National and then at regional level, the practitioners will jointly evaluate the developed scenarios, select the most relevant ones and then with other security stakeholders from the region will elaborate the selected scenarios that will be later used to identify their needs for enhanced or new operational capabilities.
2. A **Security Capability Gap** identification and documentation block, where security practitioners will describe the security capability gaps, they are experiencing. The capability gaps will be identified when practitioners compare their shortcomings and limitations they are experiencing against a desired "ideal" security state. In other words, the practitioners will describe what means they would like to have available to perform their operational duties.
3. The identified security capability gaps will be analysed in the **Analysis** building block. The security practitioners will analyse the needed capabilities using a four-dimensional analysis. The practitioners will identify the Technology, the Human, the Organisational and the Regulatory (THOR) issues that should be fulfilled and addressed to minimise the operational impact of the said security gaps.
4. The fourth building block is **promoting security market awareness**. The security practitioners invite via an open call solution providers and security innovators to address the documented capability gaps. Based on the documented gaps solutions providers and pioneers propose security solutions for addressing these gaps. A constructive dialogue between end users and solution providers is taking place in security Research, Development, and Industry (RDI) Days. Apart of Supply side presenting market ready solutions to end users, the security practitioners communicate their needs and proposed selected functionalities and features they would like to acquire.
5. The practitioners select several security products they would like to test, and experience in close to real life operational scenarios in selected testbeds. As such **Proof of Concept** (POC) **demonstrations** are scheduled for practitioners and industry to jointly test, evaluate security

products. The practitioners provide feedback and influence the security solution roadmap of suppliers in RDI and POC instances.

II. SCENARIO DEVELOPMENT

The security nature of scenarios is being utilised by many security institutions for different purposes. The US Defence Modelling and Simulation Office (DMSO) uses scenarios to establish an initial set of conditions and the timeline of significant events. For the needs of this analysis, the approach of [1] where 'a representation of the state, and present actions, so as to permit the exploration of, or reasoning about, their future state and the events that lead to it', is used. As such, a set of scenarios is employed to assist security practitioners in describing current and emerging threats that are likely to occur.

To initiate the application of the MEDEA methodology a set of scenarios are developed by practitioners using a specific template so that there is a uniform format of the incidents reported [2]. It is up to the practitioners to select the scenarios that they deem more relevant and useful. Under this light, they might consider scenarios developed across various security projects and further enhance or/and adapt them to match the peculiarities of the circumstances they encounter whilst performing their duties. From the set of developed scenarios, using the Delphi Method to approach expert consensus, a subset of scenarios is selected to be additionally scrutinised collectively in tailor-made workshops [3]. Hence, physical (or virtual because of COVID-19) interactions are then taking place between security experts, practitioners, and other stakeholders. This gives ample opportunity for the practitioners to set out their current operational capabilities and gaps, explain how they respond to threats, and denote how they may become more effective and efficient.

The scenarios are based on actual operational incidents stemming from current and emerging threats the practitioners believe they will encounter in the following years. Each scenario consists of certain sections. First, the security background is presented to introduce the countries and stakeholders involved, preliminary information, risks, likelihood, and expected impact. The following sections define parameters such as type of event, conditions, duration, and external factors (economic, social, and political stability). Also, it sets out the events that have built up to the point where the scenario takes place, as well as further elements, such as each practitioners' organisations' objectives and operational mandates. The scenario template is structured in a way to assist security practitioners to describe real-life incidents, and define and elaborate the sequence of events, actions, and responses, while they also outline what impedes the practitioners' reactions.

III. SCENARIO ANALYSIS AND CAPABILITY GAP FORMULATION

Once a scenario is developed, it is studied and examined further by the partners with the aim of identifying and documenting capability gaps. A capability gap is defined *as the difference between the current ability of security practitioners to prepare, prevent, respond, and recover from a security-related challenge, and the future desirable condition*. During the scenario analysis phase, security practitioners may provide clarifications, share their insights about additional challenges and needs, and elaborate on the operational capability gaps. The practitioners may further elicit the developed scenario and share their views about deployed or proposed solutions.

Capability Gap Formulation

MEDEA members express capability gaps using the following approach.

