RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Policy Paper

Dual-Use Research and Technology (R&T) for Estonia's National Defence, Civil Security and Public Safety: Why, What and How?

Tomas Jermalavičius and Mikk Lellsaar[1]

June 2013

Summary

The policy paper explores the rationale for investing in the so-called dual-use research and technology (R&T) to support Estonia's national defence, civil security and public safety policy objectives. In addition, it investigates which areas of knowledge and technology generally have the greatest potential for an inter-agency approach and which of those areas are most relevant to Estonia's defence, security and safety organisations. It also considers a variety of business models for pursuing the inter-agency approach to R&T and its application in Estonia. The paper finds that the application of comprehensive security and broad-based defence thinking leads to a high degree of overlap in the interests of defence, security and safety organisations. These interests can be translated into many similar needs in terms of new knowledge, technology and innovation. The inter-agency approach to addressing those needs helps to achieve greater synergy in results and to use limited resources in a more rational way, but the approach has not gained much recognition in Estonia just yet. The paper recommends a number of measures to facilitate better co-operation between Estonia's defence, security and safety agencies (end-users) in exploiting the national and international science and technology base. The measures include: the drafting of a common new knowledge, technology and innovation agenda for the entire sector; partial integration of its implementation in the field of situational awareness and information management technologies (including cyber security) through a dedicated national research and development (R&D) programme; the formulation of common requirements by defence, security and safety organisations for some existing national programmes (e.g. health); collaboration (e.g. in research on human and organisational factors, in the field of modelling and simulation technological know-how, in the development of inter-agency planning methodologies) between defence and security educational and training establishments; constant co-ordination of R&T efforts in such fields as Chemical, Biological, Radiological, Nuclear and Explosives (CBRN-E) defence, unmanned systems and platforms, space technology and physical protection of personnel and infrastructure; and the maintenance of a broad awareness of R&T needs, opportunities and activities by governmental, public and private stakeholders.

Introduction

1. In 2010, a working group led by the Estonian Ministry of Defence (MOD) was formed with the purpose of advancing inter-agency co-operation between national defence, civil security and safety organisations in the field of technology. It was partly inspired by a joint seminar organised by the International Centre for Defence Studies (ICDS), the Estonian Academy of Sciences and the MOD, and conducted in the margins of a NATO Research and Technology Board meeting in the autumn of 2010. The

[1] Tomas Jermalavičius is a Research Fellow at the International Centre for Defence Studies, co-ordinating the Centre's 'Security, Strategy, Science and Technology' theme; Mikk Lellsaar is a member of a training programme at the Estonian State Chancellery, assigned to the Estonian Ministry of Defence. The views expressed in this paper do not necessarily reflect the official position of the State Chancellery, the Ministry of Defence or any other governmental organisation.

 ISSN 2228-0294

expectation was to develop synergies in R&T investments made by Estonia's national defence, civil security and safety organisations. However, there is no clear consensus on what should be done to make those synergies possible and on why and how it should be done.

2. This policy paper has been drafted in response to an MOD's knowledge requirement and aims to support the process of aligning the interests of national defence, civil security and safety organisations in R&T. It seeks to determine the main reasons for them to collaborate in R&T, to identify potential areas of focus and to propose a business model for such co-operation. It draws heavily on previous research performed by ICDS in the framework of its 'Security, Strategy, Science and Technology' theme, including a report on defence research and development in small NATO countries (Norway, Denmark and the Netherlands) published in 2009; a study on Estonian national security policies and their science and technology implications (encompassing the areas of cyber, energy and marine environment security, anti-terrorism and crisis management) drafted for the EU-funded Crescendo consortium in 2010; a report on Estonia's defence research and development compiled in 2011; and a policy paper on Baltic collaboration in defence-related R&T written in 2012.

3. In terms of methodology, we adopted a three-pronged approach in our research for this policy paper:

3.1 First, we looked outside Estonia by performing desk research on various existing studies about co-operation and synergies between defence, civil security and safety in Europe and by reviewing, where possible, the approach of some individual countries. The rationale for this was simple: Estonia does not have to re-invent the wheel and can adapt many practices found elsewhere to suit its own needs.

