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

Call for Ideas and Solutions – Terms of Reference

Annex 2 MEDEA network of Practitioners - Capability Gap Findings

MEDEA Network of Practitioners – Capability Gap Findings (CGFs)

A. Proposals related to the following challenges, pertaining to the Management of migration flows and asylum seekers (TCP1)

1) Absence of an independent authority to monitor NGO operations. 1.CGF.1

There are institutions monitoring the application of human rights and checking this at both national level and higher levels (e.g. at the EU level, FRA institution, is an organization in charge of monitoring migration issues and human rights). However, all these efforts should be strengthened on a national level and have EU as monitoring and high-level of coordination. In addition to that, a unified EU registry of NGOs could be of benefit, including not only on the monitoring of human rights issues, but mainly NGOs which are trustworthy when they undertake tasks like unaccompanied minors or SAR, thus from a legal point of view could complement the national registry of NGOS. However, it is vital to make sure that administrative requirements for registering NGOs should not be extensively bureaucratic so that NGOs will be able to effectively deliver their humanitarian work.

2) Need for a common European migration and asylum policy and need to amend and reinforce the Common European Asylum System (CEAS), so that practitioners' requirements and needs are represented within the CEAS network. 1.CGF.2&6

The existence of different directives, national legislations, EU Legislations constitutes a major challenge, so a unified legal framework is an imperative need for practitioners. In the case of unaccompanied minors there is a huge gap in issues of protection and detection, as well as provisions for conditions in detention centres for the minors. EU legislation is effectively communicated to practitioners; however, the implementation involves different administrations, governments, activities, etc., thus cooperation among countries is imperative, respecting in parallel the fundamental rights of individuals. In addition to that, the lack of a homogeneous access to the asylum procedure leads to discriminatory practices and complicates the process with interferences between national and international laws regarding protection.

3) Insufficient means and lack of coordination for effective Search and Rescue (SaR) Operations 1.CGF.3&4

Grouping together two interconnected gaps vis-à-vis SaR, namely the fact that we have at our disposal insufficient means, while at the same time there is a perceived lack of coordination for effective SaR operations, the webinar findings are the following: SaR operations are mostly assumed by the Coast Guard, though police and various law enforcement authorities assist the

Coast Guard in their efforts. Frontex provides relevant surveillance tools and coordinates the SaR activities. Since private entities – such as NGOs – intervene in SaR operations with vessels, the European Commission has formed recommendations for the cooperation between them and Law Enforcement Agencies (LEAs). Implementing said recommendations is crucial to ensure the safety of everyone involved.

With regard to the question about whether the existence of vessels for SaR offers an extra motive for migrants to cross over to Europe, knowing that they will be rescued should anything happen, the general consensus was that although this would seem to be the case, it is not a sufficient condition in itself. Since this is a complex issue, we must take into serious consideration the fact that organised crime networks that partake in migrant smuggling, would try their best to avoid routes where they would come across SaR vessels. So, although the existence of vessels provides both a pull and a push factor vis-à-vis illegal immigration, in most cases where migrant boats see SaR vessels (e.g. in the Aegean Sea), they quickly flee without approaching.

4) No adequate training is provided to practitioners regarding current legislation with respect to migrant smuggling and the protection of unaccompanied minors. 1.CGF.5

Human trafficking

There is a need for consistent and continuous training regarding identification at the borders, which should mainly consist of screening technology and up-to-date workshops on investigative tools, persecution, criminal networks etc. (which is already provided in some EU MS). Some of the challenges that have been identified regarding human trafficking, are linked to the fact that small ships with few migrants take new routes, while transporting criminals mixed among the migrants. Therefore, identification of migrants, victims, and criminals is problematic as well as crucial, as is the timely identification of the new routes. Effective coordination of different stakeholders is needed in that respect.

Sure enough, the main identification protocol relies on interviews and collection of immigrants' fingerprints, however immigrants occasionally lie about the information they provide, making the need for accurate and precise information more critical. A possible solution relies on the creation of information hotspots which include translators, cultural mediators, forensic police and other law authorities.

Unaccompanied minors

Unaccompanied minors appear more distressed and do not adjust easily. They need additional help and guidance due to their inability to adequately gather useful information and instructions regarding their next steps. Therefore, legal aid expressly for them should be put into place, in order to provide advice and support in preparing their applications for international protection or family reunification. NGOs can offer crucial help in this domain.

A step in the right direction is also made by the Commission's proposal for a new pact on migration and asylum, which exempts minors from border procedures.

Furthermore, additional caution should be exercised while sharing information on minors. Due to their inherent vulnerability, all processes must be done carefully and 'by the book', and always in contact with the public authorities (note that the public prosecutor's office is the temporary legal guardian of minors).

5) Lack of effective and enhanced cooperation among EU Member States, as well as between Member States and third countries – Need for an advanced return process. 1.CGF.7

A priority of utmost importance is the effective cooperation not only among MS but also with third countries, whether they are countries of origin or transit. Cooperation with third countries is imperative, as there are different policies among each country (e.g. for return process etc.). The common theme that emerges through the efforts for such collaboration is the fact that third countries are both reluctant and unmotivated to efficiently cooperate in migration and asylum matters. This unwillingness causes delays and stems from many factors. First, countries of transit or origin often have their own significant internal problems to tackle, thus viewing migration as less of a priority. Hence, if they deem that there is nothing to gain, or that the benefits in cooperating with EU MS regarding migrants and asylum seekers are not substantial enough, they are disinclined to work towards this goal.