<Title> ***Capability Gap Title*** </Title>
<Section1> ***Background*** </Section1>
<Section2> ***General description of operational capability gap*** </Section2>
<Section3> ***Required capabilities*** </Section3>
<Section4> ***Additional Considerations*** </Section4>

The first section of the description is the ***Background.*** This section provides a description of **what** is required (from the practitioner's point of view - **who**) and **why**. For example, the reduction of the degree

of a solution's efficiency during certain conditions is a capability gap. If the desired capability would be available unconditionally to practitioners, this could improve the efficiency of their operations. A time to market is required (**When**) to indicate to solution providers the urgency to fulfil this capability gap. Lastly, this section should address the **Where**, that is the segment of security organisations that will benefit from a potential solution. Hence, the background provides an overview of the market need.

The second section is the ***General description of an operational capability gap***. This section provides additional explanation of what existing solutions fail to address (from the security practitioners' point of view) and what additional or complementary capabilities the security practitioners would like to have instead. This section should clarify the need of security practitioners to acquire certain security solutions. Next, the section ***Required capabilities***, should describe the minimum set of requirements and conditions that must be addressed, in order for practitioners to consider acquiring an offered solution. ***Additional considerations*** should provide additional context about the capability gap fulfilment requirements. It is quite possible that not all security requirements can be addressed in the preferred capability acquisition window. The practitioners might prefer incremental, continuous advancement of solutions instead of waiting for solutions that meet all the requirements at the same time. This section should include the requirements for accuracy, compatibility, form factor, maintenance, robustness, cost, and the technical characteristics of the desired solution.

During the THOR workshops, it is critical to trigger the interest of the participants, as well as foster trust and communication. Audio and video material can be used to illustrate the scenario and introduce the capability gaps. Discussion of the gaps revolves around the THOR dimensions. The practitioners are encouraged to discuss a number of security issues and operational needs related to the scenario under analysis. As such, the development of questions, before the workshop, that lead the discussion is a good practice to not only boost interaction between the practitioners, but also to gather the information needed. Among others, the practitioners are asked to share their knowledge and experience regarding the scenarios' capability gaps, or a particular aspect of them, and add new ones if applicable. This is illustrated in Figure 2. The main outcomes of the workshops are the documentation of the scenarios' capability gaps, the identification of additional gaps, or relevant challenges and parameters that should be taken into consideration so as to improve existing systems and procedures and develop new functionalities. These insights, gathered during the workshops, are valuable for the next phase, which is the conduction of the THOR analysis.

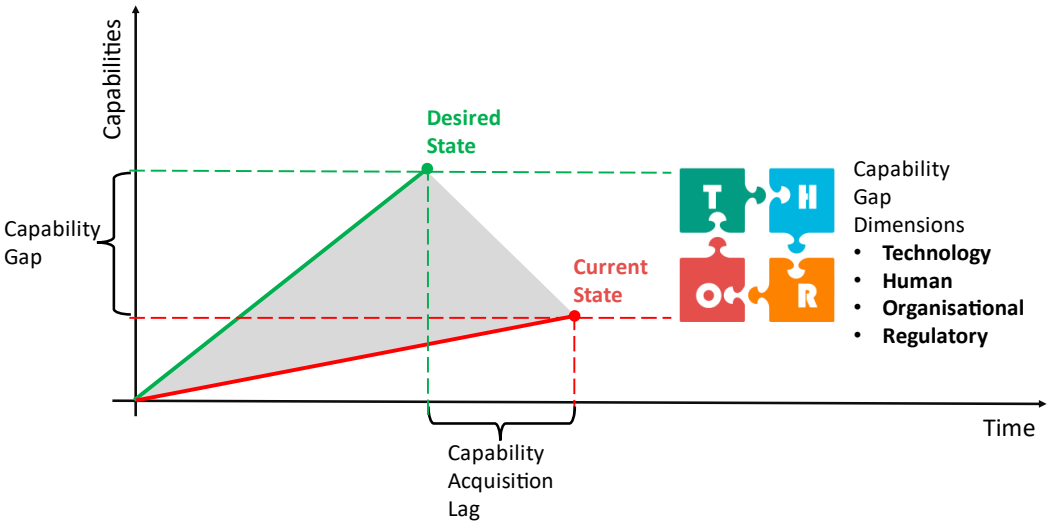

Figure 2: Practitioners' capability gap identification and analysis process.

