Position paper on the results of CERIS CBRN session 4th May, 2022, Lille, France

Introduction

The Community for European Research and Innovation for Security (CERIS) organised a CBRN session on May 4, 2022 at the CBRNe Research & Innovation conference in Lille, France. The session opened with state-of-the-art presentations by representatives of DG HOME, DG ECHO and FPI, and continued with two panel discussions of thirteen current EU-funded CBRN projects - eNOTICE, INCLUDING, NO-FEAR, FIRE-IN, PROACTIVE, HoloZcan, ECCOFEX, RESIST, VERTIgO, JA TERROR, Bullseye, EU-RADION and PANDEM-2.

The range of questions addressed at the panel discussions:

- stakeholders engagement in CBRN preparedness (including general public)
- gaps in preparedness
- multidisciplinary, multi-agency and civil-military cooperation, joint CBRN exercises
- innovative CBRN technological solutions for CBRN agents detection, PPE, decontamination, testing and validation
- acceptable risk or zero risk - what is the goal of standardisation?
- better use of European research outcomes,
- dissemination of results of EU projects.

Key points, take-away messages and recommendations on CBRN R&D&I

1. Further **synergies and true collaboration** between complementary projects are needed to amplify the results and ensure uptake. All groups of CBRN stakeholders - policy makers, researchers, civilian and military practitioners, industry representatives, citizens and civil society organisations have to be actively involved and share the knowledge and experience. But proper mechanisms for this exchange have to be explored and put in place.
   The main gap is that neither all first responders, nor Critical Infrastructure Operators are trained for CBRN response (as often this training is provided only to "specialized teams", and not even for recognition of a CBRN threat. In the current situation and all well-known war events in Europe, the CBRN risks become even more real than before. Before, CBRN was perceived as a “low probability-high impact” event. In the context of the recent events and new challenges, the probability might be getting higher, and preparedness and training for first responders, but also awareness for population becomes significant. It is high time to strengthen the R&D&I efforts, common interagency SOPs development, training and preparedness for first responders, crisis managers and population to adequately respond to CBRN threats. It is strongly recommended to reinforce the funding opportunities in all relevant programs, such as Horizon Europe, ISF, EDF, DG SANTE to encourage further works in CBRN field, and not to decrease the budget in order to avoid creation of capability gaps. Professional networks, networks of practitioners are a good instrument building the

communities where members can turn to each other when there is a problem at hand that needs urgent solution, or at least professional advice.

The past events, such as terror attacks and emerging challenges prove that immediate (e.g. critical infrastructure operators, citizens), first, second and third-line responders need to be trained or at least aware about how to recognise or to identify CBRN threats, as well as properly mitigate/respond to them and deal with the consequences. There is still a problem that stakeholders are not tightly linked, different disciplines do not work much together even within the same country, whereas preparedness at the EU level remains an even wider gap. This requires an increase in cooperation between organizations, cross-border and international cooperation, including the creation of SOPs. Some projects such as ISF project MELODY are taking steps in the direction of defining harmonised procedures in preparedness and response. More multidisciplinary and multiagency contingency planning, trainings and exercises, like the ones undertaken by the RESIST project, are necessary to train interoperability between different institutions, including learning to communicate between each other, aligning terminology, concepts used by different (public and private) actors to describe the crisis situation.

The necessity of comprehensive approach to preparedness and training has been underlined by several projects (eNOTICE, NO-FEAR, FIRE-IN, PROACTIVE, RESIST, JA TERROR, INCLUDING, Bullseye, ECCOFEX..), in particular from the following aspects:

- **Versatile scenarios**, including combined C, B, R threats of accidental or deliberate nature, hybrid threats and emerging threats; with testing and validating innovative technologies at different stages of development. Moreover, there is a need for reference scenarios from the EC with regard to "what are we preparing for", with formulation of clear objectives of the preparedness (e.g. are EMT 2 with C-RN capacities expected? Prediction of industry chemical substances for terrorist attack? etc.)
- The necessity to train CBRN stakeholders that might facilitate the management of the first moment of a CBRN incident against **critical infrastructures**. E.g. RESIST project is looking into training of Critical Infrastructures operators, considered as "immediate" responders, for their ability to react properly, safely respond to a threat, be aware of a threat, recognize how the threat is linked to CBRN, and forward precise and useful information to specialised first responders who will be responsible for managing the CBRN scene. The critical infrastructures covered are mainly related to transportation ways and critical hubs - roads, railways, airports, seaports, space stations, and nuclear research centres.
- Collaboration of various actors, including the "traditional" ones – like first, second, third-line CBRN responders and crisis managers, but also stakeholders from cross-sectorial fields such as health care, justice, civil protection - to ensure a truly **multidisciplinary approach** covering all possible actors that might be involved in a crisis response. This can be achieved via networks of networks emerging from current RIAs and CSAs.