Another component of critical significance is the parallel existence of different legislations. This element causes lags in decision making and policy formation among EU Member States. Justifiably so, those lags become more apparent between the MS and third countries, since diverse legislations hinder prompt and effective cooperation, often leading to inertia.

To deal with this issue, it is important to start a concrete dialogue with third, neighbouring countries and countries of origin under the auspices of the EU institutions. Further, it is crucial to find ways to support the stabilisation of neighbouring countries, since political and social unrest is a main driver behind emigration and asylum seeking. However, the point was made that it would be counter-productive to sign new agreements with third countries, when there are already existing agreements that are still pending to materialise. The agreements that are in place should be resolved, concluded, and evaluated before going on to making new ones.

In any case, the Commission's proposed Pact on Migration and Asylum endeavours to decongest the Member States by allowing them to provide "return sponsorship" instead of relocating people to their own territories.

6) Information databases / repositories from various practitioners at National and European level are not interconnected. 1.CGF.8

Information exchange among practitioners of EU MS, as well as between MS and third countries, is of crucial importance. Limited access to information regarding third countries provides an added obstacle. Municipalities, NGOs, and universities have been working on a system to predict migration flows from data received from migrants and origin countries. Certainly, European projects along with their respective online platforms create a valid place to share information and develop these data exchange tools. Information exchanges must exercise caution as security should be guaranteed, data should be protected, and technological glitches addressed promptly. Nevertheless, a sizeable amount of information may be found in social networks and it has been observed that social media have the capacity to drive migration flows. Note: It is vital in this aspect not to forget the human factor. Often, information exchange between practitioners is not technological but procedural. Similarly, in several cases, physical meetings are preferred by practitioners for the exchange of personal data since certain technological systems are not always secure. For sure, information exchange between LEAs and EU agencies such as Europol and Frontex is continuous. There is also exchange between the Member States with the support of the European agencies. It should be noted that certain information exchanges between MS' LEAs need a specific judicial or high rank hierarchy authorisation. NGOs have a protocol for exchanging information with LEAs, considering the confidentiality of the data. Furthermore, they frequently exchange information with other NGOs. This information exchange is especially important when dealing with vulnerable cases. In addition, those who work with unaccompanied minors are always in contact with public authorities and prosecutors. Understandably, information related to minors is delicate and must comply with the GDPR. Consequently, before sharing personal information with other organizations or practitioners it is necessary to ask for permission from the public prosecutor's office.

7) Lack of a common risk analysis process. 1.CGF.9

The Common Integrated Risk Analysis Model (CIRAM), is a model that LEAs in Member States need to apply. It is developed by Frontex and mandatory for all MS, integrating all the aspects from border management. The monitoring and assessment are carried by Frontex on regular basis. Joint operations and rapid border interventions are preceded by a reliable risk analysis. MS take these results of the risk analyses and integrate them to their operations and activities at the external borders including returns. Frontex also produces yearly a vulnerability assessment to assess the readiness of MS to assess the threat and the new challenges. From this vulnerability assessment, Frontex recommends specific actions to mitigate those vulnerabilities. However, the need of new enhanced regulations, effective processes and risk assessment is underlined, as, based on the new Frontex regulation, EU along with the MS are working together to develop more focused and tailor-made capability roadmaps and capability planning.

8) Existing technological tools used by practitioners are outdated 1.CGF.10

There is a general lack of advanced technological mechanisms and resources at the disposal of practitioners, that would be vital in order to improve efficiency in preventive security measures. For example, there is a perceived need for sophisticated border crossing preventive mechanisms such as state-of-the-art detectors and radars. Also, depending on the type of landscape, early detection can be more challenging. Therefore, in such areas it would be beneficial to use new technology such as advanced video analytics. Additionally, it is necessary to improve current capabilities related to the detection of falsified (fraudulent) documents. Likewise, practitioners should be equipped with the right tools and training to also detect falsified multimedia material which is often supplied as evidence. Undeniably, in order to be able to use such new technology, the current regulatory framework must be amended to encompass the adoption of new technological solutions.

Also, now, the new Frontex regulation is being defined and implemented. Frontex and Member States (MS) work together to develop capability roadmaps and capability planning and to look for and implement specific technologies and solutions instead of the general ones that are in place. In this context, it is necessary to take into account - for future actions and implementation - the new technologies that will emerge in the next few years, such as artificial intelligence, new network environments, encryption systems, and advanced communications in the digital world. Of course, it is critical to tackle the gap of interoperability, through finding common ground and building systems, solutions, and networks so that they can interact in a common language.

9) Health risks related to the daily operations of practitioners. 1.CGF.11

Practitioners operate in a highly stressful environment, often amid humanitarian crises. They face health hazards related to both psychological and physical health; two aspects closely inter-related in the context of the Covid-19 pandemic. COVID-19 has brought a huge impact on the psychology of practitioners, due to the continuous stress they are induced in. Since immigrants are held in quarantine for several days, the risk of virus contamination is high in practitioners. Given the precarious situation that the pandemic creates, more psychosocial and psycho-social support and improved sanitary conditions are needed in order to increase the practitioners' resilience. In addition to that, there is a need for training, psychological support and special capabilities for individuals working with unaccompanied minors that are suffering high level of stress because of their situation, living apart from their families.

