EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

Directorate B: Borders, Interoperability and Innovation
Unit B.4 : Innovation and Industry for Security

PASAG report 2 -2020 – Dual-Use for Security

Optimising access to dual-use R&T and R&D results for security

Synergies and "dual-use" in the specific areas of common/dual interest in both the security and defence programme 2019

Optimising access to dual-use R&T and R&D results for security

Synergies and "dual-use" in the specific areas of common/dual interest in both the security and defence programme

Report of the Horizon 2020 Protection and Security Advisory Group (PASAG)[1]

July 2020

Table of Contents

Executive summary....2

Introduction....6

The issue....7

1 What does dual use mean?....8

2. Is there scope for dual use in the new EU defence programme?....11

3. How to optimize the access to dual-use R&T and R&D results of the defence programme for security....14

3.1 Coordination between the security and defence programme at a strategic level: the long term scenario....14

3.2 Coordination between the security and defence programme at institutional level: a short-term practical approach....16

3.3 Access to dual-use defence research and development results: the potential legal and technical constraints....17

3.4 Access to dual-use security research and development results: the same potential legal and technical constraints?....20

4. Conclusion....22

[1] More information about the PASAG can be found here: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3010

Executive summary

Since 2004 the European Commission has been funding security research, technology and development (R&T and R&D) projects targeting exclusively civil applications, through the Preparatory Action on Security Research (PASR) and then through its research framework programme (FP7 and Horizon 2020).

This situation has changed in 2017 with the launch of a Preparatory Action on Defence Research (PADR[2]) and the start, in March 2019, of a European Defence Industrial Development Programme (EDIDP3), both intended to be pilot programmes until 2021, when they would become part of a European Defence Fund (EDF) under the EU's next Multiannual Financial Framework (2021/2027)[3].

The defence R&T and R&D funding stream is fully separated from the current and new research framework programme, Horizon 2020/Horizon Europe, which will continue funding civil security, while the defence programme will support projects with defence applications only.

Notwithstanding the clear demarcation between funding streams, the EC recommends promoting synergies and seeking complementarities between the two programmes to avoid the risk of duplication of investments and to ensure that research results in one area could be used for the benefit of applications and development in the other.

The PASAG Group has identified that there is however, no institutionalised policy approach and related mechanism in place, to promote such synergies, complementarities and access to results between the two programmes.

The PASAG Group is of the view that the prerequisite for promoting synergies between the security and defence R&T and R&D programmes lies in identifying areas/domains of reciprocal interest for both security and defence users. In fact, **the Group believes that synergies should be promoted only in the specific areas of common/dual interest in both the security and defence programme, assuming that there could eventually be scope for "dual-use" of results in those specific areas only.**

Based on this assumption, **this paper addresses the concept of "dual-use" R&T and R&D, concluding that a clarification should be provided by the EC especially in consideration of the new defence research programme**. It is indeed challenging to identify a clear demarcation between civil (security, but not only) and defence research for technologies with lower TRL, since they are loosely related to the field of application ("application agnostic"), and therefore their potential for dual-use is higher. When it comes to higher TRLs and R&D , the reality is more varied and should be examined on a case by case basis, especially in certain domains such as Cyber, Maritime, C4I (Command, Control Computer, Communication and intelligence) and CBRN (Chemical,

2 Preparatory Action on Defence Research, Guide for Applicants, European Commission Decision C(2018) 1383), 15 March 2018 http://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/guide/pse/pppa-guide-applicants-padr-18_en.pdf

3 http://ec.europa.eu/budget/mff/index2021-2027_en.cfm

Biological, Radiological and Nuclear) where there is little or no difference between security and defence applications.

The paper further examines whether there could be interest for security users[4] in accessing defence R&T and R&D on on-going and future programmes results. When reviewing projects already selected for PADR funding, within the EDIDP first work programme and the EDF Regulation[5], it appears increasingly evident that some domains present an interest for security users. Sharing results of projects could therefore be useful. This is also valid for the security programme with regards to defence users. Consequently, **the PASAG recommends that the EC better identifies the areas of the defence and security programmes where projects could present an interest for the other community in order to improve coordination and exploit synergies.**

The third section of this paper provides strategic and technical recommendations on how to improve coordination and exploit synergies in the areas of the security and defence programmes of common interest.

Ideally, the coordination of investments in the dual areas of the security and defence programmes should come from an upfront structured and institutionalised strategic process involving the respective Programme Committees and the European Commission. Security and defence users should share their respective operational capability needs and gaps in those areas of common interest and identify common dedicated technology and systems development road maps.

Such a process would however require a structural change in the way the security sector approaches planning, aligning with the practices of the defence sector. Such a strategic coordination needs preparation and would be currently premature. It could however be considered as a longer term objective that would likely envisage an ad-hoc Joint Committee between the Horizon Europe security programme and EDF, with the mandate to coordinate the content of the programmes in those areas where there is common interest and complementarities, building on the mechanisms, tools and processes related to dual use already in place within the EDA[6]. **In order to move to a long-term strategic coordination, it would be necessary to increase the visibility of the defence planning process to the security sector, from one side, and to go through an analysis of the different security domains, on the other, at the EU level, within which an initial capability-based approach could be tested.**

In addition to the above, the PASAG has identified a **number of short-term measures intended** to improve synergies between the areas of common interest of the security and defence programmes, applicable at the initial phase of the programming and at the final stage of project results.

At programming level, the PASAG recommends that the EC strengthen the existing inter-institutional coordination, especially among the EC services responsible for the security and for the defence programmes, and between the EC and EDA. A concrete

[4] PADR/EDIDP and EDF.

[5] The EDF itself indicates that it will bring positive spill over effects to the civilian field and that synergies should be sought with Horizon Europe in specific areas, identifying security research but also cyber, border control, maritime transport and space, as sectors that could benefit from the results of the projects supported by the EDF.

[6] EDA, European Defence Agency

way of implementing such a coordination, while maintaining separate the security and defence requirements, currently defined by the EC services in coordination with the respective programme committees, would be to organise joint meetings of these two programme committees dedicated to exchanges on dual-use needs and requirements, in cooperation with the EDA. Such a coordination between the security and defence work programmes (research and development) would be particularly effective in those domains where there is a clear dual interest (as previously addressed: maritime surveillance, border surveillance, CBRN, cyber security, autonomous systems, and others). It could also be proposed that the Member States agree sharing their results in those specific areas.

At project level, the Group recommends that the EC organise, on a regular basis, information events between the security and defence communities on the respective projects in the identified areas of common interest. These events would have an information purpose and would also allow to show-case mid-term and final project results to security and defence practitioners, Ministries of the Interior (MoI) and Defence (MoD). The PASAG deems that these events would contribute to increase the access to project results by the two communities as well as boost the strategic coordination of their capability needs.

However, granting access to results from PADR, EDIDP and, in the future, EDF, to security users, requires **overcoming legal and technical obstacles**, which the PASAG identified and matched with the following recommendations:

- To **optimise access to defence research actions results** only in the domains of interest to security users, the Commission should ensure that **the distribution of the Special Reports**[7] **should be extended to the pre-identified security authorities within MS and agencies of the EU.**
- **To optimise access to defence development action results,** the EC could consider extending the requirement to draft a **Special Report** in those areas pre-emptively identified of dual interest. Such reports would guarantee a partial access to the action results for policy-making and procurement purposes, with the obvious exclusion of any commercial exploitation.
- The EC should assess **extending the PCP scheme valid for EDF research actions also to development actions,** pre-emptively identified of a dual-use interest.
- Concerning classified information (CI), the EC should **open a discussion with MS on the modalities they intend to apply for actions in dual-use areas.**

For the sake of completeness, the Group went also through the **legal and technical obstacles that could hinder access to research and development results developed within H2020 security programme (and the future Horizon Europe), concluding that they seem to be less prominent than what has been highlighted above.**

[7] Special Reports are a mandatory output of the defence research programme and have been introduced for the first time in the current PADR and reiterated in the EDIDP and the EDF. Their format is detailed analysis of the research programme outcome provided to the Member States and containing classified and unclassified information.

