



### Summary statement

- The frequency of occurrence of CBRNe threats is set to increase in the coming years, with incidents such as the Salisbury Novichok poisoning providing an illustrative example of the challenges associated with recovering from and/or decontaminating the scenes of such incidents. These threats' cross-border impact (whether as a result of contaminants spreading or as a result of negative externalities placing pressure on neighbouring states) necessitates a robust response on the part of the public sector.
- Civil-military cooperation can provide many benefits to affected stakeholders. Not only does such cooperation increase civil-sector practitioners' ability to procure advanced equipment, it also facilitates knowledge sharing vis-à-vis operating procedures and best practices between the two sectors, and thus has the potential of improving a system's overall capacity to respond to CBRNe incidents.
- Civil-military cooperation's benefits from a practitioner procurement perspective derive from its ability to a.) provide industry with the economies of scale which are necessary to improve the affordability of advanced solutions, and b.) educate practitioners on the use of advanced solutions. Barriers to civil-military cooperation in procurement derive from various factors, the most relevant of which is the military sector's comparatively advanced degree of competence when it comes to dealing with CBRNe-related incidents. In addition, based on increased civil-military cooperation in the domain of CBRNe, research and development benefits as well.
- Institutionalised cooperation constitutes a best practice when it comes to fostering seamless civil-military cooperation (whether within procurement or otherwise). Such cooperation can be achieved by (among others) enshrining shared competencies vis-à-vis response to CBRNe incidents in law, or by mandating the use of shared facilities for sample analysis.
- The market for CBRNe-related projects remains relatively small, with many projects being limited by the fact that preceding projects and/or currently procured systems are built around the notion of vertical (rather than horizontal) integration. This significantly increases (from the military and/or civilian practitioner) perspective of procuring new systems, and contributes to a general lack of uptake of R&D results. This phenomenon can be addressed by (among others) standardizing elements of the EU procurement process and by financially supporting practitioner organisations as they switch to systems which incorporate 'interoperability by design'.

## Introduction

This CoU brief summarises the topic of civil-military cooperation in the field of CBRN-E and relevant EU-funded projects that participated in the 12th Meeting of the Community of Users (CoU) on Secure, Safe and Resilient Societies that took place 3-4 December 2018 at the BAO convention centre in Brussels.

The Community of Users is a DG Home initiative that aims to improve information transfer of research outputs and their usability by different categories of stakeholders. During the meetings and thematic workshops, policy updates and information about H2020 projects are provided and interactive discussions are facilitated to ensure that solutions and tools resulting from research will reach users.

## Scope & Relevance

Civil-military cooperation (CIMIC) refers to cooperation between civilian and military sectors of governments. Cooperation between these sectors may take place in a range of theatres, including within the operational (logistical and/or 'on the ground'), R&D and procurement domains. Within the context of counteracting and/or mitigating the threat of CBRNe related threats, CIMIC is of vital importance not only because the frequency with which threats falling within this category are likely to present is set to increase in the upcoming years, but because – even if this were not the case – the civilian and military sectors can often share information and/or operating procedures with one-another that allow both sides to improve their efficiency. CIMIC within the procurement cycle further reduces redundancies (civil and military stakeholders often have similar needs, but initiate and/or are engaged in parallel procurement processes), thus increasing the cost effectiveness of

both services. It also facilitates the process of procuring high quality and/or sophisticated hardware, as the technical know-how and/or use case that these two stakeholder categories can introduce to one-another has the potential of resulting in more focused, more utile, and more technologically advanced project outputs.

Perhaps most importantly, effective CIMIC within the field of CBRNe has the potential of significantly improving the sustainability of EU research projects, and (by extension) of improving the ROIs of associated EU-funding. This is because communication and/or joined procurement initiatives which may derive from effective CIMIC effectively increase the market for project outputs by linking stakeholders involved in research and production (read: supply side) to consumer (read: demand side).

## Current debates & stakeholder perspectives

This section describes why the topic is particularly important for each stakeholder group.

