EARTO Working Group
Security & Defence Research

Towards Capability Driven Approaches across Security Sectors

22 November 2021

The EARTO Working Security & Defence Research (WG S&D) welcomes the European Commission (EC) "Action Plan on synergies between civil, defence and space industries" adopted on 22 February 2021. It is an ambitious action plan with 11 challenging actions leading to a more structured and well-functioning European innovation ecosystem. The EARTO WG S&D sees the capability-driven approach as a corner stone of this Action Plan. This position paper provides inputs to the EC supporting the development of Capability Driven Approaches (CDA) across Security Sectors.

1. Why should the Security sectors follow a Capability Driven Approach?

Due to the lack of appropriate inputs from the needs assessment of the individual European or national users into the work programmes, European and national security research has *de facto* developed a semi technology-driven approach to security research. Although the EC is conscientiously identifying, prioritising and defining topics for upcoming work programs, including various consultations with a variety of stakeholders, the selection of technologies for further research projects is often not based on the independently analysed operational needs and potential of the respective technology.

Public authorities and practitioner organisations have limited capacities to keep track of (emerging) technological developments and therefore often rather automatically follow the needs, interests and technology developments of industries and research organisations they are already connected with.

However, a predominantly supply-driven technology push to security research does not automatically lead to innovations meeting strategic and operational needs of public authorities and practitioner organisations, or to successful market launches. A capability driven approach would result in a more impartial interplay between demand-driven innovation and technology push, and a more comprehensive and harmonized overview within the EC of common capability needs, gaps and (emerging) technologies. With such approach, the Security sectors would benefit from an improved innovation ecosystem in which all actors are capable of effectively working together to enhance societal security: public authorities and practitioner organisations, RTOs and universities, large industries and SMEs, and citizens, civil society organisations and NGOs.

2. Main barriers for the adoption of Capability Driven Approaches

The idea of a **CDA is not new**: it is already well established in the defence and space sectors. Within the security domain, CDA is partially used: decision making on researching and developing new (technology) solutions in public agencies in several Member States is with various extend based on capability driven approaches. However, **a complex mix of many different aspects is hindering the effective implementation and application of CDA** in the security domain:

a. These approaches are **not well-integrated** nor interconnected.
b. **Regulatory frameworks**, **market conditions** and an **institutional culture,** which is not promoting inter-agency dialogues and exchange of best practices, pose significant hurdles to cross-domain capability management and to the establishment of a common long-term vision. Moreover, **differing (technical) languages** and a **low level of trust** among different organisations from the same or different security sectors are very common. They are even intensified through the **diversity of organisations** involved on the demand side compared to for example the military world (different governmental levels, different type of organisations adding on the different security sectors).
c. The internal fragmentation of all three areas (security, defence, space) results in different operational, organizational, analytical and financial structures, which hampers the adoption of the CDA (fragmentation brings also diversity of needs). Governmental executive organisations have rather complex and multifaceted **operations-driven organisational structures** and **limited capabilities** to effectively deal with forward-looking capability development and related appropriate longer-term R&D initiatives. A dominant factor in this context is still the **short-term oriented purchasing strategy** of equipment/tools.

3. Main building blocks of a Capability Driven Approach

Discussions within the security sector regarding CDA started within the Group of Personalities[1] and were continued by the European Security Research Advisory Board (ESRAB) and the European Security Research & Innovation Forum (ESRIF). It led to the definition of a European Security Research and Innovation Agenda (ESRIA) that identifies and roadmaps key capabilities and research needs. Although those efforts are much welcomed, they do not yet represent a security specific Capability Driven Approach for the sector. Further efforts should be done to develop a CDA for security using other sectors examples while adapting them to the security domain's specificities. In this context, several key aspects of a CDA should be pointed out as relevant for the security domain as follows:

a) Understanding and definition of "capabilities"

First of all, **it is an absolute prerequisite to have a common understanding and definition of "capabilities"** in the security context, to enable the identification of gaps in those capabilities against identified current and upcoming security threats and missions of security authorities and organisations. This refers to what is meant by 'security capabilities', how to commonly define and structure them to establish a common reference for security capability and strategy developers, R&D planners and innovation managers, procurers and contractors within the security sector and possibly across sectors (sector cross-cutting capabilities vs. sector-specific capabilities).