The paper concludes providing a consideration on the relative impact the proposed coordination process between the two programmes and access to their respective results in the area of common interest, could have from a market perspective.

Summary: findings and recommendations		
Scope of dual use to be clarified	No clear demarcation between civil (security) and defence research for low TRL technologies since they are not related to a specific field of application ("application agnostic"). For higher TRLs and R&D , case by case basis approach to be encouraged, especially in certain domains such as Cyber, Maritime, C4I (Command, Control Computer, Communication and intelligence) and CBRN (Chemical, Biological, Radiological and Nuclear) where there is little or no difference between security and defence applications.	
	Clarification should be provided by the EC on the scope of dual-use R&T and R&D, in consideration of the new defence research and development programme, specifying the TRLs levels and domains of applications.	
Synergies between defence and civil (security) R&T and R&D programmes to be encouraged	There are domains of interest for security users within the future EDF programme (covering high TRLs levels and R&D levels) and within EDA programmes as well (lower TRLs). The other way round is also true. Defence users have already expressed an interest in some low TRLS civil programmes (security but not only) and in some specific domains covered by the security programme maritime surveillance, border surveillance, CBRN, cyber security, autonomous systems, etc.	
	Synergies should be promoted only in those domains of common interest within the respective security and defence programmes, to continue avoiding possible duplications. These domains are generally acknowledged but could be clarified or specified: maritime surveillance, border surveillance, CBRN, cyber security, autonomous systems, and others.	
in specific domains of common interest,	Accessing to defence results projects for security users and vice versa, in those specific areas, could also present an interest.	
	Increase	The EC should reinforce the existing inter-

at programme level to avoid and duplications **At project level, to exchange on resul**ts.	**institutional coordination at programme level**	institutional interaction among the EC services responsible for the security and for the defence programmes, and between the EC and EDA, in those identified domains.
		Organising some joint meetings between the defence and security programme committees dedicated to exchanging on needs and requirements in those domains of common interest, in cooperation with the EDA, would be to encourage.
	Promote access to results of project	The EC should organise, on a regular basis, information events between the security and defence communities to inform about the respective projects under implementation in the identified areas of common interest: show-case mid-term and final project results to security and defence practitioners; ministries of the interior (MoI) and defence (MoD).
	Overcome legal and technical obstacles to access results of defence programmes for security users	For access to defence research actions' results in those domains of interest to security users, the EC should ensure that the distribution of the Special Reports should be extended to the pre-identified security authorities within MS and agencies of the EU.
		For access to defence development actions' results, the EC could consider extending the requirement to draft a Special Report in those areas pre-emptively identified of dual interest. Such reports would guarantee a partial access to the action results for policy-making and procurement purposes, with the obvious exclusion of any commercial exploitation.
		The EC should assess extending the PCP scheme valid for EDF research actions also to development actions pre-emptively identified of a dual interest.

		Concerning classified information (CI), the EC should open a discussion with MS on the modalities they intend to apply for actions in dual-use areas.
	Legal and technical obstacles that could hinder access to research and development results developed within H2020 security programme (and the future Horizon Europe) for defence users, are less prominent than what has been highlighted above.	
Long term strategic coordination	In the long term, the coordination of investments in the dual areas of the security and defence programmes should come from an upfront structured and institutionalised strategic process involving the respective Programme Committees and the EC.	
	It would be useful to increase the visibility of the defence planning process to the security sector, from one side, and from the other side, to go through an analysis of the different security domains, at the EU level, within which an initial capability-based approach could be tested.	

Introduction

Civil-military cooperation is a core priority of the comprehensive and integrated approach to crisis management in the European Union (EU) external action context. The EU Common Security and Defence Policy (CSDP) missions and operations are indeed increasingly of a collective security and defence nature interconnecting civil security and military actors. The new EU Capability Development Plan (CDP[8]) approved by military stakeholders' points at the need to work closely with civilians to develop the capabilities needed for the EU missions. This civil-military nexus increasingly characterizes our national security and defence environments as well.

When it comes to research and development and their associated acquisition processes, however, the security and defence sectors have traditionally been exclusive of each other. The structure of the EU funding programmes, as well as a majority of the national ones, have not been reflecting the civil-military approach and, until recently, there has been no willingness from the EU Member States (MS) to finance defence research at the EU level.

[8]https://www.eda.europa.eu/info-hub/press-centre/latest-press-releases/2018/06/28/new-2018-eu-capability-development-priorities-approved.

Since 2004 the European Commission (EC) has been funding research, technology and development (R&T and R&D) projects targeting exclusively civil security applications, through the Preparatory Action on Security Research (PASR) and then its research framework programme (FP7 and Horizon 2020). At the same time, EU defence R&T and R&D were addressed exclusively within the remit of the European Defence Agency (EDA). Within Horizon 2020 however, it is acknowledged that some research activities including, but not limited to, the areas of security and space, can lead to the development or improvement of 'dual-use' technologies or goods, which could address the needs of both civil and military end-users[9]. Those research activities can be funded by Horizon 2020 provided that they are destined to civil applications. For this reason, in the absence of a dedicated EC programme for defence R&T and R&D, Horizon 2020 was considered by the security and the defence stakeholders as a useful tool for boosting innovation in dual-use technologies, of interest to both the civilian and the defence sectors.

This situation evolved in 2017 with the launch of the Preparatory Action on Defence Research (PADR[10]) and the start, in March 2019, of a European Defence Industrial Development Programme (EDIDP[11]), both intended to be pilot programmes until 2021, when they would become part of the European Defence Fund (EDF[12]) under the EU's next Multiannual Financial Framework (MFF) (2021/2027)[13]. The EDF will support investments in collaborative research and development projects of defence products and technologies. It will therefore provide a defence R&T and R&D funding stream fully separated from the new research framework programme, Horizon Europe, which will continue funding civil security.

In this new context, the PASAG Group came to the conclusion that there are no shared views on how to preserve the dual-use interest, on how to promote synergies between the two programmes and, more generally, on how to support a collective security and defence approach via the R&T and R&D programmes of the European Union.

The issue

As a general rule, the EC recommends seeking synergies and complementarities between security and defence R&T and R&D programmes, to avoid the risk of duplication of investments, but also to ensure that research results in one area could be used for applications and development in the other.

An example of this recommendation is provided in the 'Secure Societies' challenge of the Horizon 2020 work programme 2018/2020 where it is highlighted that "whereas

9 See explanatory note on "exclusive focus on civil applications" (http://ec.europa.eu/research/participants/portal/doc/call/h2020/drs-03-2015/1645161-explanatory_note_on_exclusive_focus_on_civil_applications_en.pdf)
10 Preparatory Action on Defence Research, Guide for Applicants, European Commission Decision C(2018) 1383), 15 March 2018 http://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/guide/pse/pppa-guide-applicants-padr-18_en.pdf
11 Commission implementing decision on the financing of the European Defence Industrial Development Programme and the adoption of the work programme for the years 2019 and 2020.
12 Proposal for a Regulation of the European Parliament and of the Council establishing the European Defence Fund, progress report, 1 March 2019
13 http://ec.europa.eu/budget/mff/index2021-2027_en.cfm

activities under Horizon 2020 will have an exclusive focus on civil applications (…) where necessary, actions should clearly demonstrate how they complement and do not overlap with actions undertaken under the Preparatory Action on Defence Research"[14].

The same preoccupation is reiterated in the Multiannual Financial Framework (MFF) proposal for 2021-2027, which states that "complementarity and synergies with Horizon Europe will be ensured, so that results under defence research also benefit civil research and vice-versa" but also "ensure that results under civil research can benefit the development of defence capabilities and vice-versa"[15].