### Practitioners

From a practitioner perspective, CIMIC within the field of CBRNe can be associated with several benefits. First and foremost, CIMIC has the potential to contributing to practitioners' ability to procure technologically advanced systems. This is because supplementing civil know-how and/or capability requirements with military know-how and/or capability requirements within the procurement cycle increases (from the industry perspective) the potential market size for products which are geared towards meeting these shared requirements, and provides access to economies of (relative) scale. This (in turn) incentivises industry investments into R&D, and may push the price of final solutions down, thus facilitating practitioner procurement of systems which – because they are developed for a broader (more demanding) market – are objectively superior to solutions which are procured in the absence of effective CIMIC. Operational CIMIC can also be a boon for practitioner organisations, as the sharing of operating procedures (read: knowledge transfer) can improve the effectiveness of both sides.

CIMIC between practitioner organisations – both within the operational and procurement spheres – tends to be uneven. Civil and military organisations frequently fail to agree on common technical requirements during procurement (likely because these factions are working towards addressing different capability gaps), and typically do not share common operating procedures. The degree to which cooperation between civil society and the military (in the domain of CBRNe) has developed differs between Member States; whereas in some countries this cooperation is still in a conceptual phase, in other the collaboration has been formalised already.

### Industry & SMEs

Industry and SMEs have an important role to play in facilitating CIMIC. Members of this stakeholder group are intimately involved in executing the procurement process, both within and outside the context of EU-funded research. Industry and SMEs stand to benefit from the project sustainability that derives from CIMIC (this facilitates linear commercialisation), as well as from the economies of scale which it can be associated with.

### Policy

Stakeholders within the policymaking category preside over several tools which can serve to alleviate challenges associated effective CIMIC in within the field of CBRNe. First and foremost – in allocating research budgets and in defining the parameters of procurement contract – policymakers can leverage pre-commercial procurement processes (PCP) to ensure that practitioners within both civilian and military services are consulted during the procurement process. This achieves the twin objectives of a.) ensuring that policymakers have enough information to judge whether or not tendered proposals adhere to the principle of 'interoperability by design' (this can be achieved by allocating resources towards research into these stakeholders' capability gaps, etc.), and b.) ensuring that bids are awarded to contractors accordingly. Outside of this, policymakers can foster an increased level of 'working trust' between civil and military-sector practitioners by enshrining their cooperation in issues relating to CBRNe in national law and/or in operational procedures. A topical example presented at the 12th CoU presented in the Belgian response to CBRNe threats, which involves a combination of civil-and-military practitioner units and/or institutions, and thus 'normalizes' relations between the aforementioned stakeholder groups.

At the EU level, stakeholders involved in facilitating CIMIC include DG HOME, DG DEVCO, DG GROW, DG SANTE, DG CONNECT, DG ECHO, the European Defence Agency (EDA), and the European Space Agency (ESA). The North Atlantic Treaty Alliance (NATO) is also of relevance. Of special note within the field of CBRNe is DG DEVCO's CBRN Centres of Expertise programme, which is geared – given the (oftentimes) cross-border nature of CBRNe incidents – towards protecting the EU from such events by bolstering the capabilities of countries within its neighbourhood.

Several policy initiatives and/or agencies relating to improving CIMIC within the field of CBRNe were discussed during the 12th CoU event on Secure, Safe and Resilient Societies that took place 3-4 December 2018 at the BAO convention centre in Brussels; namely:

- **EDF.** The European Defence Fund (EDF) is one of several initiatives of the EU's defence policy alongside CARD and PESCO. With the EDF, the European Commission (EC) aims to foster the competitiveness and innovation capacity of the European defence industry by financing collaborative research and development actions and cross-border cooperation. The need for the fund is driven by the increasing costs of for military R&D, especially given the high degree of fragmentation between EU Member States. The EDF in the current EU long-term budget hosts two initiatives; namely: The Preparatory Action of Defence Research (PADR) and the European Defence Industrial Development Programme (EDIDP) and in the next long-term budget will be one single programme of 13 billion euro. Funding is geared towards supporting projects over the whole life-cycle of a defence product: from the research to the development. The fund incentivises cross-border participation of SMEs, and allocated funding on the basis of an overview of MSs shared capability gaps, including within – where relevant – the civilian sector.
- **The Union Civil Protection Mechanism.** The Union Civil Protection Mechanism (UCPM) is a framework which covers prevention, preparedness, and response that has been in place since 2001. One of the UCPM's clearest contribution to CIMIC presents in the European Response Coordination Center (ERCC), which monitors disasters around the globe and coordinates EU