IV. APPLICATION OF THOR METHODOLOGY

The development and evolution of THOR Methodology

The THOR methodology, originally introduced by the FP7 project [4] and further elaborated in two H2020 projects [5] and [6], is considered a concrete framework to analyse the lacking operational

capabilities that are necessary to prevent, mitigate, and respond to a plethora of security-related challenges. The CAMINO project introduced four dimensions which could be combined to efficiently enhance resilience. Several topics were identified and each one of these topics was assigned to one of the four (THOR) dimensions and further divided into objectives. The work performed in INSPEC²T project revealed that a topic is composed of multiple objectives, but not all of them are related to one dimension [7]. That is, a topic can be attributed to more than one dimension. For example, a specific **T**echnical solution, might require a legal amendment (**R**egulatory dimension), while most likely its introduction might necessitate acquisitions of specific skills (**H**uman dimension). The work in TRILLION focused on quantifying the objectives in terms of time horizons for short- term, mid-term, and long-term needs. In addition, each objective is prioritised over others [8]. As an example, a technical solution nowadays can be preferred over another (short-time frame), while in the mid- and long-term its impact might be less severe, therefore other solutions might be needed. Following the work performed in CAMINO, INSPEC²T, and TRILLION and their resulted findings, the enhancements in THOR methodology are combined in the [9]. The THOR methodology serves the objectives of MEDEA, that is to identify common capability challenges that practitioners' need to address so as to suppress various illegal activities and actions related to the fight against organised crime and terrorism.

Application of the THOR Methodology

In the context of the MEDEA project, the THOR methodology has been further evolved to be applied to security projects and lead to recommendations to decision and policy makers. The application of the THOR methodology starts with the development of detailed operational scenarios to aid practitioners and associated experts define deficits and pinpoint the gaps that impede the optimal resolution of issues pertaining to security. Refer to Figure 3 (STEP A, STEP B, and STEP C). Then, the findings from the scenarios' analysis leads to the explicit identification of operational capability gaps. The analysis of the said gaps (STEP D) leads to identification of specific attributes (STEP E) and their subsequent evaluation and prioritisation (STEP F). The outcomes of this process are forming recommendation to decision and policy makers (STEP G).

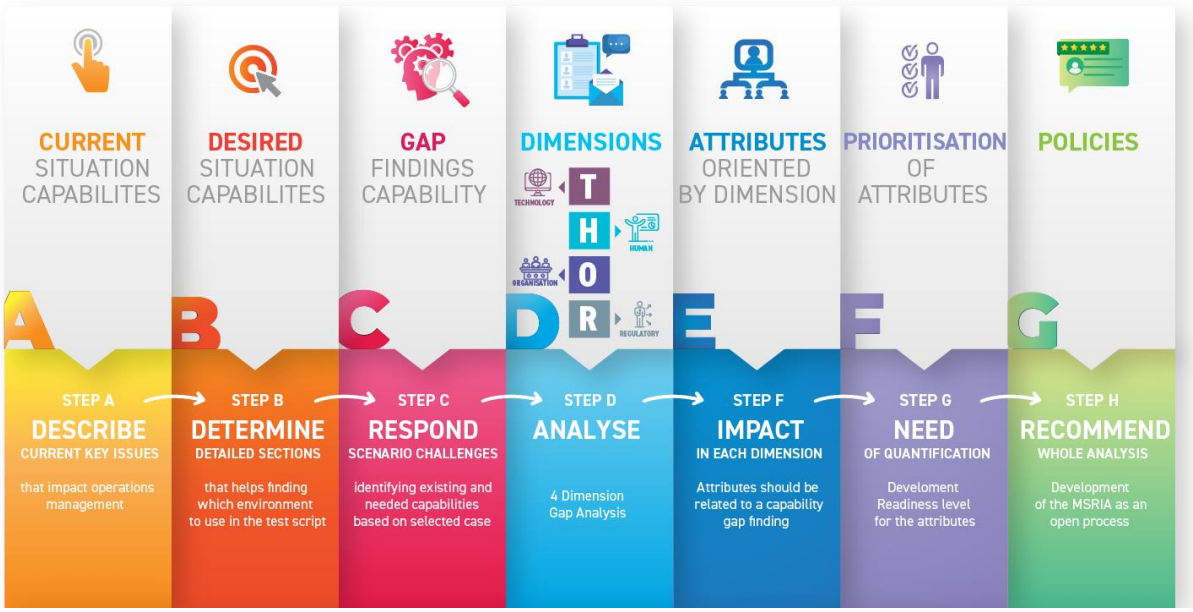

Figure 3: Application of MEDEA methodology

The findings of the THOR workshops, including a list of missing capabilities and additional information of each capability gap, are further processed following the four dimensions of the THOR analysis. The Technological, Human, Organisational, and Regulatory aspect of each capability gap is examined to find the main causes of the gap and possible solutions to overcome it. More specifically:

Regarding the **Technology** dimension, a variety of already developed solutions as well as developing ones are examined and assessed based on their adequacy to address the envisaged gap. The aim is to shortlist and prioritise the missing technical capabilities which are currently needed or desired in the mid and long-term by security practitioners. The challenges and/or possible solutions that fall under the Technology dimension may not be of technical nature. For example, sometimes the required technical solution exists but there are other factors (i.e., the cost) that block its broad use by practitioners.

The **Human** dimension focuses on the required practitioners' capabilities regarding new and advanced personal skills and trainings to suppress current and emerging security challenges. These capabilities may include trainings on new technologies, creation of motives for practitioners, and modifications on existing investigation methods. Eventual possible implications, which may follow the introduction of new capabilities are examined under this dimension as well.

The **Organisational** dimension delves into the processes and procedures followed by the relevant practitioners' organisations, that can be improved to address effectively emerging and future security threats. These may include the re-organisation of existing procedures and the development of new ones, the creation of collaborations, the development of a corporate culture, as well as proposals about the standardisation of procedures between different LEAs or across states.

Lastly, the **Regulatory** dimension aims to identify obstacles either at the institutional, policy, or legal level that may impede the effective response to current and emerging security threats. A gap that is examined regularly under this dimension is the need for adoption of aligned policies and unified regulations between distinct organisations and states, as mentioned above.

Drawing on the above mentioned, the THOR analysis is applied in each capability gap identified in the respective scenario. This implies that for each capability gap possible Technical, Human, Organisational, and Regulatory attributes are examined, applying also the information gathered during the THOR workshops. The term "attribute" refers here to the impact of each dimension to an envisaged capability gap. Based on the nature and the peculiarities of each gap, solutions to address the identified gap can be related to more than one attributes and dimensions. As such, a capability gap may have two technological and one regulatory attribute. For example, 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 the proven operational advantage they offer to practitioners.

Security Scenario Workshops

Following the scenario selection, physical interactions are carried out. A preferred audience for the workshop, apart from the MEDEA members and invited subject matter security experts, are members (practitioners) from other practitioners' networks 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 visualise the scenario and to trigger the interest and feedback of the participants. The practitioners are then invited to respond to a number of safety issues and challenges relevant to the envisaged scenario. Initially, the practitioners outline the existing capabilities that 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. Hence, an outline is set out for acquiring and incorporating said capabilities in their respective organisations.

V. MEDEA USE CASE EXAMPLE: LAW ENFORCEMENT CHALLENGES IN THE DIGITAL AGE

The MEDEA developed and sustained a TCP where its members focused on the "Fight Against Cross-Border Crime and Terrorism" challenges. Using the scenario development and the Capability gap analysis described in preceding sections, practitioners from LEAs confirm their need to use *'automated tools to detect and subsequently remove online content'* [10], [11]. These gaps are attributed to the vast

amount of open-source data that needs to be investigated by LEA Open-Source Intelligence (OSINT) teams. Nowadays OSINT teams are using either commercial solutions - but often with limited/restricted number of licenses - or in-house developed open-source tools, like crawlers. Thus, a fully-fledged automated Early Warning System is needed, with adequate number of licenses to support LEAs' capacity in OSINT analysis. Following the identification of illegal content, its removal is a challenging and demanding process, and it is subject to different regulations and procedures based on where the illegal content is hosted. Furthermore, practitioners need '*additional capabilities to intercept voice and data communications and decrypt / decipher them*' [12].

The interception and decryption of encrypted communications is a very difficult and time-consuming task. The vast number of commercial messaging applications (WhatsApp [13], Signal [14]) and the uncomplicated development of customised applications for mobile devices like EncroChat [15], makes the use of customised communication products with end-to-end encryption favourable to perpetrators. At the same time, it becomes more difficult and more complicated for practitioners to decrypt OCG communications [16]. Hence, LEAs efforts to suppress OCG activities, apart from the use of more capabilities in Early Warning, Interception of Information, necessitates '*better exploitation of existing databases and enforce open interfaces to data processing tools*' [17]. Police officers need access to a unified database that will include information from past cases and incidents.