B. Proposals related to the following challenges, pertaining to Border management and surveillance (TCP2).

10) Absence of security solution standardisation and certification 2.CGF.11

Practitioners highlighted the lack of commonly accepted and used technology standards for the security solutions deployed. Currently the security solutions are standardised as stand-alone systems. Most of the security solutions are vendor specific and not standardised / certified for deployment and interworking with existing deployed security systems. This is described with 2.CGF.11.

In the military domain MIL-STD-XXX series may be based or make reference to existing, well established standards maintained by standardisation bodies. Typically, there is a handbook that outlines the standard procedural, technical, engineering, or design information about the solutions, processes, practices the products should satisfy. There are also "specifications" that describe either the essential technical requirements for the product or the substantially modified commercial standards. Performance specifications are also used. They described solution requirements in terms of the required results with criteria for verifying compliance but without stating the methods for achieving the required results. Likewise, the standards that will be enforced for security solutions will utilise existing ones.

It should be acknowledged that dual use of technology in both military and civilian domains refers to developed solutions and products which can serve both military and civilian entities at any given time. Notably only the military products are standardised. The use of defence standards, often called a military standard, is used to help achieve standardisation objectives. The standardisation of defence solutions is beneficial in achieving interoperability, ensuring products meet certain requirements, commonality, reliability, reduces total cost of ownership, are a few benefits. On the opposite side, security products and solutions available to border guard practitioners are not standardised, interfaces and products are proprietary to manufacturers, commercial standards are used for a subset of their characteristics, interoperability between systems is not straightforward.

11) Lack of a multi-sectoral ecosystem for security solutions 2.CGF.12

Security practitioners need solutions and products with open/common interconnection interfaces for systems that will be deployed in the borders. Further to Capability Gap No 2.CGF.11: Absence of security solution standardisation and certification, an approach is required to interconnect (with minimum effort) solutions from different vendors and ensure interworking between different subsystems (e.g., common video analytics from surveillance cameras and seamless or minimum effort interworking with deployed radars and other sensors installed along the borders). It should be highlighted that interoperability will be a key component to drive the growth of security industry. The creation of a standardised ecosystem where solutions from different providers can communicate and work together will be beneficial for the end users. As a result, this will almost certainly lead to more advanced security solutions with more functionalities supported by stronger pricing and performance competition.

The delivery of products developed around end user needs will be also beneficial for solution providers since their solution roadmap will be driven by their potential customers. It should be

highlighted that the digital transformation of physical security is still in its infancy compared to other industries. The value proposition of digital transformation goes beyond the traditional Return of Investment (ROI) metrics. A combined view of returns should also measure the added value that will be created from developing solutions using advanced analytics, Artificial Intelligence (AI), and Machine Learning (ML). The focused development of security solution using beyond State of the Art (SOTA) technologies will foster the required conditions for an ecosystem with more advanced and more suitable security products, that will lead to faster adoption of security products by public authorities who are the end users.

Again, the military equivalent, the Multilateral Interoperability Programme (MIP) established to support solution providers to exchange information should serve as a good example. MIP produces a set of specifications which when implemented by the stakeholders, provide the required interoperability capability. Also, MIP provides a venue for system level interoperability testing. The result is the development of interoperable solutions, which have undergone testing to ensure their interoperability. The outcome of these activities is an ecosystem of interoperable solutions.

12) Lack in support of legacy / deployed solutions 2.CGF.13

The practitioners indicated that they are using already a large number of technology solutions for border surveillance tasks. These technology solutions vary from surveillance cameras (at the beginning the installed base of cameras were deployed for daily observation and at a later stage night vision cameras were added), together with radars, Unattended Ground Sensors (UGS), and other sensors. Recently practitioners along the borders are using Lighter Than Air (LTA) Aircrafts (also known as Tactical Aerostats) to mount sensors, Lightweight Surveillance and Target Acquisition Radars (LSTAR) to detect humans or drones, and more sophisticated cameras, and video analytics at the command-and-control centres. This list of sensors is not extensive, but its purpose is to showcase that there is a large investment made to increase practitioners' detection capabilities. As such new state of the art (SOTA) border surveillance solutions should complement the existing installed base of sensors. Therefore, the new systems should be backwards compatible with the deployed legacy systems. This requirement is identified in MEDEA TCP2 as capability gap finding no. 2.CGF.13. More important, interconnection interfaces with command-and-control systems are required to ensure the new sensors can be easily integrated with the operational command and control centres.

13) Lack of systematic identification and removal of illegal context on the internet 2.CGF.14

The practitioners had identified that they need technology solutions to assist them with the detection of illegal content in the web so they can remove it afterwards. This is described in Capability Gap Finding 2.CGF.14. Upon the identification of inappropriate context online, the practitioners should follow up with the necessary activities to either remove it or block access to it. This capability gap is two-fold. It has to do with better detection capabilities that pertain to

the identification of illegal online context, and then it has to do with its removal. In TCP2 this capability gap surfaced from videos and online content which provide detailed instructions mostly to migrants to enter undetected in Europe by indicating and providing regular updates about pathways that are not guarded 24x7. The challenge experienced is that although the illegal instructions are online and are well-advertised in Social Media, it is difficult to practitioners to identify them for a number of reasons. There are a number of OSINT tools that can be used with online platforms; however, the content is mostly in Arabic speaking language. This gap will be analysed in TCP3 under [3.CGF.2] – "Difficulties for LEAs to remove online radicalisation content leading to violent extremism and terrorism". To account the vast applicability of the gap, TCP3 will examine this gap in the context of various cross-border crimes.