The EC also expresses such concern in the proposal for a Regulation establishing the European Defence Fund (EDF) where it states that "in order to ensure coherence and complementarity in the promotion of the defence interests of the Union under the next MFF, the Commission will seek to ensure synergies with other UE initiatives in the field of civil R&D, such as security and cyber security, border control, coast guard, maritime transport and space and with the specific programme implementing Horizon Europe with a focus on civil applications so that results from defence R&D will benefit civil R&D and vice-versa"[16].

These and other documented references underscore the importance for the EC to promote synergies and complementarities between the two distinct programmes and budgets for civil and for defence R&T and R&D, in order to encourage potential spin-offs from one sector to the other.

However, no concrete policy approach or mechanism is currently in place to implement this objective.

To address the issue, this paper will focus specifically on dual-use technologies and products and areas of dual interest, as these have already proven to be a fertile area for boosting civil-military synergies, and reducing the risk of duplication, in the current EU research funding framework.

At the outset, however, it is useful to address the definition of dual use technologies and products, since currently, there is no commonly shared understanding of the scope of dual use and its applicability to the future R&D and R&T European framework.

In conversations held with stakeholders at both the EC and the national level, it is apparent that most consider this issue no longer relevant, since the situation has been clarified by funding defence and civil security research through separate streams, with no risk of duplication and no need for synergies or complementarities.

Moreover, some stakeholders argue that there are no realistic opportunities for synergies between the EU security and defence research programmes because of the many barriers that inhibit cross-fertilisation between security and defence (user requirements in the defence area come into play at a very early stage of the R&D process, defence research being long-term capability driven while security research is short term, etc.).

[14] Horizon 2020, Work Programme 2018-2020, "14. Secure societies - Protecting freedom and security of Europe and its citizens", page 6 (https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf)
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0321&from=EN
[16] https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-eu-defence-fund-regulation_en.pdf

Others, on the contrary, consider that complementarities and synergies could also apply to the R&D phase which could be of interest for applications in both sectors.

Against this conflicting background, the Protection and Security Advisory Group (PASAG) is tasked to analyse how to optimise access to dual-use R&T and R&D results for civilian security users. The Group has gone through the following questions which drive the analysis provided in this paper:

Can the results of defence R&T but also R&D be taken up in applications for the security market and in which areas?

What are the challenges?

How to overcome them?

To attempt to provide answers, this paper will firstly discuss the definition of the concept of dual use. Secondly, it will go through the analysis of a potential scope for dual use within the current and future defence research and development programmes to understand whether there is an area within which to increase the coordination and synergies between security and defence programmes. Thirdly, it will address the access to dual use R&T and R&D results for security and defence stakeholders at the EU level and will provide strategic and technical recommendations for optimising such access, while maintaining separate the two research and development programmes. Finally, it will propose an open question inviting the reader to further reflect on the long-term impact that an optimised access to results would have on the EU industrial security and defence market.

1. What does dual use mean?

From a purely practical perspective, 'dual use' refers to the possibility of a product or a technology to be applied in both the defence and civil security sectors, irrespective of which of the two has initially developed it.

Originally evolved as spin-offs from military projects, the so-called 'dual use' technologies are now developed in both the military and the civilian domain and cover a vast range of fields. It is generally acknowledged that defence research has been a strong driver of innovation with important spin-offs into civilian markets (touching many sectors of the economy)[17]. Conversely, security technologies developed for civilian markets are also recognised as having significant potential to benefit cutting-edge defence systems. This take-up of security technologies within the defence domain has increased in recent years, driven especially by reduced defence budgets, by rapid advances in key commercial technologies and by the evolution of defence missions

[17] With the creation of significant markets: internet protocol, propulsion technologies, CBRN detection equipment, etc. The Impact assessment of EDIDP[17] (European Defence Industrial Development Programme) indicates that defence R&D is at the origin of important spin-offs that benefit both the defence and the civil sector. A study on the economic benefits of the Eurofighter Typhoon programme values its technological externalities at USD 7.2 billion (minimum). The study also shows that important benefits were also derived in terms of organisational and process innovation through the introduction of a range of modern business practices throughout the supply chain. Investments in defence development may also improve the productivity of the economy by transferring resources to highly productive activities. Technology spin-offs were also identified from the Typhoon Programme to civil aircraft, to motor car industries (including Formula 1 racing cars in Italy and the UK) and to supply chains

towards a more "collective security" involving civil security and military forces, especially in the EU CSDP environment.

In the EU context, there is no commonly shared understanding as to what specifically renders a technology 'dual use'. Some generic definitions can be found in the 'EU funding for dual use practical guide'[18] but also in the 'Explanatory note on "exclusive focus on civil applications"'[19] attached to Horizon 2020, which state that a considerable number of technologies and products are generic and can address the needs of both civil and military end-users. They are commonly referred as 'dual-use' goods or technologies. The EC, but also EDA, uses the Council Regulation (EC) No 428/2009[20] that refers to dual-use 'items' as items, including software and technology, which can be used for both civil and military purposes. The only detailed list of dual-use items available is within the Regulation for the control of exports, transfer, brokering and transit of 'dual-use' items (Regulation EC No428/2009) which describes in detail the kind of items that cannot be exported. Annex 1 to the Regulation groups dual-use products and technologies in the 10 categories: (i) Nuclear materials, facilities and equipment; (ii) Materials, chemicals, micro-organisms and toxins; (iii) Materials processing; (iv) Electronics; (v) Computers; (vi) Telecommunications and information security; (vii) Sensors and lasers; (viii) Navigation and avionics; (ix) Marine; (x) Aerospace and propulsion.

In the 'EU funding for Dual-Use – a practical guide to accessing EU funds for European Regional Authorities and SMEs', the Commission provides eligibility rules for dual-use projects that could be funded by the EU instruments, such as the programme for SMEs – COSME, Horizon 2020 and the European Structural and Investment Funds (2014).

An alternative way of considering dual use technologies and goods is to look at their Technological Readiness Levels (TRLs)[21]. In this context, it is easier to identify a duality at low TRLs, although this is not explicitly mentioned in any EU official document. It is generally accepted that technologies with TRLs up to level 5 are loosely related to their field of application and are, therefore, not exclusively military or civil by nature (see Annex 1). They could be defined as 'application agnostic'. Only when applied and used in a dedicated operational environment[22], a specific technology is identified as military or civilian. Research related to sub-components and materials, insofar as they can be considered 'enabling technologies', is to be considered 'application agnostic' and therefore potentially 'dual' in nature (to be used for developments in civil security or military applications). This is the case for example, for advanced materials, nanoelectronics, information and communication technologies (ICT).

[18] "EU funding for Dual Use. A practical guide to accessing EU funds for European Regional Authorities and SMEs", European Commission, DG Enterprise and Industry, October 2014

[19] https://ec.europa.eu/research/participants/portal/doc/call/h2020/ds-04-2015/1645170-explanatory_note_on_exclusive_focus_on_civil_applications_en.pdf

[20] Article 2 of the Regulation setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

[21] TRL scale is a measurement system used to assess the maturity level of a technology during the acquisition process. The EC has formally introduced the TRL scale in its research framework programme (Horizon 2020) in 2014. See Annex 1 for further information.

[22] "Technology Readiness Assessment (TRA) Deskbook", US Department of Defence, July 2009 (http://acqnotes.com/Attachments/Technology Readiness Assessment (TRA) Deskbook.pdf)

For higher TRLs, between TRL 6 and 7, it is commonly agreed, within the defence sector especially, that they represent an early stage of a development phase specific to an application or operational scenario or to preliminary requirements already defined by the customer. This is no longer a purely 'dual' environment because the requirements associated to the utilisation of the above-mentioned technologies and goods are not anymore identical between the security and defence sectors and an application, even if only embryonic, in one domain is already identified. Generally, cross-fertilisation between defence and security at this stage seems to be limited not only by institutional challenges, such as the confidentiality attached to the representation of operational threat scenarios, but also the military/competitive advantage that might result from a cutting-edge technology, different technology development cycles, existence of specific military operational requirements, and more.