Records about known offenders and their modus operandi will assist practitioners to define a pool of suspects. The database should include OCG members' criminal records, connections with other OCGs, countries and places where the offenders carry out their criminal activities, and other characteristics which will assist practitioners with their investigations. Apart from the single database, improved search functionalities using Machine Learning (ML), or Artificial Intelligence (AI) are needed for competent authorities to be able to process data more effectively. An example of the application of THOR analysis is summarised in Table 1 for the Capability Gap Finding (CGF) no. 1.

Table 1: Application of THOR analysis - Example

Capability Gap Finding [Id]	**Technology Attributes**	**Human Attributes**	**Organisational Attributes**	**Regulatory Attributes**
Limited access and use of automated tools to detect illegal content. [3.CGF.1]	[1] Early Warning System to detect online content.	[1] Need for Resources with linguistic expertise.	[1] Need to enhance cross-border cooperation between LEAs.	[1] Legal definition that will define strictly illegal online radicalised or terrorist content.
	[2] More autodetection tools with affordable cost.	[2] Continuous professional development of OSINT teams	[2] Organise regular trainings for their OSINT teams.	[2] Reassess ethical framework with respect the use of AI, ML.
	[3] Autodetection capabilities in deep/dark web.	[3] Additional personnel fluent in foreign languages and dialects.	[3] Encourage practitioners to learn foreign languages.	[3] Amend legal framework to assure the protection of fundamental rights and endorse the establishment of autodetection.
	[4] Data analysis capabilities and translation tools.	[4] Encourage the involvement of native speakers in OSINT units.	[4] Development of IRUs at national level.	

The application of THOR analysis for the capability gap described in table 1 resulted in 4 Attributes found in the **T**echnology, **H**uman and **O**rganisation dimensions, and 3 attributes in the **R**egulatory

dimension. Similarly, the application of THOR analysis for the following 3 CGFs: "Difficulties for LEAs to remove online illegal content" [3.CGF.2], "Better exploitation of existing databases and enforce open interfaces to data processing tools" [3.CGF.11], and "LEAs require additional capabilities to intercept voice and data communication and decrypt / decipher them" [3.CGF.12], revealed the number of attributes associated in each THOR dimension, as shown in Figure 4.

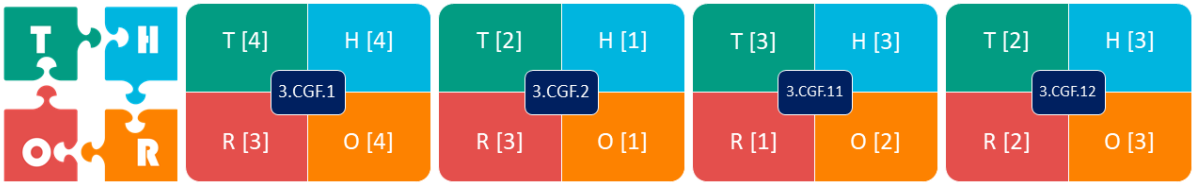

Figure 4: Number of attributes in THOR dimensions for the case study.

Technology related challenges

Police Officers should have access to state-of-the-art (SOTA) solutions that will help them to detect illegal content online as early as feasible. These solutions should advance LEAs detection capabilities and offer them Early Warning (EW) advantages. For the implementation of innovative technological EW solutions to be effective, interagency collaboration and an engagement strategy that promotes co-operation and data sharing are required [18]. Application of the THOR methodology highlighted the fact that technology should be used as an instrument to facilitate and promote cooperation between Law Enforcement and Judicial authorities across different EU Member States (MS) and facilitate the exchange of real time information without the risk of being compromised. Other than the advancements required for OSINT and SIGINT (for lawful interception and blockchain monitoring) solutions, equally important is the use of Technology to offer very accurate translation services to LEAs, since most of the illegal content is in languages most Police officers they cannot comprehend. This highlights the need to improve LEAs' capabilities with advanced technology solutions across all phases of police investigation like interception and data collections, examination, and forensic analysis.