To complete this common reference on security capabilities, a **common security technology taxonomy**, allowing for a bi-directional link between capabilities and technologies, should be defined. Identifying and defining the capability gaps is the first step, connecting these to technologies is the following step. Both actions are needed to explore the possibilities of technologies to close the identified gaps and to identify additional requirements for the (emerging and/or to be developed) technologies[2].

b) Common vocabulary

Hand in hand with a common understanding comes the need for a **common vocabulary**. Not only at cross-national level, but even across organisations at Member States level, CDA suffers from a lack of a common vocabulary for the definition of capabilities, gaps and technologies. As a result, descriptions of capability gaps and potential solutions can neither be compared nor cross evaluated. A controlled vocabulary for the description of capabilities is a key enabler for any capability driven approach.

Capabilities can be defined at **different levels**: at the strategic, operational and tactical level. However, capabilities defined at the strategic level should be leading for the more detailed and concrete capabilities at the lower levels. Capabilities at the strategic level could be further broken down into individual capabilities at the operational level and these ones into (parameterizable) elementary capabilities at tactical level. There are undoubtedly capabilities that are specific for a particular sector, and capabilities that are similar and shared across domains. In either case, it is worthwhile making cross-sector analyses as the technologies to be used may be similar. Applying a common reference and common technology taxonomy will help in 1) aligning and harmonizing the sector-specific capability frameworks that are already in place, and 2) informing the RTOs, R&D organisations and other capability developers about potentially similar/comparable approaches to look at.

c) Joint ambitions

The European security sector and market are highly fragmented, both at EU and national level. **Jointly formulating ambitions**, identifying and defining the required **common capabilities and gaps** with respect to civil security and across security sectors is needed. A substantial number of actors of civil security, defence and aerospace originated from various Members States should be regrouped in any CDA. Actors from governments, end-user organisations, research (RTOs, universities), industry and other solution providers should be involved. RTO, university and industry representatives should cover a broad range of technical domains (knowing the state-of-the-art, trends and developments). It will be essential to identify various existing technologies to cover the capability gaps within the various sectors as well as to identify and monitor the technological initiatives that are currently under research or validation, and to be open towards combining/using solutions coming from various disciplines.

Good examples of such joint ambitions setting exercise are:

- the EDA CAPTECH working groups, developing their sector-specific Strategic Research Agendas (SRAs), aimed at defining an Overarching Strategic Research Agenda (OSRA, on Agency level),
- ENLETS which is defining capability gaps and required technologies in the field of law enforcement, and
- IFAFRI which has identified 10 common capability gaps of First Responders across the globe.

[1] Report of the Group Of Personalities on the Preparatory Action For CSDP-Related Research, February 2016

[2] 'Technologies' are not restricted to only software and hardware, but also include (work) processes, methods, procedures and trainings; a better and more encompassing term for this is 'socio-technical solutions'.

d) Implementation of change management

Following an inclusive approach is not only needed to jointly define common ambitions, capabilities and gaps and identify potential (emerging) technologies, it also supports the anticipation and preparation for the characteristic resistance to change by adequately **implementing change management**. For example, the main (market) drivers for the security domain are largely (although not exclusively) based on digitalisation leading to changes of the business and organisational strategy for all stakeholders. This will lead to the application of new methodologies and tools, as well as to new challenges potentially requiring new capabilities and stimulating disruptive changes of organisational structures, business processes, skills and tools. Accordingly, a more systemic view on potential solutions is needed for innovation management in security rather than view on digitalisation innovation only. Successfully implementing new solutions in an existing complex environment usually leads to certain changes in this environment. In specific, the mentioned (side)-effects require attention for dealing with resistance of people and organisational structures to successfully adopt new technologies and capabilities, not only under the topic of digitalisation. Given the potential sensitiveness and impact of solutions, the CDA in Security should anyway sufficiently consider the **inclusion of end-user and societal acceptance of solutions**, for example through verification and validation (V&V) processes (demand/user driven approach).