However, this is not always the case. The reality is more varied and should be examined on a case by case basis, especially in certain domains such as Cyber, Maritime, C4I (Command, Control Computer, Communication and intelligence) and CBRN (Chemical, Biological, Radiological and Nuclear) where there is little or no difference between security and defence applications.

Some defence technologies developed through military programmes, especially in the area of large unmanned systems, could be deployed as such for civil use to enhance first responders' capabilities, but also to support border management and conduct investigative tasks. A defence industry technology or product can find a civil application thanks to investment as from TRL 6. Conversely, some security research project outputs can be of interest for defence users (small UAVs developments). Examples financed by Horizon 2020 are outlined in the table below[23].

[23] EU funding for Dual Use, "Dual use support Guide for Regions and SMEs", European Commission, p.48

Examples of funded projects

Icarus — Unmanned Search and Rescue. Involving 23 partners, amongst them Ecole Royale Militaire (BE) and Nato Undersea Research Center (IT). The project aims at using unmanned aerial systems and ground vehicle tools for search and rescue of civilians. The technologies developed will be used for detecting, locating and rescuing citizens. [FP7 Security. EU contribution: € 12.6 million].

Darius — Deployable SAR (Search and Rescue) Integrated chain with Unmanned System — is a project looking at how unmanned systems developed through military programmes can be deployed for civil use to enhance first responder capabilities and intervene in hazardous areas. The project is led by BAE Systems (UK). [FP7 Security. EU contribution: € 7.5 million].

Sectronic — Security System for Maritime Infrastructures, Ports and Coastal Zones — is a project aiming at observing and protecting critical marine infrastructures involving all observation means (offshore, onshore, air, space). Amongst the partners: Norwegian Defence Research Establishment. [FP7 Security. EU contribution: € 4.4 million].

Firerob — Autonomous firefighting robotic vehicle — is a project which aims at developing a prototype of autonomous unmanned firefighting vehicles able to efficiently fight against fire in hazardous environments. [FP7 SME. EU contribution: €0.8 million].

Sunny — Smart Unmanned aerial vehicle sensor Network for detection of border crossing and illegal entry — is a project whose objective is the design and realisation of a platform to gather data and information from distributed sensors active 24/7 in any weather conditions in order to patrol frontiers and intercept intrusions. [FP7 Security. EU contribution: € 9.6 million].

Sniffer — Capture and analysis of odours. It offers significant potential for border security applications related to the detection and analysis of persons, illegal substances and in particular explosives. [FP7 Security. EU contribution: € 3.5 million].

Smart@Fire: this is a pre-commercial procurement project aiming at developing integrated ICT solutions for smart personal protective equipment for firefighters and first responders that are transferrable in a global market. [FP7 ICT. EU contribution: € 1.5 million].

Some defence research organisations have taken part in FP7 projects. This is the case of the Swedish Defence Research Agency (projects Lotus [FP7 Security), Encounter [FP7 Security]), the Norwegian Defence Research Establishment (Sectronic), the Ecole Militaire Belge (DOTNAC [FP7 Transport], TIRAMISU [FP7 Security]) or the Direction générale de l'armement (FR) (Wezard, HAIC, OPENAIR [all FP7 Transport]).

The European Regional Development Fund (ERDF) has also recently opened support to the achievement of the civil objectives of projects with a clear dual nature. This was the case of the 'TURTLE' project in Portugal to develop a robotic vehicle for underwater operations that could be used for both civil and defence applications.

Duality can also apply to programmes conceived for civil security or defence use, for instance in the space sector. Many satellite programmes are of a dual-use nature (in France and Italy, the Pleiades and Cosmo Skymed programmes[24]). Such dual space-based systems are developed on a single orbital platform, which can provide a differentiated service depending on the customer.

[24] For example, in Earth observation satellites, the difference is in the resolution of the images (higher for classified defence applications) or the availability of the service (prioritisation).

In conclusion, in some cases, it may be difficult to identify a clear demarcation between security and defence research, and conversely to identify pre-emptively dual-use domains or project phases (TRLs or development phases). Technologies with lower TRL are loosely related to the field of application ("application agnostic"), and therefore their potential for dual-use is higher. When it comes to higher TRLs or some specific domains such as cyber, CBRN, maritime, communications, a more pragmatic approach would require a case-by-case analysis where the operational environment in which the technologies are to be used is carefully assessed.

2. Is there scope for dual use in the new EU defence programme?

The section above has identified several examples of EU civil programmes supporting projects of a dual use nature, especially within Horizon 2020 and the ERDF. This will likely continue to be the case within the next MFF where Horizon Europe, but also the ERDF, will continue to finance dual use technologies or goods provided that their use is limited to civil applications, as is the case currently.

What remains to be understood however is whether there is scope for dual use within the defence R&T and R&D programme (PADR/EDIDP and the EDF post 2020). Although they have been clearly designed to develop defence research and capabilities for Ministries of Defence (MODs), they do not rule out a potential duality in specific domains.

Indeed, the Commission proposal for a Regulation establishing the EDF does take into account this possible duality and suggests increased synergies between defence and other research sectors. It highlights that the EDF supports actions from the lower levels of maturity (upstream technology) to the higher levels, including prototype developments and clarifies that it will not include basic research, which will continue to be supported by other schemes such as Horizon Europe[25]. There is no clear indication at the moment of the scope of the 'defence-oriented' research, except that it should target emerging and future security threats.

Additionally, the EDF proposal argues that by adopting an integrated approach for defence research and development, bringing together the activities of the EDRP (defence research programme) and EDIDP (defence development programme), the Fund would not only contribute to a better exploitation of the results of defence research, but would also bring "positive spill over effects to the civilian field" [26]. It indicates that *"the Commission will take into account other activities financed under the Horizon Europe Framework programme in order to avoid unnecessary duplication and ensure cross-fertilisation and synergies between civil and defence research"*[27]. The EDF explicitly provides that synergies should be sought with Horizon Europe in specific areas,

[25] Proposal for a Regulation of the European Parliament and of the Council establishing the European Defence Fund, progress report, 1 March 2019 (recital 5, page 6)

[26] Ibidem (recital 27, page 15)

[27] Ibidem, (recital 25, page 15).

identifying security research but also cyber[28], border control, maritime transport and space, as sectors that could benefit from the results of projects supported by the EDF.

It is evident from the above that the EC implicitly considers that civilian users could benefit from the results of some defence projects. Effectively, it is very likely that police forces could benefit from developments in the area of soldier protection and security practitioners would certainly benefit from development of maritime situational awareness, cyber and space. At the moment, however it is difficult to identify concrete examples of potential synergies because the EDF programme has yet to be launched.

However, indications on some potential areas of synergies can be derived from the Capability Development Plan (CDP[29]) generic list of priorities that should drive the EDF future work programmes, among other drivers[30]. The CDP is organised in priorities which are quite broad31. Some of these could be of significant interest to civil security users. There is indeed a potential overlap between some CDP domains and Horizon 2020 security domains, especially in command and control and information, cyber, maritime but also space.