The digitalisation of tools and the broader use of Artificial Intelligence (AI) and Machine Learning (ML) in the field of security could help LEAs in their fight against organised crime and terrorism, however the required innovative products should be integrated in the Police Standard Operating Procedures (SOPs) and interface existing solutions that are in service. Apart from the need for new technologies, another issue that emerged from THOR analysis is related to the fact that even when technological solutions exist, they are not commonly used by LEAs for different reasons, be it their cost or the fact that they are backwards compatible with existing systems, or do not fulfil all LEA needs, and as such, additional products are needed.

Human related challenges

New security solutions are mostly utilising AI which is a disruptive technology. AI does not only offer numerous benefits to LEAs, but it also introduces several concerns related to its use. Therefore, it is not only the nature of crime that evolves. There is the need for continuous trainings for LEAs to be able to keep up with the technological advancements and the complexity of the modus operandi of criminals since perpetrators are "early Technology adopters". The introduction of SOTA solutions in police organisations has not only to do with technical aspects of getting these solutions up and running but it also necessitates the professional development of serving Police officers. Some complex solutions required knowledge of big data analysis, while solutions for profiling, and social media analysis impose the recruitment of scientific and specialised personnel in police forces.

Furthermore, the application of THOR methodology stressed the need for additional and more frequent "traditional" police training which typically consists of simulations, joint training activities between LEAs from different countries, or trainings in cross-country investigative methods. Notably, police forces should recruit trained and skilled professionals based on the type of criminal activities they encounter on their operations. The advancements in Natural Language Processing (NLP) tools do not meet police analyst expectations. As such, OSINT teams should expand their capacity with skilled staff

that speak many languages (especially Arabic based languages and dialects). To efficiently fight against crime and terrorism, more skilled and trained officers are required to suppress the illegal transfer of money between organised crime groups either using cryptocurrencies or other traditional monetary exchange methods.

Organisation-related challenges

Even though the use of SOTA solutions to advance LEA EW capabilities is adequately explained, equally important for LEAs is the promotion and development of a culture of preparedness and prevention. Moreover, structural changes that will assist the inclusion of SOTA solutions in LEAs are required. These changes should endorse the addition of new capabilities (either through professional development or with the recruitment of new resources) and specialisation within LEAs, so that the organisation can modernise with AI applications their procedures. This might include the creation of departments that are dedicated in specific threats or specific tasks. In addition, at the organisational level, the need for multi-disciplinary and multi-agency / stakeholder cooperation was underlined. As such, the organisation of common events and trainings should establish and promote collaboration between different Police organisations from EU MS. It would be beneficial for LEAs to involve additional security stakeholders in the fight against organised crime and terrorism. The inclusion of additional security stakeholders (like online service providers, societal organisations, volunteers, etc.) is considered critical especially when it comes to the fight against online and new forms of crime.

Regulatory related challenges

Regarding the fourth THOR dimension that focuses on regulatory aspects, Police Officers identified the need for enforcing regulations and directives to strength inter-LEAs collaborations and support information exchange. Aside from a cultural change required to promote intelligence exchange among LEAs, there is the need for new policy recommendations to facilitate the interconnections of existing LEAs databases and to promote the development and use of SOTA tools capable of performing complex queries in the interconnected databases. Police Officers who participated in MEDEA activities indicated that the legally binding level of these regulatory (and policy) frameworks should vary according to the stakeholders involved. For example, the legal framework governing the process of intelligence exchange between LEAs should be more binding than the directives or recommendations that frame the cooperation between LEAs and other security stakeholders.

The adoption of common definitions and the alignment of laws among EU MS is another need identified during the THOR analysis. Additionally, various practices are considered as criminal activities in certain countries, but not in others, like the use of the Hawala system [19] to transfer money. Even at the national level, LEAs do not always follow the same laws and procedures. Thus, the adoption of a common approach, at least at a Regulatory level, could be very helpful in fighting organised crime and terrorism. Legal frameworks should also be developed, or amended, to accompany the advent of new technologies and technological advancements. For example, AI enhancements should be regulated by relevant laws. To that end, legal frameworks should be amended so as to not impede LEAs in their activities (nor facilitate criminals).

To sum up, after defining specific capability gaps and identifying security challenges, THOR analysis is employed to analyse operational issues along its four dimensions, that can contribute to the formulation of strategies to address challenges, improve responses, and anticipate issues and anomalies in a better equipped manner. A critical component of the THOR methodology that should not be overlooked is that it reveals the interconnection of deficits and the interplay among the distinct four dimensions. Hence, a gap that may be attributed to the lack of technological solutions for its upkeep, might - in reality - be credited to the pre-existing lack of a pertaining regulatory framework, or faulty/inadequate training. This is proven to be central in grasping the fine - and at first glance hidden - aspects of the shortfalls' root causes.