3.2 Second, we looked at the state of play in Estonia, which encompassed: (1) identifying instances where strategies and policies in national defence, civil security and safety require inter-agency co-operation; (2) reviewing institutional R&T policies and projects with the purpose of finding potential overlaps of interests; and (3) checking the record of actual co-operation in the two above-mentioned domains. This included desk research on various Estonian policy documents and interviews with policymakers and experts from the MOD, the Ministry of the Interior (MOI), the Ministry of Economic Affairs and Communications (MEAC), the Ministry of Education and Research (MER), the Ministry of Finance (MOF) and their subordinate agencies (the Estonian Defence Forces (EDF), the Police and Border Guard Board, the Rescue Board, the Estonian Internal Security Service, the Estonian Academy of Security Sciences (EASS), the Maritime Administration, the Civil Aviation Administration, the MOI Information Technology and Development Centre (SMIT), the Estonian Information System's Authority, Enterprise Estonia and the Tax and Customs Board).[2]

3.3 Third, we sought to harness expert perspectives on R&T and on specific areas of potential co-operation through a survey questionnaire and a dedicated workshop conducted together with the EASS. This served as a tool to validate

[2] To be truly comprehensive in our approach, we should have also included other governmental stakeholders whose policies and capabilities influence civil security and public safety: the Ministry of Foreign Affairs (which, for example, co-ordinates Estonia's participation in civilian crisis management operations abroad); the Ministry of Justice (and its Prisons Service); the Ministry of Social Affairs (the Health Board is involved in disease and pandemic prevention and response); the Ministry of the Environment (the Environmental Board and the Environmental Inspectorate are involved in environmental emergency prevention and response) and even the Ministry of Agriculture (responsible for food safety and veterinary emergency management). Time limits, however, did not allow us to do that. Future efforts to define dual-use R&T potential, policies and mechanisms should include these organisations.

and refine our recommendations flowing from the previous two strands of research.

4. Our research relied on open sources, which inevitably prevented us from developing insights about inter-agency co-operation in R&T based on classified programmes and plans. In addition, we concentrated on end-user perspectives and steered away from supply-side considerations, even though it should be acknowledged that effective R&T policy-making emerges through dialogue between the two sides. However, at this point, we thought it necessary to help end-users sharpen their thinking about their own requirements and co-operation opportunities before engaging the supply side and exploring 'the art of the possible' with it.

5. Our workshop results should not be expected to cover all aspects of the topic at hand. The workshop included both generalists – capability, technology and acquisition planners – and specialists in particular technologies. The latter group could not possibly encompass all areas of R&T pertinent to national defence, civil security and public safety. Therefore, it is inevitable that some potential co-operation areas were omitted, even though every effort was made with the survey questionnaire and in desk research to address this shortcoming. The workshop was immensely useful, however, for capturing the insights of a diverse multi-agency and multi-disciplinary audience.

6. The paper is divided into four main chapters, each incorporating our findings from all three prongs of research: the first chapter deals with terminology; the second chapter addresses the rationale for an inter-agency approach to R&T; the third chapter zooms in on more specific knowledge and technology domains where the inter-agency approach is necessary and could succeed; and the fourth chapter considers possible business models for pursuing the inter-agency approach. The paper ends with conclusions and recommendations on how and in what areas Estonia could seek to build synergy in R&T investments for national defence, civil security and public safety sectors.

7. We would like to thank all Estonian and foreign experts and decision-makers who made themselves available to share their knowledge and perspectives with us. We are also very grateful to our colleagues at ICDS and the MOD for their valuable comments on drafts of this paper.

I. Terminology issues

8. The departure point for our enquiry into the subject of this paper was the term **'dual-use technology'**. We found it somewhat deficient in two respects:

8.1 'Dual-use' is more commonly employed to refer to technologies that generally have peaceful civilian uses but could also be adapted by potential adversaries to serve their military or security objectives.[3] Thus, 'dual-use' has a connotation of benign and hostile uses of technology, which is certainly not the meaning we have in mind. Accordingly, this is a term often encountered in the context of exports control. As a result, for example, in Ireland the term 'dual-use' is not used to describe the subject of civil-military co-operation in developing new technologies.[4] On the other hand, the term is increasingly popular and widely used in debates at the European level, exactly with the dual

[3] An excellent example of 'dual-use' technology in this meaning is Iran's expertise in concrete that increases the resilience of buildings during earthquakes, but which is now being put to use to enhance the protection of underground facilities that house elements of Iran's nuclear programme against the threat of bunker-busting bombs. See "Smart Concrete," *The Economist*, 3 March 2012, http://www.economist.com/node/21548918.

[4] Telephone interview with Michael Murphy, Enterprise Ireland, 24 January 2013.

– civil security and military – use in mind.[5] For the latter reason and for want of a better term, we adopt the 'dual-use' label, but with the understanding that it denotes technology that can be employed both by civilian – security or safety – and military users for the benefit of civil security, public safety and national defence.