14) Insufficient safeguards of intelligence about practitioners' assets and resources 2.CGF.15

Practitioners would like to prevent adversaries from gathering intelligence about them. This is described with capability gap number 2.CGF.15. In detail, security personnel operating along the borders, apart from the fact that they are custodians of sensitive information (both classified and unclassified) they use certain assets and operate certain technologies with a finite number of resources. The information about personnel resources, the solutions deployed, and their location are routinely targeted by adversary intelligence entities. Aside the Human Intelligence (HUMINT), perpetrators also use Technical Intelligence (TECHINT). For example, facilitators use similar technologies like the security personnel (e.g., night vision goggles) or they are aware of the type of sensors deployed, thus they know their technical capabilities of the equipment. Furthermore, they are aware of the technology/solution shortfalls and more importantly, they exploit migrants to identify areas along the borders that have vulnerabilities. Consequently, security practitioners would like to minimize and mitigate the risks related to perpetrators who collect information about their deployed systems and resources.

15) Underutilised lessons learned culture 2.CGF.16

Another gap that surfaced from the practitioners' workshop is related with the overall lessons learnt process. More specifically, the need for the adoption of a solid approach to efficiently exploit lessons learnt from past events and other EU MS was identified. Knowledge developed from dealing with similar incidents in the past, actions that worked or failed to work, what measures were more efficient than others and general what constitutes tacit knowledge, are not adequately exploited by many organisations. Transfer of knowledge can occur within the same organisations, practitioners from different disciplines that encountered similar challenges, and even between practitioner organisations from other EU MS.

To optimally exploit knowledge and lessons learned, an organisation should use a repository to record past events, their timeline, the stakeholders evolved, findings from debriefings, etc. Past records from incident databases can be examined and analysed to retrieve useful experience and

avoid their recurrence (if possible) or better mitigate their consequences. Lessons learned can be derived for the technology (solutions that make an impact), Human (training required or joint exercises between stakeholders who should collaborate more effectively), Organisational and Regulatory/Policy dimensions. Past incidents can also be used for awareness and focused trainings. Lastly, analysts will gain valuable knowledge from past incidents and might come across useful findings.

⚠ Please note that this capability gap is also identified in TCP4 with 4.CGF.20

16) Insufficient technology adoption mechanisms 2.CGF.17

There are concerns about an "innovation emergency" across practitioners' organisations from EU MS, the causes of which is related to limited or restricted adoption of technological solutionσ by them. The reasons that SOTA technology tools are not embraced by practitioners are: (1) The practitioners' institution strategy is not aligned with technology roadmaps; (2) Practitioners organisations are not part of industry efforts to advance products and develop solutions; (3) Current practitioners needs and gap capabilities are not performed in a systematic and standardised manner; (4) No technology training is offered to practitioners; (5) Technology deployment plans require a change management approach (which is unpleasant by nature to practitioners); and last but not least an effective governance structure to advance the technology adoption by practitioners is associated with political will for transformation. The practitioners formulated with [2.CGF.17] that there is a mismatch between established procedures and capabilities enabled by innovative solutions. There are a number of research projects in security, however the research results are not yet considered by practitioners' organisations.

⚠ Please note that this capability gap is also identified in TCP4 with 4.CGF.9

17) Lack of early detection in difficult/challenging landscapes or weather conditions 2.CGF.18&19

Border security and surveillance at the EU outside borders is a 24x365 operation required to ensure EU MS security against a variety of threats. As such, reliable long-range threat detection and positive identification of potential threats at day and night, in all environment conditions across different landscape is needed. Whether Border Guard Authorities need to survey either green or blue borders, looking for people crossing the borders, or small boats sailing to shore, solutions are required to offer early warning and threat assessment needed so practitioners can respond efficiently and effectively. Early warning systems are required to timely detect potential threats which should then be identified, so that their threat level can be assessed. The time for early detection is determined by the time required by practitioners to reach the border first and deter the threat. Consequently, technology solutions to provide early detection in environments where it is difficult to survey are needed taking into account the landscape characteristics and the lack of power sources. This capability gap is identified as 2.CGF.18. Moreover, technology

solutions to offer standard performance for a variety of weather conditions (same performance 24x365) is recorded in capability gap 2.CGF.19.

> This capability gap is being complemented by cooperation between EU MS and third countries (2.CGF.2).

18) Lack of a Common Pre-frontier Intelligence picture 2.CGF.20

A solution that will offer the desired prefrontier intelligence picture for various border types is required. This involves intelligence from land borders, maritime borders, and intelligence sharing among practitioners from different discipline organisations in the same country (initially) and subsequent cooperation between multidiscipline organisations across the borders (from different EU MS). Since its establishment in 2013 (Regulation (EU) No 1052/2013), the European Border Surveillance system (EUROSUR) is a framework for information exchange and cooperation between Member States and Frontex to improve situational awareness and increase reaction capability at the external borders. The EUROSUR's vision to "help detect and fight criminal networks' activities and will be a crucial tool for saving migrants who put their lives at risk trying to reach EU shores" is challenged for its effective implementation after the 2015 migration crisis. The capability gap no 2.CGF.20 refers to better situational awareness (monitoring, detection, identification, tracking) while the subsequent gaps 2.CGF.21, 2.CGF.22, and 2.CGF.23 refer to better reaction (prevention and interception of unauthorised border crossings) capabilities. (Ref. to EUROSUR Fusion Services).