responses to them by connecting EU MS agencies 24/7. When a disaster occurs, the organisation can deliver assistance in the form of expertise and funding. Because countries 'volunteer' services to the UCPM, the UCPM can actively decide to structure deployments in such a way the CIMIC is furthered. The ERCC was mobilized a total 32 times in 2017. Expertise is provided by the EU-28 Member States, as well as Iceland, Montenegro, Norway, Serbia, the former Yugoslav Republic of Macedonia (FYROM), and Turkey, all of which committed themselves in 2015 to registering specific assets for use by the ERCC's Civil Protection Modules. Because data is often scarce when it is most valuable, the ERCC also asks Member States to share information in a relevant, reliable, timely, and simple matter. The ERCC's Analytical Sector collects data from early warning systems, ECHO field, ECHO partners, EU Del, Media, and Satellite Imagery and aggregates them to map capacity and plan to responses.

- **JCBRN Defence Centre of Excellence (NATO).** The JCBRND CoE is one of over 24 NATO centres of excellence. NATO centres of excellence were introduced after the end of the Cold War, when defence budgets started to shrink but the alliance wanted to maintain the know-how and/or expertise that derived from the allocation of regional and/or niche roles within the alliance. The JCBRND CoE focuses on issues relating to CBRNe. In concrete terms, it provides advice on all CBRNe related areas, helps to develop doctrines and/or standards for dealing with threats falling within the CBRNe category, and enhances defence against such threats through the provision of training and through the dissemination of lessons learnt. The centre is of particular relevance because – as part of its work on doctrines – it develops strategies to engage and/or involve civilian-sector practitioners within the country-CBRNe process.

## Research

Stakeholders within the research category play (as outlined in previous paragraphs) an important role in informing the decisions of policymakers as they relate to the procurement cycles that service actors involved in CIMIC.

## Relevant projects & project hubs

Activities conducted as part of the following projects and/or organisations were outlined during the 12th CoU meeting:

- **eNOTICE.** (September 2017 – August 2022; ongoing). The eNOTICE project sets up an operational transactional network for optimising investments by pooling and sharing resources, expertise, and effective practices. The eNOTICE consortium includes both civilian and military CBRN TC. By organising joint activities (including those which are of relevance for CIMIC) between the eNOTICE network members and external partners,

and by liaising with other networks of CBRNe stakeholders establishes a European network of CBRNe TC, testing and demonstration sites has been established. Part of the project is a web-based information and communication platform, which allows sharing and dissemination of information during and after the project. It helps to make the eNOTICE network visible and attractive to CBRNe-TC and external stakeholders, to provide access to CBRNe-TC capacities according to a 'capacity label', and to encourage and facilitate communication and interactions between all parties.