e) Forward-looking mind-set and skills

Thinking in capabilities rather than specific solutions, requires a **forward-looking mind-set and skills**. Especially representatives from governments and end-user organisations in the security sector should have a broad vision on the future of their organisations and need to have an open, non-conservative mind. Engaging in a CDA requires all actors to 1) think big, 2) take a longer-term perspective (10-15 years) and 3) not exclusively focus on technological possibilities. In addition, there should be a realistic view on the financial possibilities of the organisations. Facilitating the thinking of all relevant stakeholders and creating an inclusive forward-looking capability planning process requires science-based **methodologies** (and experts) as well as enhanced foresight capacities and future-oriented threat analyses. For such activities, Member States and EU level efforts should be institutionally interconnected. Potentially, the JRC's Observatory for Critical Technologies could facilitate such connection.

f) Scenario-driven CDA

CDA should be **scenario-driven** with scenarios that are both realistic ones as well as well-designed wildcards that facilitate non-linear thinking really going beyond the 'here and now' status. The scenarios should include both security, technological and societal challenges and threats as well as opportunities. Three types of scenarios can be differentiated:

- contextual scenarios, setting the strategic scene,
- operational scenarios, sketching the operational environment where the practitioner organisations have to operate in, and
- tactical scenarios, supporting the measurement of performance of existing and/or simulated (elementary) capabilities.

Furthermore, these scenarios need to be near-, mid- and long-term scenarios. This **time dimension** is essential to make decisions regarding the development of roadmaps, when to achieve readiness levels, and required investments.

g) Sand-box environments

Again, a definition of different levels of capabilities (using a standardized vocabulary) could be used not least to identify fields where there is less pushback to ease into a transition to a more "open" approach. Common methodologies could support the process, like **sand-box environments**. These are controlled environments in which (future) scenarios can be played and new technologies including their effects on this environment can be tried out. Following an **iterative Concept Development & Evaluation approach,** in which technologies with human-system interactions can be tested, is another essential building block of CDA. It prevents CDA from being only an intellectual exercise, and supports sound technology development, skill development, piloting and demonstration as well as the assessment of potential systemic changes/effects caused by the operationalisation of the new solution. Especially due to privacy, security and ethical requirements as well as societal technology acceptance, **sand-box environments which support technology experimentation are a fundamental prerequisite for innovation in the security domain**. Sand-box environments illustrate **the added value of capability development alongside technology development**, mutually inspiring each other.

h) Procurement and development of technologies

A CDA should result in **filling the identified current and future gaps**. Therefore, a good mechanism needs to be installed to communicate the needs and expressed intentions to **procure and develop technologies** to possible solutions providers and/or include other approaches to overcome financial hurdles. Current EU approaches such as PCP and PPI projects are good examples for this. Actively involving solutions providers (at least to a certain extent) in the capability assessments is needed as they are very much aware of emerging technological functionalities, and they need to understand the

operational challenges faced by the security organisations to produce technologies actually fitting the (future) operational environments.

Figure 1 may serve as an attempt to **summarize the scope** of a capability driven approach.

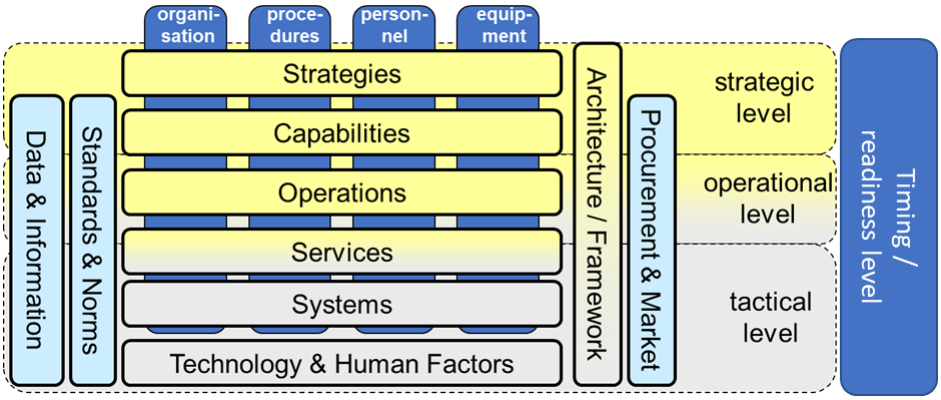

Figure 1: Scope of Capability Driven Approach (inspired by NATO Architecture Framework)