8.2 We are convinced that 'technology' must go hand in hand with **'research'** or, to borrow a part of the definition of 'research and development' by the Organisation for Economic Co-operation and Development (OECD), with 'creative work undertaken on a systematic basis in order to increase the stock of knowledge'.[6] This expands considerably the scope of possible co-operation opportunities between civil security, safety and defence organisations. We therefore prefer to use the term 'research and technology' (R&T) instead of just 'technology' in our paper. Within the 'research' part, we highlight in particular **applied research**[7] projects, addressing the knowledge needs of various civil security, safety and defence organisations. This lays the ground for experimental development of new technology and the subsequent introduction of new applications (products or services), but with more specific capability requirements for different agencies as a driving force. (Indeed, it is suggested that the Technology Readiness Level (TRL) 3, i.e. the 'proof of concept', is the level beyond which technology becomes more specific in terms of its application – be it civil security or military.)[8]

9. We view the scopes of both 'research' and 'technology' in a broad sense. Research encompasses social sciences and humanities as well as natural sciences and engineering; technology is understood not only as components of 'hardware' (equipment and devices), but also as methods and processes (including those related to the human dimension, not only materiel).[9] Again, this broadens the number of co-operation areas and opportunities for civil security, safety and defence stakeholders.

10. It must be noted, however, that when it comes to 'dual-use', most studies – especially EU-funded – narrowly focus on technical R&T, even though EU research programmes (e.g. the Security Research Theme of the Framework Programme) also include research in social sciences (e.g. topics related to behavioural studies, organisational management, etc.). Judging from our interviews with experts and policymakers as well as from the findings of previous ICDS studies, Estonian end-users are similarly technically-minded and, to a degree, hardware-oriented in their understanding of R&T and its expected outcomes. The workshop, however, revealed that the so-called 'soft' aspects (human factors, decision-making, organisational management, resource and capability planning methodologies, etc.) are also considered by the Estonian end-users to be perfectly legitimate fields of research.

11. When speaking about common investments in R&T by civil security, safety and defence organisations, one of the key terms is **'co-operation'**. There is an entire spectrum of possible forms of interaction between organisations from avoidance and

[5] For instance, the European Space Conference 2013 included a session entitled 'Security, Defence and the "Code of Conduct" for Outer Space Activities: The Dual Use of EU Space Programmes and European Space Activities'.

[6] Organisation for Economic Co-operation and Development (OECD), *Frascati Manual: Proposed Standard Practice for Surveys on Research and Experimental Development*, Paris: OECD Publications Service, 2002, p. 30, http://browse.oecdbookshop.org/oecd/pdfs/free/9202081e.pdf.

[7] Defined as 'original investigation undertaken in order to acquire new knowledge. It is, however, directed primarily towards a specific practical aim or objective' (OECD, 2002, p. 30).

[8] French Ministry of Defence, "Informal Paper: Proposal for Dual-Use – Civil and Defence – Issues to Be Proposed for the Inclusion in the European Commission's Forthcoming Research and Innovation Programme," 2011.

[9] For a more detailed elaboration of definitions, see Tomas Jermalavičius, *Estonian Defence Research and Development: Lessons from the Past, Outlook for the Future,* ICDS Report, Tallinn, 2011, pp. 11–12, http://icds.ee/fileadmin/failid/ICDS_Report-Estonia_s_Defence_R_D-September_2011.pdf.

competition to communication (information sharing, awareness enhancement) and co-ordination (the de-conflicting or harmonisation of policies and activities) and then to collaboration and partial or full integration. Co-operation encompasses communication, co-ordination, collaboration and integration (see a chart below) which we see as distinct, though overlapping, forms of interaction.

Figure 1: Continuum of co-operation modes

12. The nature of preferred (or practiced) forms of interaction very much determines the areas and methods of R&T co-operation for various agencies. For instance, if the ambition is only to enhance awareness about what is being done by different agencies, then regular meetings, databases and newsletters are more than enough. The co-ordination of R&T investments across defence, civil security and safety sectors may already require such tools as cross-roadmap reviews of common technology needs.[10] Integration presumes such elements as joint planning, feedback and review, common technology roadmaps, common funding, project management and result-sharing mechanisms (beyond R&T – also joint procurement and maintenance).

12.1 At the European level, for instance, current discussions and agreements (e.g. the European Framework Co-operation for Security and Defence) focus on 'co-ordination' and, to some degree, on 'collaboration' to ensure that military end-users could benefit from R&T conducted under the auspices of the European Commission (EC) and the European Space Agency (ESA), and vice versa, i.e. that civil security and safety end-users could benefit from military R&T run by the European Defence Agency (EDA). This level of ambition is pre-determined by a complex institutional structure at the European level, which makes an integrated civil-military approach in the EC-EDA-ESA triangle very difficult. The same consideration, however, is not, or should not be, so salient at national level, especially in a small country.