- **GIFT-CBRN** (September 2014 – August 2017; closed). The GIFT CBRN project aimed to address gaps in forensic investigation protocols and training that have hampered the successful interrogation of evidence, either at a crime scene contaminated with CBRNe agents, or of the agents themselves back at the lab. Through the cooperation of Europe-wide CBRNe research agencies, first responders, industrialists and subject matter experts, the project set out to further develop the investigative and analytical methods that were previously (until this project) only used in a secure laboratory environment and instead enabling them to be used at the scene of the crime. The latter objective requires not only that delicate equipment can be transported to a remote location, but that it is also capable of withstanding the problems of a harsh CBRNe environment; such as decontamination.<sup>1</sup> The overall objective of the GIFT toolbox is to facilitate the timely sharing of critical data for processing with the appropriate entities, while ensuring that the appropriate chain of custody is maintained.<sup>2</sup> To test the usability of the procedures and methods of the CBRNe forensics toolbox developed in the project, a series of three exercises (field tests) were developed and implemented, each dealing with one agent at a time.
- **TOXI-TRIAGE** (September 2015 – August 2019; ongoing). The TOXI-TRIAGE project aims to meet the needs of casualties and end-users in CBRNe incidents and has developed ACCIMAPs for CBRNe specialist actions, which will be tested in the next 12 months. The seven specific objectives that the TOXI-triage project addresses are the operational; technological; ethical and societal dimensions of CBRNe response and recovery, and importantly the economic base from which sustainable CBRNe and multi-use systems are derived. The project features deliverables geared towards the rapid non-invasive assessment of exposure/ injury through monitoring metabolic markers of injury; managing and exploiting the semantic web; traceability by design; aptamer-based bio-sensing; casualty-to-discharge system integration; and integrated environmental and stand-off hazard designation. BFREE. The aim of the BFREE project, funded by the EDA JIP-CBRN programme, was to develop an efficient method for processing mixed CBRNe samples. The project's most concrete output takes the form of a novel method for removing biological contaminants from mixed CBRNe samples. Being funded by the EDA, the project is geared primarily towards servicing stakeholders from within the defence sector. This notwithstanding, the project's outputs were published in a scientific journal, and are of likely relevance to civilian practitioner organisations.
- **RACED** (December 2011 – November 2014; closed). The RACED project is funded through the EDA JIP-CBRN programme, and is geared towards assessing military decontamination procedures, and to advising various stakeholder groups on issues relating to the question "how clean is clean enough?". The project's concrete outputs present in the form of a risk management tool for assisting operational decision making, based on the previously identified decontamination procedures and/or the political and/or institutional level of ambition when it comes to decontamination. The RACED project is primarily geared towards servicing the military, but many of the project's findings – especially because CBRNe threats (see for example the recent Salisbury poisoning) may present in civilian environments – can be transposed to the civilian sector.
- **ENCIRCLE** (March 2017 – March 2021; ongoing). The ENCIRCLE project is an example of a project following the new strategy within the EU for CBRNe which is not aimed at producing science but at facilitating the delivery of innovations suitable for practitioners and the market. The ENCIRCLE consortium is strengthening the European industry by helping to create the tools and strategies needed to consolidate the EU CBRN communities of suppliers and practitioners in order to strengthen the field of CBRN safety, security and defence in the European Union. This includes consultation with EU CBRNe communities of suppliers and practitioners through workshops and surveys which are targeted towards gauging stakeholders motivation and views concerning the CBRNe defence and civil security markets. The project provides tangible insights into the potential added value of CIMIC from a market and/or (by extension) a security perspective.

## Possible synergies (and links to policies and practitioners' operations)

Within the field of CIMIC, there are clear (operational) synergies between research outputs, practitioner needs, policymaker initiatives, and industry activities. Initiatives such as the International Forum to Advance First Responder Innovation (IFAFRI) – currently chaired by the European Commission's DG HOME – show clearly how research activities can bridge the gap between practitioner needs, limited policymaker knowledge, and industry activities, thus leading to common interoperable solutions.

Embedding research into a wider capability development process can also contribute to better streamlining the common needs of EU security practitioners and to developing innovative solutions which not only are interoperable by design, but which are also triggered by policy priorities, respond to critical and urgent operational needs, and show an adequate balance between cost and effectiveness.

<sup>1</sup> GIFT-CBRN Project website, available: <https://giftforensics.eu/>.

<sup>2</sup> Ed van Zalen, "GIFT, the European CBRN forensics approach," CBRN Forensics Magazine - Issue 2, Falcon Communications Limited: United Kingdom, p. 9.

<sup>3</sup> ENCIRCLE Project website available: <http://encircle-cbrn.eu/>.

For an overview of information exchange and interoperability-related projects funded under the Horizon 2020 framework prior to 2016, see sections 5 (CBRNE threats) and 9 (Horizontal issues) of **DG HOME, “Community of Users on Secure, Safe and Resilient Societies – Mapping Horizon 2020 and EU-funded Capacity-Building Projects under 2014-2017 Programmes,” Working Paper (Brussels: European Commission, forthcoming).**

The projects referenced within this section of the aforementioned document are universally geared towards tackling similar subjects as those discussed in this brief, and thus have the potential of exhibiting synergies with them.

## Lessons learnt and challenges

Despite the clear advantages associated with achieving a higher level of CIMIL, several factors currently impede progress. The first is an asymmetrical level of competency between military and civilian stakeholders when it comes to CBRNe. CBRNe tends to be an area where the military sometimes has a higher level of competency than the civilian side does, with the result being that stakeholders within the military have little to no incentive to actively cooperate with the civilian sector when it comes to the procurement process. The second is that the EU's current procurement strategy – outside of not considering CIMIL as a factor which needs to be actively pursued – oftentimes fails to ensure a vertical approach to integrating research outcomes are adopted by practitioners. This problem is exacerbated by these projects' typical funding structure: industry stakeholders are often expected to pay a large share of their R&D costs through their

own overhead, and are subsequently faced with the prospects of having developed a technology for which there is no clearly defined market. Combined with the fact that civilian-sector practitioners often tend towards procuring modified (rather than freshly developed) versions of pre-existing solutions – largely as a cost-cutting mechanism – this constitutes something of a vicious circle in which lack of demand on the part of practitioner organisations results in unwillingness to invest in R&D on the part of industry.