i) Increased cooperation activities

Last and certainly not least, **increased cooperation activities** are of fundamental importance bringing effectively together end-users, public authorities, industry and research. **Creating a community** that is committed and has the (financial) means to collaborate, is even at Member State level difficult to achieve. At EC level, the main challenge for the adoption of a CDA is the political, legal and organizational alignment to define a framework for joint collaboration between the different European MS and their stakeholders in the critical security areas of the civil, defence and aerospace. For example, it would prevent that national industry stakes hamper the timely and efficient development of capabilities and capacities (i.e. national sovereignty prevails strategic sovereignty at EC level). Potentially, the Community for European Research and Innovation for Security (CERIS) could facilitate this community building.

To summarise, the essential prerequisite for any successful implementation of a CDA as described above is a **sustained political will** to do it: **it requires ownership, sustained funds for participation of security stakeholders, and a visible uptake of its results into actions**.

4. Fostering the technological and industrial base in the EU

The CDA, if implemented correctly, leading to a clear longer-term vision for the future and how it will be funded and adopted, opens a window of opportunity for selected capability demands for joint developments and investments across organisations and nations including aspects of standardisation, IPR, public procurement and also further research needs. Only such **joint developments can generate enough economies of scale** to be economically robust (e.g. to invest in protecting IPR), and to be at the same time flexible enough to have an appeal to other potential customers outside of the EU. To be able to do that would increase the attractivity of the market and in turn lead to a healthier technological and industrial base. In the long run, a common basis for a CDA also increases the chances of mitigating fiscal aspects such as different regulations and market conditions (including procurement patterns) in different Member States as well as enabling the clustering of the current fuzzy diversity of solutions providers. Early system requirement specification based on a capability development strategy enables innovative technology and solution development that is the basis for sound IPR development and global competitiveness of new technologies and new solutions.

To increase EU capabilities, it is needed that Member States are really **committed to collaborate at EU level**, not only guided by the needs and interests of larger Member States and their national industries, resulting in potential advantages for these solution providers during the procurement process. Also including capability gaps and needs of smaller Member States enables industries and other solution providers of these Member States to engage in researching and developing new solutions. Having at the EU level an inclusive overview of gaps and required technologies offers: 1) to all potential providers, the opportunity to address the identified gaps (creating a level playing field), and 2) to the procurement agencies, more diverse offers of potential providers (increasing value for money). In the end, this will contribute to increased industrial and innovation sovereignty of the EU as a whole.

Aligning existing approaches into the proposed "joint" capability driven approach, and identifying capability demands (gaps and needs) that are sufficiently aligned at the various levels as indicated above, would allow to generate a "competition of ideas" for the capability in question, giving the customer some variance of possible solutions. For RTOs this can be a challenge as parts of existing and stable value chains are endangered. However, in the long run, having a clear vision for the future of what is needed and how it will be funded and adopted, this will increase the quality of the solutions and **creates opportunities for new value chains** to emerge.

In addition, a CDA would require discussing current shortfalls and potential collaborations and should result in better awareness of the needs and ideas of "the others", and in turn in better interoperability of services and more efficient security processes. Also, a capability- or demand-driven approach requires the involvement of end-users already in the definition of development programs, and throughout the whole development process; the satisfaction with, and the acceptance of, the final product (and its success on/fitness to the market) is more likely.

5. Role, position and activities of Research and Technology Organisations

a) Nodal position of RTOs in the ecosystem

RTOs tend to be closer to industry, especially to SMEs, than academies and, in many cases, working together with universities and other fundamental research bodies, they can smoothly streamline technology transfer to industry and users. Moreover, RTOs have a strong focus on creating business value thanks to robust IPR policies[3], used as assets for collaboration with industry and/or creating new business through spin-offs or start-ups. RTOs play a key role in disseminating research opportunities to industry and gathering strategic stakeholders, public and private, across Europe to create competitive consortia and critical mass. Many RTOs have strategic collaboration agreements with policy makers and practitioners at Member State level establishing a firm link between policy, needs and research.

b) Impartiality of RTOs

RTOs are ideally suited as partners to the public and to private players in a CDA as they are themselves to a degree impartial to some of the challenges that the other actors have to deal with. They can be used to create an impartial overview of current and foreseeable technological options to fulfil a certain capability (horizon scanning, technology analysis and assessments, technology foresight studies) and thereby providing the push function (what might be available in the near future, how can this be beneficial for capability development).