Engagement of citizens in CBRN response and communication to public during CBRN crises are considered a top challenge and are currently studied by project PROACTIVE. The problem is addressed from both angles – on one hand, it is necessary to familiarize the citizens with the response procedures, to involve them in trainings and exercises, to explain what to expect and what to be prepared for in case of a crisis, so that they can protect themselves and others. On the other hand, first responders and crisis management experts need to learn to deal with the population (including

vulnerable groups) in the most efficient and ethical way, doing all the necessary procedures and at the same time providing the clear information and instructions, reassuring, encouraging and helping the people in the crisis situation. Effective and inclusive communication with the public and patients remains a critical gap. H2020 projects PROACTIVE and eNOTICE are pioneers in the field of engaging real volunteers and vulnerable citizens from the general population in the exercises with first responders in CBRN training centres.
FIRE-IN project also looks into improvement of population resilience, and puts forward the development of public self-protection and awareness, education of people, necessity to negotiate the values with communities before the emergency, cultural change towards risk tolerance and resilience, standards for communication with citizens, unified system of warning citizens in the EU, common understanding of such communication, guidelines for citizens.

Civil-military cooperation in CBRN field is indispensable to share the knowledge, experience and train civilian and military actors together (the approach followed by eNOTICE and Bullseye projects that have civilian and military partners in the consortia), with better structured interaction between civilian and military actors with clearly defined and equally distributed roles and responsibilities. A unique system of data collection and verification shall be used. The fact that CBRN technology is often considered "dual use technology" is a challenge both in research but also in real cross-border cooperation.

Cross-border exercises are very important with the focus on standardised approach in cross-border training to comply with procedures and standards of neighbouring countries, on legal, administrative and organisational aspects including language and communication barriers, that would lead to identification, harmonisation and proper addressing the capability gaps in the EU.
It is necessary to define SOPs in case of interagency cooperation, cooperation between individual emergency services, cross-border and international assistance.

2. CERIS is considered an excellent environment to exchange information, to raise awareness and share results in the R&D&I projects. Face-to-face meetings, as well as online meetings when necessary, help to know who is doing what, build on each-other's results, build synergies with collaborative project events or joint demonstrations and create new consortia. But besides that, this exchange of information should not happen only within CERIS. Projects and their results need to be known and taken up by Member States, at least by the countries whose partners participate in these projects, the importance of it was underlined by technology development projects, such as EU-RADION, PANDEM-2, VERTIgO, HoloZcan. So far, it has been discovered that Member States seldom know the results of EU projects. Dissemination efforts have to be directed to spreading the knowledge not only to the EU actors, but also locally, at the national levels, that would increase the chance of the generated results to be further developed and reach the market. Ideally, a common repository of all Key Ministries and Agencies addresses should be compiled to benefit all CERIS-related projects. Ensuring vertical dissemination, between R&D&I authorities, and response authorities is essential.

3. The **technology developed by R&D&I projects must reach the EU market**. The majority of projects finish the EU funding at the TRL levels 6 or 7, only large demonstration projects show integrated solutions of up to TRL 8-9. Since the Commission does not have a possibility to support projects after their end, it is desirable that corresponding Member States uptake the results and create the

appropriate environment for the technology further development and finalisation to be ready for commercialisation. An example can be taken exactly from the CBRNe conference in Lille, where French Ministry of Defence, [Agence Innovation Défense - www.defense.gouv.fr/aid] and [DGA - GINCO NRNC – dga-mnrbc.ginco.fct@intradefgouv.fr] were represented while both are offering technological incubation. Such initiatives and programs are promising solutions for French entrepreneurs. Ideally, a similar listing of all EU Member States initiatives could be identified.
The EU network of practitioners project eNOTICE - network of CBRN Training Centres - works a lot with practitioners of all disciplines and collaborates with industry as the industry is seen as one of the main contributors and beneficiaries of the network. Participation of industry starts from practical operational aspects, such as testing their tools/technologies/equipment with practitioners at training centres, in order to be sure that their development meets the needs of users. It is clear that development of new tools, e.g. CBRN detection tools or early warning tools and all other tools and technologies developed by researchers, need validation. In the case of low TRL (4-6) detection and identification methods the statistical study design behind the testing and validation procedures is a challenge, so the relevant IEC/ISO standards cannot always be applied. Therefore, specific testing and validation protocols must be developed according to the specific use cases and scenarios. This enables the finalization of development towards a cost-effective manufacturing technology. The developed detection technologies must be usable even in the specific conditions at the place of intervention. They must offer clear detection outputs that will allow the intervention commander on scene to make correct informed decisions.