Use Case Findings

Members of OCGs are using End-to-End (E2E) encrypted communications which are offered commercially and are free to use, e.g., messaging and telecommunication services like WhatsApp and

Signal. Decrypted communications are introducing additional challenges to security practitioners when it comes to Lawful Interception (LI). Advancements in quantum computing are required to support decryption and assist LEAs' investigations, while monitoring modern communications in order to collect and analyse information in real time, is more challenging than ever. On the contrary, apart from the need for SOTA solutions, practitioners are also in need of mature technologies, like applications to access multiple databases to retrieve information or access past incidents databases which are not offered to front-line police officers. In this aspect, practitioners need access to unified databases across EU MS that maintain records of illegal content which is being removed. Advancements on AI and ML are not seen in Early Warning systems, thus offered solutions are not efficient to automatically detect online illegal content even in the surface web. In addition, there are not many E2E investigation solutions like automated tools to detect illegal content and translate it from non-well-spoken languages to a language the practitioners can analyse. Finally, offered solutions, apart from their high acquisition cost, do not always support interworking with deployed systems, or do not address the complete range of capability gaps, hence, more than one solution is often required to address most of modern security threats.

Application of THOR methodology in the Human dimension revealed that the lack of reliable translation tools triggers the need to recruit resources with linguistic expertise in OSINT teams, while there is the need for continuous professional development of information analysts. Overall, LEAs should encourage the involvement of native speakers in analysis teams to assist the relevant investigations, profiling, risk assessment, etc. The introduction of tools is always related with the need of additional training to police officers and the establishment of training curricula that will support all phases of police investigations, follow the technology advancement and the continuous complexity of the modus operandi of criminals. Lastly, for the capability gaps resulted from the use of E2E encrypted communication among perpetrators, LEAs should use other technology solutions to intercept communications in open and closed spaces. Also, sharing best practises from successful interception and decryption cases might assist LEAs in dealing more effectively with LI.

Results in the Organisational dimension exposed the need for enhancing cross-border cooperation between LEAs on information exchange and the need to organise joint trainings for their OSINT teams. Moreover, LEAs should offer incentives to encourage practitioners to study foreign languages so as to assist in the analysis of detected 'suspicious' online content, while at the national level, the Internet Referral Units (IRUs) should follow the example of the EU IRU. Furthermore, the cooperation between LEAs and online service providers should be improved to supress online illegal activities and advance interception techniques in communications when there is a court order besides the knowledge transfer between security practitioners and telecommunication experts. In this direction, LEAs should develop training in decryption techniques using joint workshops between LEAs and professionals from telecommunication providers. Equally important, LEAs should update their SOPs to promote usage of existing information databases and foster a culture of interconnecting information repositories with advanced search engines so practitioners can benefit from simultaneous information queries across multiple databases.

In the Regulatory dimension, the main findings with respect to the increasing use of encrypted communication by OCGs are the need for an amendment that will safeguard LEAs' capabilities to lawfully intercept and decrypt these communications, and the need for changes in the current legislative framework to support the adoption of SOTA LI tools so LEAs can gain a competitive advantage to dismantle OCG operations. Similarly, there is a need for policy recommendations to facilitate the interconnections of existing LEA databases and to support the development of tools capable of performing complex queries in interconnected databases. Moreover, regulatory directions are needed to support a framework to advance the existing cooperation between online platform providers and LEAs. The adoption of a new proposal for a regulation that will prevent the dissemination of harmful online illegal content is also advised. In this aspect, a common and inclusive definition of what constitutes illegal online content, which should be very descriptive and detailed, and should be adopted by all EU MS, is recommended. A legislative improvement to assure the protection of fundamental rights and freedoms that will endorse the establishment of autodetection mechanism is required, while

the need to reassess the ethical issues with regards to the use of automated processing by LEAs through techniques in the field of ML and AI will ultimately also benefit societal security.

VI. CONCLUSION

Summing up the core findings and lessons learned from the above-mentioned application of the THOR methodology in the MEDEA project shows that the interplay of the four THOR dimensions provides valuable inputs on the nature and the causes of the capability gaps of practitioners. These inputs can be used to adopt more efficient solutions. For example, a technological gap may be filled by reformulating the pertinent regulatory framework.