A more specific indication of possible dual use areas in the defence programmes comes from the projects already selected for the PADR funding in 2018 (defence research), some of which would be of interest to security users, as well. This is the case for the 'situational awareness at sea' topic that led to the funding of the OCEAN 2020 project[32]. The technology demonstrator for enhanced situational awareness in a naval environment which is expected to demonstrate the added value of unmanned systems in enhancing situational awareness, could be of interest for civil users. It is worth to mention here that the topic BES03 of the H2020 "Secure societies" Work Programme 2018-2020 makes explicit reference to avoiding overlapping with actions undertaken in the above-mentioned PADR topic. The 'Force protection and soldier systems' topics

[28] A concrete example is cybersecurity. The Commission recognises "the need to establish synergies between cyber defence research and development actions and other Union initiatives in the field of cybersecurity,"28, particularly through the future European Cybersecurity Industrial, Technology and Research Competence Centre

[29] The Capability Development Plan (CDP) provides a full capability picture that supports decision-making processes at EU and national levels regarding military capability development, contributing to increased coherence between Member States' defence planning. The CDP prioritises military capabilities that need to be addressed and developed by Member States and underpins the identification of cooperative activities that can be implemented by Member States in the cooperation framework of their choice, including under the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF)

[30] For more information on the CDP process, see https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f
https://www.eda.europa.eu/what-we-do/our-current-priorities/capability-development-plan

[31] The 2018 EU Capability Development Priorities cover the following lines of action:

- Enabling capabilities for cyber responsive operations
- Space-based information and communication services
- Information superiority
- Ground combat capabilities
- Enhanced logistic and medical supporting capabilities
- Naval manoeuvrability
- Underwater control contributing to resilience at sea
- Air superiority
- Air mobility
- Integration of military air capabilities in a changing aviation sector
- Cross-domain capabilities contributing to achieve EU's level of ambition

[32] "Open cooperation for European Maritime AwareNess – OCEAN2020" (www.ocean2020.eu)

dealing with electronics, voice and data communication, sensors, human interface devices but also CBRN detection systems, also have dual-use potential. The 'Inside Building Awareness and Navigation for Urban Warfare' is another example with a clear interest for civil security and domestic counter-terror operations[33]. Finally, the 'Autonomous swarms of unmanned vehicles project' which is developing a testbed to experiment new applications for the autonomous operations of UVs for a military scenario consisting in the protection of an airport, could also be used for civil security applications, in the area of border control, disaster monitoring, large area reconnaissance, Critical Infrastructure Protection, protection of public spaces and search and rescue. The topics of the 2019 PADR work programme have also a strong dual potential, when it comes to Artificial Intelligence, electromagnetic spectrum etc[34].

For higher TRLs (which includes design and prototyping), the EDIDP[35], published on 19 March 2019, offers clearer indications on the topics covered by the first work programme. There is a balanced mix of priority areas in line with the CDP, covering also dual-use domains. This is the case for force protection (resilience and protection of civilian population and infrastructure[36]), but also for CBRN detection capabilities,[37] cyber defence and security[38]; information management, C4, Unmanned systems (to protect critical infrastructure in urban areas), earth observation with automated interpretation of data, Artificial Intelligence for defence systems, maritime surveillance capabilities. Enhancing the protection of civilian populations and infrastructure against disruption falls squarely within the interest area of civil security operators. Other examples include Remotely Piloted Aircraft Systems (RPAS) for surveillance of maritime zones, land borders or critical assets which is also of interest to security users. Recent disruptions of air traffic at Gatwick Airport in London by unidentified drones are a clear example of where military grade solutions to detect and protect critical infrastructure would benefit civil security applications. The European High-Altitude Platform Station (Euro-HAPS) is a solution foreseen for defence but also for surveillance of maritime zones, land borders or critical assets.

Additionally, various EDIDP topics openly state that "attention will be paid to the civil and dual-use on-going initiatives at Union level to avoid any duplication (of funding)", in general[39] or with specific programmes such as Space Surveillance & Tracking (SST)[40], Copernicus[41] or Galileo[42].

---

[33] It provides a proof of concept for an innovative system to improve soldier awareness inside buildings through deployment of miniaturized sensors which can move and adapt to the environment to provide better coverage and improved situational awareness in confined spaces.

[34] Commission Decision on the financing of the 'Preparatory action on Defence research' and the adoption of the work programme for 2019 Brussels, 19.3.2019 C (2019) 1873 final.

[35] Commission Implementing Decision on the financing of the European Defence Industrial Development Programme and the adoption of the work programme for the years 2019 and 2020 Brussels, 19.3.2019 C(2019) 2205 final

[36] COMMISSION IMPLEMENTING DECISION on the financing of the European Defence Industrial Development Programme and the adoption of the work programme for the years 2019 and 2020 Brussels, 19.3.2019 C(2019) 2205 final. Topic 4.1 p.2

[37] Ibidem, p.3.

[38] Ibidem, 4.2 p.5, p.6.

[39] This is the case for Counter-Unmanned Air Systems (UASs) capabilities, p. 5.

[40] http://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness/Space_Surveillance_and_Tracking_-_SST_Segment

[41] Ibidem p.5

[42] Ibidem p.8

It appears evident that the designers of the EU defence programmes are encouraging synergies between the defence and the security programmes and trying to avoid duplications in areas where there is the potential for dual interest.

As a result, the PASAG can conclude that there is significant potential for a more focused effort to identify dual use R&D opportunities that would benefit both the defence and the civil security domains. Consequently, it recommends that the EC undertakes a structured analysis of the dual opportunity, identifying the scope and domains of application and establishing appropriate processes and mechanisms to enable the exploitation of the relevant synergies between the two security and defence research programmes. This would improve the effectiveness of the programmes and significantly reduce the risks of duplication.

The next section will explore possible modalities to increase coordination and synergies in dual use R&T and R&D and optimise access to dual use results for civilian security users.

3. How to optimise the access to dual-use R&T and R&D results of the defence programme for security

The first two sections of this paper have analysed the dual-use concept and recalled that, at the EU level, there is a perceived need to improve coordination and exploit synergies in the areas of dual interest for the current and future security and defence research and development programmes (PADR/EDIDP and EDF). However, while these policy expectations are clearly expressed in all the EU official documents related to the security and defence programmes, there is no formalised strategic coordination process in place between the two programmes yet.

In the view of the Group, such a strategic coordination process between the security and defence programmes should be established, not only to avoid possible risks of duplication of investments within the dual scope of the two programmes (at the project selection stage), but also to improve the synchronisation of topics within the respective work programmes. The latter would facilitate the preliminary identification of the topics and projects whose results could be shared between security and defence stakeholders. By doing so, it is also deemed that the substantial defence investment at the EU level (€13 billion for 2021-2027) could be leveraged, without reducing the benefit for the defence stakeholders.

3.1 Coordination between the security and defence programme at a strategic level: the long-term scenario

Ideally, the coordination of investments in the areas of dual interest between the security and defence programmes should derive from a structured and institutionalised strategic process involving the respective Programme Committees and the European Commission. Security and defence users should share their respective operational capability needs and gaps in dual areas and discuss how they would like to fill these gaps with dedicated technology and systems development road maps. Such a process would allow security and defence users "to acknowledge a common zone where they can

identify common strategic goals and effectively allocate and coordinate resources to achieve them"[43].

As a consequence, the demand side for dual use technologies and solutions at the EU level would be better structured and the dual-use research and development projects resulting from coordinated work programmes would be conceived from the beginning to meet shared security and defence needs, and would entail that access to the results is made available ex-ante to both security and defence EU and MS institutions. Moreover, this would have a positive impact on the dual-use offer at the EU level because technology and solution providers would indeed have greater motivation to invest (and co-invest) to develop dual-use technologies and products with the understanding that they can be leveraged into a broader community of security and defence users within the EU. This in turn would ensure that providers will be more willing to grant access to dual-use results to security and defence public authorities for policy making or procurement purposes.