c) Medium- to long-term technological perspective of RTOs

The capabilities of RTOs allow them to have a medium- to long-term technological perspective, detecting trends and synergies between the different sectors and technological branches, and participating in the different stages in the process of research and development of innovative solutions responding to new global security challenges. RTOs support industry in the development and adoption stages of different technology-based solutions. RTOs can help to facilitate technology and know-how transfer from academic research into industrial application, and together with industry and help bridging the dreaded gap between the proof-of-concept for a technological solution and the clear implementation strategy. This "valley of death" is often challenging to companies, as heavy investments are required while the realisation is still in doubt.

d) Analysis capacity of RTOs

RTOs are well suited to analyse and understand the very specific challenges that are prevalent in the "exotic" market of security capabilities, and can not only provide information on that but also provide and develop methodologies as described above to counter those challenges. In general, RTOs have a broad picture of (inter)national research and innovation carried out in the different sectors, by detecting technological and policy trends as well as developing new tools and solutions for the medium and long-term future. Likewise, they have a good overview of current solutions on the market to respond to the needs of the three sectors. This enables RTOs to detect synergies between gaps and potential solutions across these sectors and exchange lessons learnt between these sectors.

e) RTOs as enablers of cooperation

Finally, a close cooperation among end-users, public authorities, industry and research are a prerequisite for global competitive technology and service developments. Enabling, fostering and moderating such multi-stakeholder environments are prime capabilities of RTOs.

f) Examples of RTOs developing and implementing CDA

RTOs are already undertaking many activities to foster the adoption of Capability Driven Approaches in different domains. For example in Germany, the Netherlands, Spain, Austria and Portugal, RTOs are working on the development and implementation of CDA in their strategic research and innovation planning support to civil security organisations (police and civil protection agencies) as well as to the defence domain. These activities are also focused on strengthening the currently missing foresight capacities in these sectors (capability pull rather than technology push).
Both in multi-year national research programs and EC-funded projects, RTOs perform R&D activities on key enabling technologies that provide solutions in the civil, security and defence domains. RTOs establish connections and synergies between different actors.

[3] EARTO Paper: Towards a Balanced Approach Between IPRs and Open Science Policy, 31 July 2020

Within the context of security, several RTOs take part in EC-funded practitioner network projects, like i-LEAD, MEDEA, CYCLOPES and FIRE-IN, supporting practitioner organisations in adopting CDA. The FIRE-IN project for instance is following a CDA by identifying common gaps and performing a related solution screening as well as by formulating remaining gaps into research and standardisation roadmaps.

Another exemplary project, DRIVER+, has developed a Trial Guidance Methodology based on a CDA supporting practitioners to identify capability gaps, and to systematically assess the added value of (socio-technological) solutions in addressing these gaps. The Portfolio of Solutions was developed to collect experiences and lessons learned of trialling new solutions, and to catalogue available and emerging solutions categorized by (crisis management) functions and gaps. The online Crisis Management Innovation Network Europe (CMINE) platform was developed to stimulate discussions between the various actors (practitioners, researchers, industry, government, EC). A Centre of Expertise network has been established organizing various practitioner organisations throughout Europe supporting each other in applying the DRIVER+ outcomes and implementing a CDA and fostering innovation in crisis management and resilience. In order to create a common vocabulary, a standardised terminology list has been developed. All these products are freely available and are being used and further developed in various EC-funded projects and by many different organisations.

6. EARTO WG S&D recommendations for EU security authorities

Based on the RTOs experiences across the various security domains, the EARTO WG S&D gives the following recommendations regarding the adoption and implementation of Capability Driven Approaches across the different internal security sectors:

A. **Implement a continuous process:** A Capability Development process delivers benefits when based on a long term and steady application. It is therefore imperative to implement a continuous process that enables methodologically experienced experts to develop, test, improve and maintain methods, procedures and results over several years in time. In collaboration with the JRC, RTOs could provide such expertise. **This can only be done if the funding of the core elements of such activities is organized as a longer-term (at least 5 to 10 years) commitment, and that a core team of people and organisations uphold this process.** Maybe a one-size-fits-all CDA would not work for all internal security domains, but a common basis with some domain specific instruments, making use of experiences in the defence sector, seems to have great potential. In order to achieve this, **a clear ownership and governance structure of this process at the EC level should be established**, potentially linked with the JRC's Observatory for Critical Technologies. At EC level decisions need to be taken for instance regarding the common terminology and technology taxonomy; several EC-funded projects[4] and other initiatives[5] have already proposed terminologies and taxonomies, but none have been formally adopted and implemented yet.