This methodology has a track record of being useful in pinpointing broad problematic areas and specific tricky issues alike, by unravelling and promoting understanding of the deeper inter-connections between its four dimensions. Thus, the THOR approach can be adapted to any setting where many factors interact, requiring merely collaboration between experts and practitioners across disciplines, and of several expertise.

The interwoven interplay of the method's four dimensions has further showcased how important human and organisational aspects are to support the technological and regulatory aspects (i.e. the existence/formation of adequate structures, procedures, training curricula, guidelines, SOPs) as well as protocols (steps, roles, user requirements and responsibilities of key actors). It is further revealed how the Regulatory dimension can be a means to enhance technological solutions and not hinder innovation. Hence, unravelling the interconnections between the four THOR dimensions not only helps speed up processes to address operational capability gaps but also provides stakeholders with a clear policy roadmap.

VII. ACKNOWLEDGMENT

MEDEA 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.

VIII. REFERENCES

[1] 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.

[2] G. Kokkinis, *Identifying and Prioritizing Security Capabilities in the Mediterranean and Black Sea Regions Using THOR Analysis,* Mediterranean Security Event, 2019.

[3] 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.

[4] CAMINO consortium, "Comprehensive Approach to cyber roadMap coordINation and develOpment," 31 03 2016. [Online]. Available: https://cordis.europa.eu/project/id/607406. [Accessed 08 03 2019].

[5] INSPEC2T consortium, "Inspiring CitizeNS Participation for Enhanced Community PoliCing AcTions," 30 03 2018. [Online]. Available: https://cordis.europa.eu/project/id/653749. [Accessed 19 11 2019].

[6] TRILLION consortium, “TRusted, CItizen - LEA coILaboratIon over sOcial Networks,” 31 08 2018. [Online]. Available: https://cordis.europa.eu/project/id/653256. [Accessed 19 11 2019].

[7] 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.

[8] 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.

[9] MEDEA Consortium, “Mediterranean practitioners’ network capacity building for effective response to emerging security challenges,” 01 06 2018. [Online]. Available: https://cordis.europa.eu/project/id/787111. [Accessed 08 05 2022].

[10] MEDEA, TCP3, 3CGF.1, “Limited access and use of automated tools to detect radicalisation content leading to violent extremism and terrorism,” 13 05 2020. [Online]. Available: https://www.medea-project.eu/2020/10/07/3-cgf-1. [Accessed 08 05 2022].

[11] MEDEA, TCP3, 3.CGF.2, “Difficulties for LEAs to remove online radicalisation content leading to violent extremism and terrorism,” 13 05 2020. [Online]. Available: https://www.medea-project.eu/2021/05/26/3-cgf-2. [Accessed 08 05 2022].

[12] MEDEA, TCP3, 3.CGF.12, “LEAs require additional capabilities to intercept voice and data communication and decrypt / decipher them,” 13 05 2020. [Online]. Available: https://www.medea-project.eu/2021/05/26/3-cgf-12. [Accessed 08 05 2022].

[13] WhatsApp Inc. (Facebook, Inc.), *WhatsApp.*

[14] Signal Foundation, Signal Messenger LLC and contributors, *Signal.*

[15] CYFOR, “EncroChat: What is it and why did criminals use it?,” [Online]. Available: https://cyfor.co.uk/encrochat-what-is-it-and-why-did-criminals-use-it/. [Accessed 08 05 2022].

[16] C. W. Bill Goodwin, “Police EncroChat cryptophone hacking implant did not work properly and frequently failed,” 11 03 2022. [Online]. Available: https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed. [Accessed 08 05 2022].

[17] MEDEA, TCP3, 3.CGF.11, “Better exploitation of existing databases and enforce open interfaces to data processing tools,” 13 05 2020. [Online]. Available: https://www.medea-project.eu/2021/05/26/3-cgf-11/. [Accessed 08 05 2022].

[18] United Nations Office for the Coordination of Humanitarian Affairs, “Five approaches to build functional Early Warning Systems,” 17 01 2019. [Online]. Available: https://reliefweb.int/report/world/five-approaches-build-functional-early-warning-systems. [Accessed 08 05 2022].

[19] M. El-Qorchi, “The Hawala System,” *Finance and Development,* vol. 39, no. 4, 2002.