Training centres often test new equipment. The most suitable tools are used for trainings. So new technology is a crucial part of trainings. Sometimes first responders who train in a certain TC bring their own equipment because they want to be trained for their everyday work. How are we able to integrate innovation and make it attractive for end-users, for TCs? How can we show benefits of new technology to the people on the ground, how they are going to use it? Will it be possible for TCs to choose what technologies they want to test? How shall we balance the technology push and the needs of practitioners to have certain types of technologies? What they would like to have, but do not have yet - PPE? Early warning systems? (Smart) sensors? Portable systems? Robots? Software? ICT tools to collect data and support decision making process? What kind of technologies could be interesting for practitioners right now, at this moment? How can new technology, tools, and equipment be more inclusive and more adapted to the needs of the vulnerable groups? CBRN practitioners often do not know what technology and what innovations are available, and how they can benefit from it. For example, rapidly developing AI technology – what capabilities can it give to first responders, to crisis management actors? What users can do with it in their everyday activities, how can it help them? What new materials are used and what is improved innovative design of PPE? How will the technology be perceived by the public? (PROACTIVE research results can support this point). Users often lack such information, while technology developers also lack information about the users' needs and very often don't know how to approach users for technology testing in the field. It is necessary to ensure regular communication and efficient collaboration between practitioners and technology developers, and the eNOTICE network of training centres is seen exactly as the cradle facilitating the dialogue in such a crucial domain as CBRN where design of technology exactly corresponding to the user's requirements and expectations is particularly significant and even life-saving. For this reason, the growth of new training and testing centres like the Calvarina base, managed by SAFE, is a fundamental asset to sustain the eNOTICE approach and its sustainability in

the long term ensuring an increasing impact for the benefit of the overall community of EU stakeholders.

The eNOTICE network promotes collaboration with industry and research offering grounds for testing and validation of technologies. However, companies face a number of challenges when testing technologies in the field. These challenges are broken down in the following groups, some of them generic, others more specific:

Laws and Norms

- National and international laws/agreements often prescribe export restriction rules to cross-countries movements of materials and technical information related (mostly military but also some civilian, plus dual use can be tricky and in case of doubts normally the stricter rule applies)
- Norms are not globally standardised (differences between EU, UK, North America, etc.) which makes it difficult to reach global validation of products. Developers try to use as reference civil and/or military standardised norms and test protocols if possible (ISO, EN, BS, NFPA, ASTM, STANAG, etc.)

Logistics

- The complete value chain of the process to test CBRN equipment or tools is almost never in a single site location, this means material and information need to travel between different places, often cross-countries (test labs, field test facilities, industries, etc.)
- International export control regulations and customs procedures make it sometimes difficult and costly to transport equipment and materials from/into countries, which is especially challenging when the exercise/training takes place outside the EU, or when a technology provider from outside the EU is bringing technologies in the EU. CBRN equipment, being "dual use" by nature is often under specific import/export regulations, which could pose issues in cross border cooperation (in training and / or operation).

Time

- It usually takes time for companies to obtain authorisation for export/import of materials and information,
- Product/tool/process design and re-design according to the feedback of end-users after the exercise
- Manufacture of the end products,
- Testing of developed technologies is not limited to one exercise, the complete full set of testing and validation is a long process

Costs

- Production for testing is expensive and is a pure investment (because no sales take place), it's especially difficult for small SMEs that do not have lots of resources.
- Legal and technical expertise
- Transports (material needs to travel across the world)
- Tests can be very expensive esp. full system testing. Sometimes, for full systems testing starting from scratch, for all tests, the costs can be up to 100.000 euros or more, just for the testing. For specific tests, e.g. in simulant chambers, several specific tests can be performed,

that might be around 10 – 20k per test depending on where the test takes place, how many garments are tested). Validation of full systems can take up to 2 years
- Accidental damage of equipment in the field, that requires extra expenses for insurance
- The use of Virtual Reality can reduce the costs for training implementation, which are very high especially when considering CBRN practical courses. With this regard, the experience gained from the EDIDP-funded project VERTIgO will be essential for other (also non-defence oriented) initiatives as well

Expertise availability

- CBRN is a "small world" but experts are not around the corner, it's difficult to find appropriate profiles to work with
- Cooperation amongst full process stakeholders (Industry, Users, Govt. Institutions, Experts, Research Institutions). There are not many networks existing, eNOTICE is a good example, but then again there is a lack of "full-cycle" networks that would involve all relevant stakeholders
- Different stakeholders' cooperation is possible but inside national laws
- Not many places where cooperation is promoted globally
- Lack of harmonisation in the method of work
- The companies must fully comply with practitioners' procedures and standards, e.g. the procedures of CBRN samples delivery are very strict
- More cooperation between civil and military actors can facilitate the identification of suitable expertise and the exchange of relevant good practices and lessons learned.