However, today it is not realistically possible to implement the above-mentioned strategic coordination process because of the many structural challenges to be addressed in a medium to long term to reach this goal, especially in the security area. In fact, such process would require a structural change in the way the security sector approaches the cycle of planning from threat assessment to the definition of capabilities to mitigate the identified threats, in order to align it to what happens in the defence sector. As a matter of facts, the defence research and development programmes are led by a capability driven approach addressing short to long term needs[44]. A strategic long-term planning vision therefore drives the EU defence research and development programme as well as the national defence programmes, both of which are guided by priorities identified in capability development plans. In the EU environment, common capability needs and gaps are identified by the EDA, which has been specifically created to develop a European defence capability process. Specific tools such as the CDP[45] (Capability development Plan detailed into SCC (Strategic Context Cases)) and the OSRA (European Overarching Strategic Research Agenda declined into Strategic Research Agendas/SRAs and Technology Building Blocks/TBB)[46], align research agendas with operational needs and requirements[47]. This is not the case with the security research and development programmes because a strategic planning approach is still lacking not only at the EU level but also in most of the Member States. The H2020 security work programme remains essentially a list of domains and topics segmented in various

[43] Alberto P. Contaretti "EU-SECII project. The security governance approach" (SIAK Journal-Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis, 2009) https://www.bmi.gv.at/104/Wissenschaft_und_Forschung/SIAK-Journal/SIAK-Journal-Ausgaben/Jahrgang_2009/files/Contaretti_4_2009.pdf

[44] Capability based planning is a disciplined planning tool that comprises various phases, starting from the enunciation of the Political Guidance and the determination of the defence priorities; followed by an environment/threat assessment, a Mission Analysis (identifying what should be done to achieve pre-determined operational goals and objectives, considering defence missions and operational concepts as inputs). Scenario development is the further stage of the capability-based planning process. Following this, capability requirements are developed and capability gaps between current and required capabilities are assessed. Solutions definition is the last stage, divided into a research and technology road map, and a development road map to address gaps and off-the-shelf acquisition if solutions already exist. See detailed description of the EU capability development process. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%206_CDP.pdf

[45] https://www.eda.europa.eu/info-hub/press-centre/latest-press-releases/2018/06/28/new-2018-eu-capability-development-priorities-approved

[46] See detailed description of the OSRA approach: https://eda.europa.eu/docs/default-source/brochures/eda-osra-brochure.pdf

[47] Operational requirements are directly to technologies in a systematic and traceable manner.

security areas (border, maritime, critical infrastructure, cyber, etc), addressing challenges identified in the European Security Strategy with no link to national planning processes, which do not exist in the Member States.

It is thus structurally more difficult for security users to compare and share a mid- to long-term vision with the defence stakeholders because they are driven by shorter-term needs, and related limited budgets, and not by a comparable capability-driven vision.

The Group considers that a structured strategic coordination between security and defence research and development agendas in those areas of dual interest is not realistic yet, because of the different long-term planning approaches that characterise the security and defence sectors. In the long-term scenario, an ad-hoc Joint Committee between Horizon Europe security and EDF could be set up, with the mandate to establish a coordination process to align the content of the programmes in those areas where there are complementarities of a dual-use nature. Today such Committee would be premature.

However, it should be noted that there is a growing awareness among a limited number of EU Member States of the importance of mid- to long-term planning in the security domain, similarly to what happens in the United States since several years. This trend shows that, despite the structural difficulties highlighted above, conditions do exist for starting a reflection on a meaningful policy reform in this field to boost a forward-looking planning process in the security sector that could also drive research and development investments.

The Group has also noted that capability planning is not only inherently difficult for the security sector but also often not sufficiently known. A first practical recommendation to advance towards a strategic coordination, therefore, is to increase the visibility of the defence planning process to the security sector.

The Group also recommends that the EC goes through an analysis of the different security domains, at the EU and national levels, in order to identify specific security areas with dual use potential, within which an initial capability-based approach could be tested, while engaging the defence sector with a parallel but coordinated programme. This process would stimulate an ‘EU-triggered’ strategic vision specific to these domains, with the significant benefit of developing aligned defence and security technology and development roadmaps and identifying possible joint R&D efforts in specific dual-use domains, particularly in border protection, maritime surveillance, CBRN and cyber security. In this regard, considering that some embryonic pieces of a capability process do exist in areas such as border security (case of Frontex), it could be taken as a successful starting point to be extended to other dual-use areas.

3.2 Coordination between the security and defence programme at institutional level: a short-term practical approach

The Group has assessed a number of measures applicable in the short term within the areas of dual interest of the two security and defence programmes that would make realistic progresses towards a long-term structured strategic coordination.

Such measures would be applicable at programme/institutional level and at project level.

At programme level, a first step could be to establish an appropriate institutional coordination mechanism that would build on the existing interactions among different DGs of the European Commission and would involve the services responsible for both security and defence programmes. This would structure and formalise the existing sharing of information on topics and projects of common interest, so far carried out on a voluntary basis, among the responsible staff within the European Commission. It could also make better use of the existing tools and mechanisms already developed in the defence intergovernmental environment to enhance R&T civ/mil synergies.

In fact, institutionalised formal interactions on dual-use opportunities do exist already, especially between the EC and the defence intergovernmental environment represented by EDA. EDA in particular has developed a process to leverage existing funding mechanisms at EU level to support dual-use research in order to boost production of KETs-based products and investments that can bring dividends to defence systems [48]. The prioritisation process set up by EDA which consists in identifying appropriate funding instruments, including EC ones, that could match each Technology Building Blocks (TBB)[49], is a good example of progress towards seeking synergies and avoiding duplication of investments. Moreover, while the research and innovation activities carried out under Horizon 2020 have an exclusive focus on civil applications, the Commission exchanges information with EDA to assess which areas could also benefit defence capabilities. This process has been formalised by giving EDA an observer status within H2020 "Secure societies" Programme Committee to monitor both the definition of the biannual work programme and the projects with the potential to benefit the areas considered of 'dual' interest, such as border surveillance, CBRN and, overall, cyber.

Similarly, in the case of the PADR, run and managed by EDA on behalf of the EC, the choice of topics is subject to an internal verification within different EC services to avoid duplications, especially with H2020 projects that have already been financed. The EDIDP and the proposal for the future EDF also point to the need for attention to the on-going civil and dual-use initiatives at EC level to avoid any duplication (see previous chapter).

[48] Particularly in the area of Key Enabling Technologies (KETs). EDA's roadmap for dual-use technologies consists of the following elements: identifying and supporting dual-use Key Enabling Technologies (KETs), the development of nano-technologies through the JU ECSEL and the research for dual-use technologies eligible for funding through Structural and Investment Funds. KETs are the building blocks of advanced products and underpin traditional, high-tech European value chains. These advanced products are essential for the defence systems of today and the future. The main areas of interest are nanotechnologies, advanced materials and nano-electronics. The high-level group advises the European Commission to establish a strategy to boost industrial production of KETs-based products and investments will also bring dividends to defence systems. See Study on the dual-use potential ok Key Enabling Technologies (KETs) Contract EASME/COSME/2014/019, 13 January 2017. https://publications.europa.eu/en/publication-detail/-/publication/c092b731-f415-11e6-8a35-01aa75ed71a1

[49] https://eda.europa.eu/docs/default-source/brochures/eda-osra-brochure.pdf

As a result, the PASAG recommends that the EU establishes clear guidelines on how to ensure inter-institutional coordination, especially among the EC services responsible for security and for defence, and between EC and EDA, in order to promote synergies between the two research and development funding streams in the areas of dual interest , making better use of the EDA existing tools.

A concrete way of implementing such a coordination, while maintaining separated the security and defence requirements, today defined by the EC services in coordination with the respective programme committees, would be to organise some joint meetings of the two programme committees dedicated to exchanging on dual-use needs and requirements.

In addition, it would be desirable to formalise the existing voluntary coordination process between the EC services in charge of drafting the contents of the security and defence work programmes. Such coordination would be particularly effective in those areas where there is a clear dual interest (as previously addressed, maritime surveillance, border surveillance, CBRN, cyber security, autonomous systems, and others). As a way of example, this coordination process could provide for the staff in charge of the defence work programme to assist the security unit in the drafting phase of the security work programme by informing them of the existence of defence projects potentially leading to results of a dual interest. Moreover, it could request them to jointly agreeing on dual areas and topics that could be of potential interest for their respective users because of similar functional requirements.