B. **Broaden the collaborative framework:** This initiative may be extended with the sustained establishment of a **broader collaborative framework** (initiatives that are being launched in different technological domains and industrial sectors), **with institutionalized working groups** formed by the different actors (EC institutions, public authorities, practitioner organisations, industries, RTOs and universities) in the various sectors. **This collaborative framework should deploy its activities in different EU regions, aiming at interfacing with already existing CDAs on Member States level** (and even below), so that its actions and results can achieve a wider scope. Main objectives would be to bring together and align interests, opportunities, threats and risks, definitions and categorisations of (main) security capabilities and related technologies, plans, a common language, etc.

C. **Have an open discussion on gaps:** Next to having such a funded and sustained instrument and mechanism for a successful CDA, **it is fundamental for EU security authorities for having an open discussion on gaps**. In many respects, the provision of security is understood as a core task of the nation state and as such the identification of (joint, EU-wide) capabilities or capability gaps is threatening the nation state narrative in several respects – a challenge that is for example particularly visible with respect to the development of joint response procedures linked with the Union Civil Protection mechanism (UCPM). The identification of joint capabilities works better in the military context; an important reason for this is that defence related matters in all Member States are being dealt with by a Ministry of Defence, which makes it easier to collaborate in international networks. For the various domains within Security, this is not the case: in a single Member State the responsibilities are distributed over various Ministries and agencies, and on top this varies considerably between Member States. This hinders a harmonized CDA within the broad area of Security. Next to the "one-shop" advantage, the defence sector benefits from its longer-term perspective, which also enables the definition of needed capabilities and related gaps in the (far) future. Joint discussions around potential shortfalls in the future are by far less sensitive than those on immediate, current gaps. It is thus recommended to not only generally foster a more foresight-oriented approach, but to **actually develop and initiate the**

[4] For instance STACCATO, ETCETERA, CRESCENDO, ACRIMAS, DRIVER+
[5] NATO's Emerging and Disruptive Technologies, EDA Prioritisation Platform

process by firstly focussing on the discussion around common gaps in the near future (10-15 years ahead).

D. **Establish a more structured and harmonized approach for capability and innovation management between the various national authorities:** Sharing and discussing joint capability gaps in a transparent way at EC level, without necessarily promoting (and protecting) only national industries and RTOs, would be welcomed. This would also help to enhance the involvement of public authorities in EC-funded research and innovation projects: in our experience only a limited number of these actors is active as partner (mainly due to the longer-term orientation) and/or providing financial support to RTOs participating in these projects.

EARTO WG S&D Members stay at disposal to the EC services to provide any further inputs as seen fit.

RTOs - Research and Technology Organisations: *From the lab to your everyday life. RTOs innovate to improve your health and well-being, your safety and security, your mobility and connectivity. RTOs' technologies cover all scientific fields. Their work ranges from basic research to new products and services development. RTOs are non-profit organisations with public missions to support society. To do so, they closely cooperate with industries, large and small, as well as a wide array of public actors.*

EARTO - European Association of Research and Technology Organisations
Founded in 1999, EARTO promotes RTOs and represents their interest in Europe. EARTO network counts over 350 RTOs in more than 20 countries. EARTO members represent 150.000 highly-skilled researchers and engineers managing a wide range of innovation infrastructures.

EARTO Working Group Security and Defence Research *is composed of 65 EU Affairs Specialists working within our membership to elaborate and to voice consolidated positions of RTOs and address them to the EC and other bodies.*

EARTO WG Security & Defence Research Chair:	*EARTO Contact:*
Marcel van Berlo, TNO	*secretariat@earto.eu*
marcel.vanberlo@tno.nl	*+32 2 502 86 98*
	www.earto.eu