Situational picture is a three (3) layer picture composed with information on events (events layer) patrolling assets (operational layer) and findings from Analysis processes (analysis layer). Each EU MS manages its own National Situational Picture while Frontex manages the European Situational Picture, which is covering Member States' territory and the ***Common Pre-frontier intelligence picture (CPIP)*** which is ***covering the area beyond the external borders*** (land, sea, and air). As such, the Common Pre-frontier intelligence picture is a gap mostly applicable to Europe's Border and Coast Guard Agency (Frontex) tasked to provide the National Coordination Centres (NCC) with effective, accurate, and timely information and analysis on the pre-frontier area. The risk indicators complement CPIP needs to be improved, enriched with the findings of OSINT and IMINT (at minimum).

19) Lack of border crossing preventive mechanisms 2.CGF.21-23

Prior to introducing and describing these three gaps, the different border types (airport, green and blue) should be introduced. **Airport borders** are the least challenging for practitioners to control. Border crossers arrive in a confined space, are visible as they walk through various checkpoints, their papers are checked quickly against information in databases and they are observed for unusual and suspicious behaviours by a large number of border guards, dogs and their handlers, and occasional profilers. **Land** (***Green***) **borders** are similar to airport checks only for the established border Crossing points (BCPs). Most of the land border management

challenges are encountered along the land borders between BCPs. The distances between the BCPs are the majority of the land borders. Security along this border type is composed of many distinct elements, including physical and artificial barriers, the deployment of border patrol personnel and installation of surveillance technological means like long-range radars, sensors sprinkled on suspected routes, patrols by vehicles and UAVs and observation towers. In general, border controls which years ago were handled by military units, have been replaced by technology, fast response units from Border Guard Authorities (BGAs) when alerted and the assistance of national police. Once suspected illegal crossers are detected, border guards can be dispatched to intercept them if possible, and local national police is notified of the incursions of unwanted and irregular crossers for further law enforcement actions within the internal space of the EU. **Sea** (***Blue***) **borders** present their own challenges. Their management requires massive investments in vessels and observation technology to detect small boats before they reach the territorial waters and shores of the EU.

Better preventive mechanisms are needed along the borders. Legislation and procedures between EU and third countries should be adapted. This is a brief description of capability gap no 2. CGF.21. Along the border management task, BGA should enforce preventive measures to discourage, timely detect, and prevent cross-border illegal activities such as migrant smuggling, trafficking in human beings and terrorism. Risk Analysis is a powerful tool which is not fully exploited at practitioners stationed at EU external borders. Moreover, the use of additional means (equipment and resources), are one of the measures used to deter illegal activities along the borders. It should be emphasised that the outcome of the ongoing border management activities produced intelligence to adversaries about the number of resources, equipment, and the required time to respond to illegal border activities, therefore there is a continuous need for additional preventive measures to offset limited response capabilities. In other words, additional preventive measures are needed to balance BGA limitations to respond at the same time at different locations with the required means.

There are two more capability (sub) gaps associated with prevention. ***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 (C2) centres***. This is described with 2.CGF.22. In addition, ***more sophisticated detection methods are required to prevent smuggling to normal Border Crossing Points (BCP) and along borders in general***.

⚠ This is described with 2.CGF.23, which will be researched in future workshops.

20) Lack in special forces (rapid deployment teams) 2.CGF.24

Each EU MS located at the EU external borders is responsible for the management of their borders, thus it is a national obligation to proceed with necessary actions to prevent crisis situations and to respond with the available means effectively, at an early stage, at its borders. Migration flows can increase rapidly leading to security incidents difficult to be managed, therefore personnel on the ground for migration management is required. This is described with

capability gap 2.CGF.24. In addition, the development of Rapid deployment teams with certain capabilities and skills (translators, social workers, medical staff) will assist BGAs to better respond to high migration flows.

21) Gaps in EO Service timeliness 2.CGF.25-28

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).

22) Insufficient EO Service quality 2.CGF.29-33

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).

23) Lack in EO Service awareness, skills, and acceptance 2.CGF.34-36

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).

C. Proposals related to the following challenges pertaining to the Fight against cross-border organised crime and terrorism (TCP3)

24) Limited access and use of automated tools to detect radicalisation content leading to violent extremism and terrorism. 3.CGF.1

The automatic detection of online illegal content (either content that facilitates radicalisation or promoting crime activities or provides instructions of how to perform them) is a much-needed capability for LEAs. The capability gap arises from the vast amount of open-source data that needs to be searched by the Open-Source Intelligence Team (OSINT). Nowadays OSINT teams are using either commercial tools but with limited number of licenses or restricted functionalities because of their acquisition cost or in-house customised open-source tools. As such an automated Early Warning System is needed, with adequate licenses to utilise LEA's capacity in OSINT.