Sharing results

- Sometimes not possible because restricted (mostly MIL)
- Not only norms are not harmonised but also performance levels accepted as valid by different countries/institutions/experts thus difficult to share and agree on results
- IPR issues - non-disclosure agreements have to be concluded with the participating practitioners to protect the company's IPR
- Interoperable data management plan between projects with similar TRL could promote the sharing of results and raw data as well

Technical challenges

- As seemingly simple a problem as lack of power supply in the field can be and obstacle when the equipment cannot be plugged to a socket. This is usually easy solve, it just needs preparation in advance.

- Internet / Wi-Fi connection – same thing, it has to be negotiated and provided in advance, otherwise CBRN sensors, software, etc. cannot function without reliable connection in the field. Cybersecurity issues must be also taken into account.

- Cross-border communication and language might be a problem if the hosting TC training professionals or practitioners do not speak English. But usually it is possible to find at least 1-2 persons who can assist through the exercise/tests to brief about the objectives, goals, procedures, and translate when needed.

- The definition of calibration process related to several sub-components of the complex, integrated measurement devices is also a challenge. To overcome this problem, we must design and execute strictly separated calibration protocols to test the performance of the sensor system and the integrated sub-components which support real time operation and have crucial impact on the detection

- The biggest challenge is calibration of equipment in the field, because every time depending on the location it will be different. One other challenge besides the issue of spatial properties is the temporal variability of samples in bio-detection systems. Developers must pay attention to seasonal data collection to build the appropriate databases as reference for the final calibration and software support.

- The conditions in the field are of course different from the "sterile" lab conditions, so companies must apply rigid quality assurance and quality control procedures to comply with the standards and ensure the data quality, in field conditions where background noise is usually very high. The combination of appropriate QA/QC procedures together with skilled personnel results in valid and more useful field data.

- Some specific technical challenges related to particular technologies testing can occur, such as using a robot or a drone in unknown environment; weather conditions in the field might be difficult to use drones or sensors; necessity of spare parts for electronics that might break down; problems of hardware interfacing, etc.

- The use of VR can facilitate the delivery of multi-agencies and multi-countries joint training sessions, allowing multiple users practicing together on the same scenario at the same time. With this regard, results from VERTIgO project aims at supporting the creation of the first European Exercises Simulation Platform (EESP).

Favourable environment for exchanges and regular communication between technology suppliers and users are key to understand each-others' needs and limitations, and to achieve best results beneficial for all. Many projects are working on new detection technologies. New technologies require mutual understanding between the industry, developers, trainers, implementers and users. Creating "mutual understanding" requires efforts and identification of the respective partner who has the interest / capacity.

It is essential to define the R&D priorities, so that the users clearly express what technology/tools/equipment they need most, and that technology suppliers know what to work on. For example, NO FEAR project reminded that the first responders in a CBRN release in a public site are not protected, and in many cases they are not "blue lights" but rather operators of critical infrastructure or private contractors. There is need to develop tools for those first responders (as the 5 R – Recognize, Remember, Report (using M/ETHANE), Respond, Remove).

4. The issues of **standardisation** in CBRN require further effort and clear policy in:
   - aligning the terminology - same terms can mean different contents for different stakeholders, depending on the field of use or on the country;
   - definition of zero risk or acceptable risk in CBRN incidents response and aftermath - as long as toxicity thresholds for CBRN agents are not defined and not commonly agreed (for long term exposure of "regular citizens" – post decontamination), it creates a problem to determine

detection thresholds and decontamination requirements. In the same line – military units and public safety organisations have different standards for PPE protection of responders (e.g. Fully encapsulated suits with a self-contained breathing apparatus, or a mask with a canister and a light garment), to a civilian incident. This gap comes from different perception of risk – zero risk or acceptable risk to responders in a CBRN incident, and causes issues of trust among those involved in the response as well as with the public;

- harmonisation of procedures can be a long intermediate step towards standardisation and is currently considered by projects PROACTIVE, Bullseye, FIRE-IN, JA TERROR.