As an outcome of this coordination process, risks of duplication of investment and human efforts would be avoided, and both the security and defence budgets would be optimised by developing complementary research streams within domains of dual interest. Moreover, the security budget would remain strictly committed to support civil applications as well as the defence budget to support military application (similarly to what was done between the EUCISE Horizon project and PADR OCEAN 2020).

At the project level, the PASAG recommends that the EC establishes a process for increasing awareness of results among the two programmes. The EC could organise, on a regular basis, information events to raise the awareness of the security and defence communities about the respective projects that are under implementation (in the areas of common interest only). These events, accessible upon invitation only, would have an information purpose and would also allow to show-case mid-term and final project results to: ministries of the interior (MoI) even though they do not represent the whole security user community (but could play a coordination role) and defence (MoD); and EDA. The Group deems that these events would contribute to increase the access to project results of the two communities as well as to boost the strategic coordination of their capability needs.

3.3 Access to dual-use defence research and development results: the potential legal and technical constraints.

Coordination and synergies at programme design and project level are important but not sufficient when thinking about access to results. Additional legal and technical constraints need to be overcome to effectively optimise access to dual-use results, especially from the defence programme.

Given that the PADR and EDIDP legal and technical provisions related to access to results will be substantially reflected in the future EDF, this sub-section will focus on the constraints that could come from this programme, especially in terms of Intellectual Property Rights (IPR), procurement and handling of Classified Information (CI).

Intellectual Property Rights (IPR)

With regard to the ownership of project results, the EDF proposal makes a difference between research and development results. Concerning the former, the EDF states that the ownership of the results originated from a research action supported by the EDF belongs to the generator[50]. This is fully in line with the provisions of the security research programmes, the current H2020 and the future Horizon Europe. The results are owned by the Union, and all the MS shall have access rights free of charge, only when the support of the Union is provided to research in the form of public procurement[51]. With regard to the results of a development action supported by the fund, the EDF proposal simply states that they shall not be owned by the Union[52].

With regard to the access to results, there is again no single EDF provision, but two different rules would apply to research and to development actions.

Concerning **research**, the Union has full access to results for non-commercial and non-competitive use[53] while the MS have access to results via a Special Report, mandatory for each research action funded by the EDF and containing classified and/or non-classified information[54]. The Special Report has been introduced for the first time in the current PADR and reiterated in the EDIDP and the EDF. The proposed EDF regulation states that the Special Report shall be distributed free of charge to all the MS which are allowed to "use it for purposes related to the use by or for their armed forces, or security or intelligence forces". In this regard, it appears that the main designated recipients are not necessarily limited to the Ministries of Defence (MoDs) of each MS.

[50] (Art 22, Par 1)

[51] (Art 22, Par 2)

[52] (Art 25 Par 1)

[53] (Art 22, Par 7)

[54] (Art 22, Par 6) That can be used for several purposes, including "study, evaluation, assessment, research, design, and product acceptance and certification, operation, training and disposal, as well as the assessment and drafting of technical requirements for procurement".

Therefore, in order to optimise access to defence research results, especially for the security users, the first technical recommendation is that for the domains of a dual interest, the Commission should ensure that there are not unnecessary restrictions to the distribution of the Special Reports also to the pre-identified security authorities within MS and agencies of the EU.

With regards to **development actions**, the Union has no access to results and no Special Reports are envisaged. Indeed, the IPR constraints applicable to development actions are very tight and do not appear to allow room for access to results by public or private entities.

The second technical recommendation is for the EC to consider extending the requirement to draft Special Reports also to those development actions that are mainly supported by Union funding and in those areas pre-emptively identified as of a dual interest at the Union level. The rules for the content of the circulation of these special reports should be reflecting the ones applicable to research actions. Such reports would guarantee a partial access to the action results for policy-making and procurement purposes, with the obvious exclusion of any commercial exploitation.

Pre-commercial procurement (PCP)

The PCPs[55] have been introduced in Horizon 2020 to support the introduction of research outcomes into the market and to incentivise the demand for new technologies by encouraging providers to invest in research and development with the reasonable expectation that there will be a market for their products.[56].

Since 2015, the above-mentioned H2020 secure societies work programme, includes a special provision according to which all the EU MS contracting authorities could benefit from access to PCP results, including their exploitation for further procurement. With this approach, the EU is promoting a more European dimension for "technical solutions applicable or interoperable transnationally, and of interest to the whole of the European Union beyond the few Member States involved in the initial pre-commercial procurement process"[57]. This has the potential of reducing the fragmentation and increasing the size of the EU security and defence markets.

The EDF proposal includes a generic provision for PCPs (Art 18) and a special provision for PCP research actions, which is particularly relevant when considering access to results. In Art 22, Par 8, the EDF proposal states that the "contracting authorities shall

[55] In fact, the aim of the PCPs in Horizon 2020 secure societies work programme is "to encourage the export of […] products beyond the borders of the country where they are designed and manufactured and where the relevant intellectual property is owned. Communication, Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public, Brussels, 14.12.2007 COM(2007) 799 final services in Europe https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0799:FIN:EN:PDF https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0799:FIN:EN:PDF

[56] ibidem

[57] ibidem

enjoy royalty-free access rights to the [research] results for their own use. Moreover, they shall also have the right to grant or request the owner to grant non-exclusive licenses to third parties to exploit the results under fair and reasonable conditions without any right to subcontract". As a result, all national procurement authorities of the EU MS could be able to procure the same technologies and solutions on the basis of the PCP results achieved through EU funding. Consequently, this special condition, facilitating access to results from PCP projects to MS' procurement authorities, is particularly important to achieve a truly European dimension in the security and the defence markets, with no negative impact on the commercial exploitation of results by IPR owners.

For development actions, on the contrary, the draft EDF regulation does not envisage any special provision for PCPs.

With specific regard to EDF research actions, it appears that the application of the above-mentioned special condition could allow third parties, the EU national procurement authorities, to be granted access to the PCP research results, under fair and reasonable conditions. In this regard, the third technical recommendation would be for the Commission to assess extending the PCP scheme valid for research actions also to development actions pre-emptively identified of a dual-use nature.

Protection of classified information (CI)

Often security and defence projects generate sensitive foreground (information, knowledge or technologies) that may need to be classified. The decision on the level of classification and the subsequent protection, on the basis of national and EU legislation, is the responsibility of its originator and has a major impact on the access to project results.

The proposed EDF regulation provides that the originator of foreground IP is "decided upon by the Member States on whose territory the recipients are established"[58]. Consequently, Member States may decide to be the originators of classified foreground and set up a specific security framework for its protection or attribute this task to the Commission [59]. In the latter case, the classification level is established at the EU level (EU Classified Information - EUCI) and the Commission is responsible for protecting the EUCI by, among others, assessing the need-to-know of any individual or entity requesting access to it. When classification of projects' foreground is performed by the MS, its level of assigned protection would depend on the national security assessment of the involved countries.

In the case of the EDF programme, the level of classification of each classified project deliverable would be defined by its originator, most probably upon prior consultation with the national security authorities of the other involved Member States. This situation could imply that, the originator decides to assign the highest classification among the ones proposed by the involved MS, with the consequent extra burden for the

[58] (Art 30, Par 4)

[59] ibidem

protection and handling of classified information put on countries that would have chosen a lower classification level if they were alone in a project.