25) Difficulties for LEAs to remove online radicalisation content leading to violent extremism and terrorism. 3.CGF.2

Once the online radicalisation content is identified, it should be removed. However, the removal of online content is not a straightforward process, and it is subject to different regulations and procedures based on there it is hosted. Currently, the EU regulatory framework on content moderation is increasingly complex and has been differentiated over the years according to the category of the online platform and the type of content. It will be beneficial to harmonise the removal processes across all EU MS for a start.

26) Better collaboration is required with Educational and Social Services for minors possibly prone to be radicalised. 3.CGF.5

Although practitioners have become experienced to assess whether an individual is vulnerable to being drawn into terrorism because of radicalisation, they are often lacking the background information about these individuals. Subsequent steps like assess the nature and extent of that risk and develop a support plan for the individuals concerned are jeopardised because actors from Educational and Social Services are hesitant to cooperate with police. Therefore, practitioners are missing the capabilities to acquire valuable intelligence from these stakeholders and identify timely minors at risk.

27) Need for common processes, procedures, and laws among practitioners to suppress online radicalisation. 3.CGF.7

The practitioners acknowledged that the identification of online user who posts terrorist/illegal content is difficult task. Yet, even if the LEAs can quantify the risk associated with specific online users there is confusion on what measures should be taken against them. Therefore, security practitioners need the establishment of common processes, procedures, and laws that will be enforced to EU MS through regulations and directives.

28) Intelligence exchange between practitioners from different organisations and countries is needed from the early stages to monitor effectively the Organised Criminal Group (OCG) activities. 3.CGF.9

Intelligence sharing between practitioners serving in multi-disciple organisations (e.g., police, customs, and judicial authorities) is a required capability. Considering the cross-border character of the criminal activities and the multitude of law enforcement agencies involved (different countries and different organisations) better tools and updated procedures that will enhance co-operation and enable all stakeholders to have the same operational picture are needed.

29) Need for improved surveillance capabilities for both land and sea smuggling routes. 3.CGF.10

Improved surveillance means are required for the detection of suspicious transported containers by both land and sea routes. LEAS need real - time geo-location information about suspected freights (online tracking). OCGs use several and different routes for smuggling drugs \ illicit items \ counterfeit products and LEAs should be capable of monitoring them. In additions OCG are using countermeasures like jammers to diminish current LEA capabilities. More important additional trained resources are required for surveillance tasks.

30) Better exploitation of existing databases and enforce open interfaces to data processing tools. 3.CGF.11

The practitioners would need a single and 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, types of trafficked items, countries and places where the offenders carry out their criminal activities, and other characteristics which will assist practitioners with their investigations. Apart of 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.

31) LEAs require additional capabilities to intercept voice and data communication and decrypt / decipher them. 3.CGF.12

Practitioners need better capabilities to intercept and decrypt the ciphered communications between OCG members. The interception and decryption of these communications is a very difficult and time-consuming task. The vast number of commercial applications and the uncomplicated development of customised applications for mobile devices, makes the use of customised communication products with encryption favourable by to perpetrators. At the same time, it becomes more difficult and more complicated to practitioners to decrypt OCG communications.

32) Limitations in suppressing the non-legal transfer of funds (economic crime using the Hawala method and Cryptocurrencies) attributed to smuggling activities. 3.CGF.13

Practitioners need additional capabilities to first detect the illicit ways OCG are using to transfer funds and finance their activities. Financial networks like the Hawala system, or modern cryptocurrencies is a very a challenging task for LEAs to dismantle them. Typically, LEAs usually focus on the intelligence capabilities during an operation and often neglect or not pay adequate attention to the financial crime associated with money laundering. Therefore, changes should be performed to fully exploit the available capabilities and agree what is needed in terms of additional capabilities to suppress illegal transfer of funds.

33) Requirement for stronger and more effective cooperation between stakeholders from various disciplines across different EU Member States and EU third countries. 3.CGF.14

There is a need to improve the current cooperation among different agencies involved in the same anti-crime operation. Improved cooperation between LEAs and Coast-guard authorities, custom authorities and judicial authorities is very important as they are all involved in the fighting of drug smuggling. The collaboration with judicial authorities would better support legal aspects related to interagency cooperation and large-scale operations. LEAs from various organisations should enhance their current level of cooperation using an information sharing platform instead of existing communication channels though appointed liaisons / contact officers.

34) Need for additional capabilities for SIGINT, IMINT, OSINT to facilitate LEAs' information analysis units. 3.CGF.15

Technological advancements in the fields of Signal Intelligence (SIGINT), Image Intelligence (IMINT), and Open-Source Intelligence (OSINT) should be exploited to help competent authorities in their fight against drug smuggling. SIGINT not only can be used to gather intelligence by intercepting signals and electronic communications on the routes of transporting drugs, but it

can also be deployed to process, and extract data related to cryptocurrencies. IMINT can be used for surveillance of drug transporting routes. Also, GIS products can be used to analyse the available data from the geographical point of view. Finally, OSINT can be used to gather information about the OCG members and involved companies.

35) Need for innovative solutions to advance the detection (and analysis) of concealed drugs within vehicles, containers, transported goods, and people. 3.CGF.18

The detection of drugs is a much needed for the LEAs. Detection should be improved by using widely equipment installed at specific locations. In addition, there is need for portable solutions to identify and analyse on the field the confiscated substances. Apart from this, training courses must be carried out regularly for front line officers to be able to detect drugs fast and effectively by using simpler tools.