Another observation relates to standards. Standards are widely used in the military domain whereas civil security standards are less integrated at EU level. Thus, it is likely that integration of civil and military cooperation is more easily accepted by the military domain than by civil society.

## Way forward

The experiences shared by project represented at the 12th CoU event indicate that several courses of action constitute viable ways forward when it comes to improving CIMIC within Europe. First and foremost, asymmetry in competencies vis-à-vis CBRNe – a structural variable which 'blanket' disincentivises cooperation – can be addressed by policymakers' integration of the military within CBRNe-related operating procedures. A topical case presents in Belgium, which actively involves several branches of the military – notably the military crime lab and the military forensics team – in government response to CBRNe incidents. Institutionalised cooperation facilitates the development of more all-encompassing CIMIC, and (in the process) contributes to the formation of relationships which are conducive to engagement in shared procurement initiatives.

Issues with procurement in CIMIC – though they are likely to be partially addressed as a result of institutionalised operational cooperation – can also be addressed through several policymaker-

centric measures. Most important is the implementation of measures which ensure vertical integration within project cycles. A general lack of standardization (or enforcement thereof) results in projects defaulting to horizontal integration, which (in turn) fosters incompatibility between civil and military-sector stakeholders. As a general rule, it is useful to consider what other use cases a project output could have, and to (on the basis of such an analysis) conceptualise business models which would allow it to be commercialised outside of the niche use case for which it was initially intended. Planning in parallelism in this way contributes not only to the sustainability of project outputs, but also to the goal of furthering CIMIC. This is because envisioning parallel use cases which factor for the other side (for example, an EDA project which envisions commercialisation through practitioner networks) serves not only to bring these stakeholder together, but to improve information exchange and operational interoperability (thus reducing the barriers to cooperation).

## Key Contacts

<http://www.securityresearch-cou.eu/>

---

### EC DG HOME

Philippe Quevauviller  
Philippe.Quevauviller@ec.europa.eu

---

### JCBRN Defence COE

<https://www.jcbrncoe.cz/index.php>  
COL Dipl.-Kfm.  
Wolfgang Karl-Heinz REICH  
reichw@jcbrncoe.cz

---

### GIFT-CBRN

[www.giftforensics.eu](http://www.giftforensics.eu)  
Ed van Zalen  
e.van.zalen@nfi.minvenj.nl

---

### TOXI-TRIAGE

<http://toxi-triage.eu>  
Paul Thomas  
C.L.P.Thomas@lboro.ac.uk

---

### ENCIRCLE

<http://encircle-cbrn.eu/>  
Clive Goodchild  
clive.goodchild@baesystems.com

---

### eNOTICE

<https://www.h2020-enotice.eu/>  
Jean-Luc Gala  
jean-luc.gala@uclouvain.be  
Olga Vybornova  
olga.vybornova@uclouvain.be

## Forthcoming CoU events & other related events

- 13th CoU event, 25 – 29 March 2019, Brussels;
- 14th CoU event, 16 – 20 September 2019, Brussels;
- Security & Counter Terror Expo – 5 – 6 March, London;
- CBRNe Summit Europe 2019; 9 – 11 April, Birmingham;
- 3rd International Conference – CBRNE Research and Innovation; 20 – 23 May 2019; Nantes;
- 8th International Symposium on Physical Protection and Decontamination; 21 – 23 May, Munster;
- NCT Europe 2019; 25 – 27 June 2019; Vienna;
- Defence and Security Equipment International (DSEI); 10 – 13 September 2019, London;
- 13th CBRNe Protection Symposium and Exhibition of CBRNe Protection Equipment; 20 – 26 September 2016, Malmo, and;
- MILIPOL Paris 2019; 19 – 22 November 2019; Paris.