A final point to be considered on protection of CI is that any background IP contributed to a defence research and development action carries with it its pre-existing classification level and attributes it also to the foreground IP created through the action. Consequently, the originator will have to assess the need-to-know of any third-party requesting access to results of an action containing classified background and seek the authorisation of the MS authorities which have classified that background in order to grant access to the foreground to the requesting third-party. In absence of a preliminary MoU among all the MS involved in a research/development action using classified background, this process may become very cumbersome.

The rules for the protection of CI described above are fully in line with their equivalent applied to H2020 within the secure societies challenge. The only substantial difference is in the possibility of the MS operating within the EDF framework to choose whether to set up a national security framework for each action or let the Commission do it.

The Group's fourth technical recommendation for the EC would be to open a discussion with MS on the modalities to handle classified information they intend to apply with specific regard to actions in dual-use areas and on the possibility to refer to the EUCI handling system

3.4 Access to dual-use security research and development results: the same potential legal and technical constraints?

The previous paragraph has focused on the legal and technical constraints that could potentially hinder or make more difficult the access to the results of the defence research and development programme for the security sector.

A question remains about whether the defence sector would encounter similar difficulties to access security research and development results both in the current H2020 and in the future Horizon Europe framework programmes.

The answer to the above-mentioned question is that the representatives of the defence sector would not experience the same legal and technical barriers than their security homologues for a number of reasons described below.

First of all, it is important to highlight that, in the absence of specific concerns related to classification of research results, the H2020 and Horizon Europe access rights to security research results are wider than for defence research programme The general H2020 and Horizon Europe rule, in fact, establishes that access to results (limited to non-commercial and non-competitive use) is granted to the Union institutions, bodies, offices or agencies for developing, implementing and monitoring Union's policies and programmes[60]. In addition to this rule, only within security research actions, "beneficiaries having received Union funding shall also grant access to their results

[60] Common understanding of the EU Parliament and Presidency of the Council on the Commission Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, Art 37, Par 5

(always limited to non-commercial and non-competitive use) on a royalty-free basis to Member States' national authorities, for developing, implementing and monitoring their policies or programmes in that area"[61]. Clearly, the latter provision would facilitate access to security research results also by national defence public authorities.

It must be stressed that dissemination is and will remain a key principle of the EU research framework programme, including the security area. Provisions such as "beneficiaries shall disseminate their results as soon as it is feasible, in a publicly available format, subject to any restrictions due to the protection of intellectual property, security rules or legitimate interests"[62] or "open access to research data shall be the general rule under the terms and conditions laid down in the grant agreement"[63] seem to be quite distant from the approach adopted in the EDF proposal and would definitely facilitate the access to research results, at least for defence public authorities.

Secondly, it has been already mentioned that the H2020 "Secure societies" work programme includes a special clause for pre-commercial procurements (PCPs) according to which all the EU MS contracting authorities could benefit from access to PCP results, including their exploitation for further procurement. The Commission proposal establishing the new Horizon Europe research framework programme includes a very similar provision to the one applicable to the research actions funded through the EDF. According to it, the contracting authorities participating in pre-commercial procurements actions funded within Horizon Europe "shall enjoy at least royalty-free access rights to the results for their own use and the right to grant, or require the participating contractors to grant, non-exclusive licences to third parties to exploit the results for the contracting authority under fair and reasonable conditions without any right to sub-license"[64]. Again, this would increase the possibility of the MS authorities not only to access but also to use security research results originated in the framework of a PCP.

Finally, in terms of classified information originated by a research action, a very significant difference can be observed between the security and defence research and development programmes. If the standard rule for the proposed EDF is that the originator of classified IP is agreed upon by the Member States where the recipients of the Union funding are based, in H2020 and Horizon Europe the originator is always the Commission. Consequently, the classified results originated by a security research action as well as the possible background included in them, are EUCI protected according to the provisions of Commission Decision 2015/444[65]. In its capacity as originator, the Commission is fully in charge of protecting and handling EUCI, including being the only subject entitled to assess the need to know of individuals requesting access to such information. This mechanism based on a sole entity seems to be simpler to grant access to classified research results to individuals from the defence sector who need to have it.

[61] ibidem
[62] Ibidem, Art 35, Par 2
[63] Ibidem, Art 35, Par 3
[64] Ibidem, Art 22, Par 3
[65] Ibidem, Art 16, Par 4

In consideration of all the above-mentioned reasons, the legal and technical constraints for the defence sector to access security research results seem to be less prominent than the vice versa.

As a concluding remark, the Group wishes to stress once again that the legal and technical obstacles that characterize the two sectors are important but not fundamental to determine the level of accessibility to dual-use research and development results. A pre-requisite to an optimised access to dual-use R&T and R&D results for security remains the establishment of a strategic coordination between the security and defence programmes at the institutional level described in the previous paragraphs of this chapter.

4. Conclusions

In this paper, the Group has firstly gone through the analysis of a potential scope for dual use within the current and future defence research and development programmes to understand whether there are areas within which to increase the coordination and synergies between security and defence programmes. Secondly, it has addressed the access to dual-use R&T and R&D results for security stakeholders at the EU level and has finally provided strategic and technical recommendations for optimising such access, while maintaining separated the two research and development programmes.

The most important recommendation provided by the Group to the EC is to undertake a number of short and long-term measures to increase the strategic coordination between the two programmes in order to avoid possible risks of duplication of (public) investments within areas of dual interest (at the project selection stage) and also to improve the synchronisation of topics between the respective work programmes. The latter would facilitate the preliminary identification of potential topics and projects of common interest whose results could be shared between security and defence stakeholders.

Within the strategic coordination mechanism mentioned above, security and defence actors would definitely gain a wider knowledge of the respective projects and results and would therefore ensure to reduce duplication and maximize public investment in research and development.

By way of a conclusion to this analysis, it should be noted that the impact of such coordination and access to results could however have little effect on the structure of the industrial base or on any decisive improvement of the equipment of forces, in the absence of a common or concerted acquisition policy between MS in both sectors.

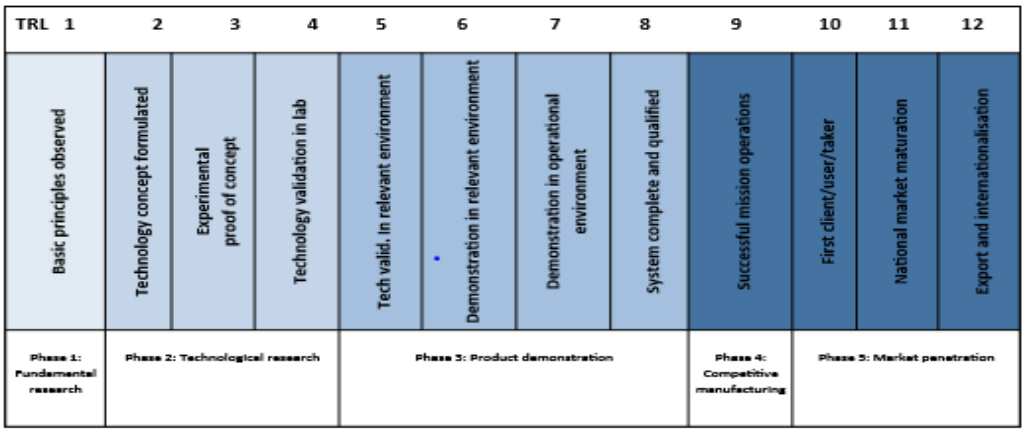
ANNEX 1

G. Technology readiness levels (TRL)

Where a topic description refers to a TRL, the following definitions apply, unless otherwise specified:

- TRL 1 – basic principles observed
- TRL 2 – technology concept formulated
- TRL 3 – experimental proof of concept
- TRL 4 – technology validated in lab
- TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 7 – system prototype demonstration in operational environment
- TRL 8 – system complete and qualified
- TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Figure 11 Revised Technology Readiness Levels (TRLs)



Source: Adapted from COM (2012) 341, A European Strategy for Key Enabling Technologies — A Bridge to Growth and Jobs