D. Proposals related to the following Natural hazards and technological accidents (TCP4) challenges.

36) Inadequate Perception of Fire Risk and Lack of Risk Awareness in Wildland Urban Interface Areas 4.CGF.1

It was agreed that there is **Lack of security culture:** wildfire risk prevention is not integrated in the mindset and lifestyle of the citizens living in the WUI areas. Also, many citizens remain inactive even if they are informed about the fire risk, that is there is **no perception neither ownership of fire risk.** Both WUI residents and practitioners operating in WUI areas agreed that there are no adequate citizen awareness campaigns and there are no **Systematic** risk communications to residents. Lastly, **Tourists and visitors** to WUI fire-prone areas are **more** exposed to fire risk than locals since they have limited knowledge of the territory and the local risks. As a result, there is *Inadequate Perception of Fire Risk and Lack of Risk Awareness in Wildland Urban Interface Areas.*

37) Lack of Reliable and Real-Time Information on Crisis Communication4.CGF.3

Usually the people **do not know where to get reliable information from** before a WUI fire occurs or during the fire event. Authorities are **not** adequately trained to **provide clear and straightforward information**. Consequently, the residents or the population at risk seldom follow recommendations. It was confirmed that there is *Lack of Reliable and Real-Time Information on Crisis Communication.*

38) Lack of Interoperable Systems and Real-Time Situational Awareness in Firefighting4.CGF.4

It is widely observed that there **is lack of communication, cooperation and information-sharing** between different authorities. Each practitioner organisation that is likely to be involved in a WUI fire incident has **no interoperable systems to exchange information**. Typically, if there are any **WUI fire response plans**, these **are not shared among agencies** neither a common platform is used. As a result, what is known as **Common Operational Picture** (COP) during the incident **is not shared** (most of the times) **between different practitioner organisations**. Therefore, *not All Stakeholders Share the Same Operational Picture. Lack of Interoperable Systems and Real-Time Situational Awareness in Firefighting.*

39) Lack of evidence-based knowledge regarding evacuation due to fire behaviour in Wildland Urban Interface areas 4.CGF.7

There are **no formal guidelines and evacuation plans for WUI settlements**, and the **evacuation instructions may be misused or disregarded** and eventually jeopardize population's safety. *Difficulties in evacuating large number of people in a small amount of time while preventing that people get trapped while trying to escape,* is one of the major issues in fire management.

40) Lack of a Standardised and Interdisciplinary Methodology for Developing Wildland Urban Interface Prevention Plans 4.CGF.2

First Responders, local and regional authorities, homeowners, residents developed prevention plans individually (if they develop any), without consultation and guidance from authorities, (which in many cases are not capable of issuing specific WUI prevention plans) often **following different methodologies**. As such, there is *Lack of a Standardised and Interdisciplinary Methodology for Developing Wildland Urban Interface Prevention Plans.*

41) Lack of Evidence-Based Knowledge (Including Risk Assessment and Cascading Effects) on Fire Behaviour in Wildland Urban Interface Areas 4.CGF.5

It was agreed among practitioners that it is **difficult to accurately anticipate the fire development and the cascading effects in WUI areas**. There is **heterogeneity of the conditions inside WUI areas**, notably concerning fuel categories (buildings, gardens and natural vegetation) and their spatial distribution patterns. There is also **scattered presence of individuals and groups of people in an actively burning area**. Lastly, there are no risk assessment models adapted to the specific characteristics of fire behaviour and propagation in WUI areas. To summarise the above, there is *Lack of Evidence-Based Knowledge (Including Risk Assessment and Cascading Effects) On Fire Behavior in Wildland Urban Interface Areas*.

42) Inadequate Fire-Fighting Knowledge and Shortage of Fire-Suppression Resources and Operational Means for Operating in Wildland Urban Interface Areas 4.CGF.6

There is **no adequate knowledge concerning wildfire management in WUI areas**, a non-homogeneous environment with numerous particularities ((including human presence spatial and temporal patterns). Often, there is **missing geographic information about people and buildings in danger during a WUI fire**. There are **challenges in training of first responders in the WUI environment,** while there are no specific firefighting operational means, either terrestrial or aerial, suitable for intervention in the WUI area. Thus, there is *Inadequate Fire-Fighting Knowledge and Shortage of Fire-Suppression Resources and Operational Means for Operating in Wildland Urban Interface Areas.*

43) Limits in implementing in-place sheltering4.CGF.8

There are **misconceptions concerning the use of houses as shelters** while **no specific guidelines exist for home-protection in WUI areas**. Moreover, there are **no building standards in** vulnerable **WUI environments and people do not feel safe in their houses when surrounded by fire.** As such, there are notable *Limits in implementing in-place sheltering.*

44) Lack of adoption of innovative tools in firefighting4.CGF.9

There is **mismatch between established procedures and capabilities enabled by innovative solutions**. It is important thus, to underline that the *current procedures inhibit deployment of innovative tools*.

45) Need for improved (spatially and temporally) weather forecasts and more accurate tracking of flooded areas 4.CGF.10

It was agreed that there is **…**

Need for **cooperation between the meteorological** community, the **hydrological** community and the **practitioners**, who will eventually exploit the flood modelling outcomes.

Need for **better instrumentation** in most Mediterranean areas (where rich relief is dominant) to better represent the local weather conditions through networks of weather radars, dense rain gauge networks and most importantly dense streamflow gauge networks.

Need to have **weather forecasts that take into account specific needs and particularities of an area:** the optimal temporal and spatial resolution as provided from weather forecasts and required from flood models is not straightforward --> depends on specific needs and particularities of an area.

Better **prewarning time** for evacuation orders and other measures to be taken

EFAS (European Flood Awareness System) notifications could **consider greater return periods** in order to "catch" extreme events.

Need to **determine an optimal accuracy in weather forecasts,** which depends on specific requirements of each case: Increased accuracy is a constant requirement; yet, the determination of optimal accuracy is also not straightforward (depends on specific requirements)

As a result, there is *Need for improved (spatially and temporally) weather forecasts and more accurate tracking of flooded areas*

46) Need for improved (spatially and temporally) flash flood related information to authorities and the general population 4.CGF.11

Need to **identify ways to better disseminate the outcomes of the probabilistic approach** (which is typical in weather forecasting and flood modelling) to the general public.

As such, there is *Need for better dissemination of information related to flash flood event to authorities and to general population.*

47) Need for full exploitation of aerial means and Earth Observation during the response phase of a flood event and their incorporation in real time situational awareness systems. 4.CGF.12

Use of **aerial means (*i.e.* drones)** to get pictures of the **situation** (closed roads, bridges, victims ...)

Need for **satellite images** in real time. Update/refresh images)

Need for a **better monitoring of the flood with ground sensors** to keep track of the progress of the event
It was confirmed that there is *Need for full exploitation of aerial means and satellite images during the response phase of a flood event and their incorporation in real time situational awareness systems.*

48) Need for an automatically real time situational awareness and decision support system 4.CGF.13

Need for efficient **information tool** and a **data sharing** system between authorities.

Need for an **algorithm to select reliable information from Social Media** (improve VOST).

Need to issue **guidelines on how to process information** from different sources e.g. civilians to first responders.

Exploitation of EUCPM (EU civil protection mechanism) Experts for assessments.

Therefore, there is *Need for an automatically real time situational awareness and decision support systems*

49) Need for robust & resilient communications means in case of natural hazards 4.CGF.14

Need for specific guidelines for **robust and resilient communication network.**

Need for a pan-European communication system, independent of private companies, **dedicated lines to emergency situation**.

To summarise the above, there is *Need for robust & resilient communications means in case of natural hazards*

50) Need for efficient and specific rescue means in case of flash floods 4.CGF.15

Specific training for first responders and crisis management for flash flood and how to respond to small scale events.

Need for **efficient aerial and ground-based evacuation means.**

Need to **enlarge EU RescEU** system to also include others rescue means, such as helicopters.

Thus, there is *Need for efficient and specific rescue means in case of flash flood*

51) Need for efficient and specific rescue plans in case of flash floods 4.CGF.16

Need for **generalized and detailed plans** in case of flash flood in every flash flood prone areas.

Need for **guidelines and methodology** to create plans: lack of comprehensive, effective, and up to date operational plans/ guidelines.

Need for efficient and specific rescue plans in case of flash flood.

52) Need for improving awareness of population toward natural hazards alerts 4.CGF.17

Need for development of **reverse 112** system in Europe.

Need for **local population training & information** on how to react in case of natural hazards: how to behave, what measures to take (*e.g.* leave the house, move to a higher ground *etc*.)

Need for **suitable alerts** on different means issued simultaneously: real tools for better efficiency.

Better **prewarning time** for evacuation orders and other measures to be taken (see CGF2, depends on forecasting)

Need for **region (local) specific alerts** with instructions about what to react

Need to **filter social media outputs** for alerting the population with reliable information

As such, there is *Need for improving awareness of population toward natural hazards alerts*

53) Need for solutions to efficiently archive past flood events (both for prevention and preparedness) in a standardised format and make them accessible to practitioners 4.CGF.18

Need to have **reliable post-event information** on the affected population, impacts on assets (industry, structures, CI, environment *etc.*). Lack of a **dedicated entity** that would perform and an automatic retrospective.

Need to **keep track** on the correlation between rainfall and flooding: where when and what happened. Need for a **coherent picture of the flood event** (conditions under which it took place, details on what happened and when, impact assessment)

Need to establish a **methodology to efficiently exploit lesson learned** from past events at all levels

It is important thus, to underline that there is *Need for solutions to efficiently archive past flood events (both for prevention and preparedness) in a standardized format and make them accessible to practitioners.*

54) Need for standardised information sharing among all stakeholders engaged in response to flash flood events 4.CGF.19

Need for a **standard on how entities should exchange relevant data** (both during and after the event)

Need for **standardized information sharing in a structured, holistic and integrated** way with all actors involved in prevention & preparedness: authorities, hydrological specialists, multidisciplinary experts, urban engineers, civil protection.

Need for solutions to efficiently archive past flood events (both for prevention and preparedness) in a standardized format and make them accessible to practitioners.

55) Need for a solid approach to efficiently exploit lessons learnt from past floods 4.CGF.20

Need for a **better knowledge of vulnerability/exposure** of the territory: definition and prioritization of flash flood prone areas.

Need for **policy integrating risk prevention** and actions to be taken.

Need to **identify appropriate (case-specific) mixture of approaches** for flood mitigation, combining structural and non-structural (mostly nature-based) solutions.

Need for a solid approach to efficiently exploit lessons learnt for past floods.