13. The aspiration to pursue 'dual-use' R&T implies that there is, among other things, a wish and a need for synergies in developing new knowledge and technology for civil security, safety and defence organisations. **'Synergy'** is one of the most frequently used terms in the debate on 'dual-use' and its rationale.[11] In the civil-military context it means 'a greater effectiveness or efficiency, achieved through combined actions or co-operation between the civil security and the military sectors than would or could be achieved separately'.[12] In practice synergy often comes in a particular form – **spin-offs** and **spin-ins** – defined as 'the application of a technology developed primarily for one sector in the other sector'.[13] This definition suggests that, in practice, much of the technology development across Europe still takes place in the stovepipe of civil security and defence, but both sides are increasingly eager to capture the results of the other side's R&T investments and apply them to meet their own capability requirements.

[10] See Ronald N. Kostoff and Robert R. Schaller, "Science and Technology Roadmaps," *IEEE Transactions on Engineering Management,* Vol. 48, No. 2, May 2001, pp. 132–143.
[11] In a NATO context, the term 'multiplier effect' is more popular, but its meaning is similar to that of 'synergy'.
[12] Ecorys Netherlands, *Study on Civil Military Synergies in the Field of Security,* Final Report for the European Commission DG Enterprise & Industry, Rotterdam, 2012, p. 23, http://ec.europa.eu/enterprise/policies/security/files/doc/study_ecorys_cimisos_final_report_en.pdf.
[13] Ibid.

II. Rationale for an inter-agency approach to R&T and the current state of play

14. The security studies literature is in agreement that the distinction between external and internal security of nation-states has become blurred due to the rise of transnational security issues. Threats arising far from national borders may eventually come to affect internal security, while internal security issues tend to spill over to other countries.[14] There are also a number of security threats that cut across many theoretically distinct security sectors (i.e. political, military, economic, societal and environmental).[15] Threats originating in one sector may have profound implications for other sectors. Examples of such threats are terrorism and insurgency, the proliferation of weapons of mass destruction (WMD), state failure and internal armed conflicts, organised crime, human trafficking, the disruption of critical infrastructure and services (e.g. through cyber attacks or energy supply disruption), climate change and even wildlife crime.[16]

15. The above consensus about the nature of contemporary security threats is well-reflected in the strategic documents of Estonia, the EU and NATO. It is stated in the 2010 National Security Concept of Estonia that 'the impact of political confrontation, economic disputes, competition for resources, religious and ethnic tensions, failed states and non-state actors is often global. Globalisation brings along the entwinement and rapid proliferation of security threats.'[17] The 2003 European Security Strategy maintains that 'the post-Cold War environment is one of increasingly open borders in which the internal and external aspects of security are indissolubly linked' and that 'in an era of globalisation, distant threats may be as much a concern as those that are near at hand.'[18] It is also stressed in the NATO Science and Technology Strategy that 'the line between defence and security is blurring. Indeed the same threats are being encountered in domestic security and external operations, for example Improvised Explosive Devices and cyber attacks.'[19]

16. The probability of a conventional (inter-state) armed conflict is often regarded as low in the post-Cold War era. However, it cannot be entirely discarded. According to Colin S. Gray, 'there will be wars between states […] because they will have a great deal about which to fight.'[20] This observation is valid for the Nordic-Baltic region where Russia's military modernisation, military activities and political hostility are viewed with growing concern. It is stated in the Estonian National Defence Strategy that 'a direct military attack against Estonia is unlikely; however, such a threat cannot be ruled out altogether.'[21] Conventional armed conflicts, just as soft security threats, also reverberate across multiple sectors in terms of their impact. They are not purely military issues that must be dealt with, but also cause disruption and insecurity in the political, societal, economic and environmental spheres.

---

[14] See Derek Lutterbeck, "Blurring the Dividing Line: The Convergence of Internal and External Security in Western Europe," *European Security,* Vol. 14, Issue 2, 2005, pp. 231–253.
[15] For a discussion of threats in distinct sectors of security, see Barry Buzan, *People, States and Fear,* Harlow: Pearson Education Ltd, 1991, pp. 116–134.
[16] The World Wildlife Fund (WWF) has recently linked rampant wildlife trafficking with the funding of civil wars, insurgency, terrorism and state destabilisation in sub-Saharan Africa. See WWF, "Fighting Illicit Wildlife Trafficking," December 2012, http://awsassets.panda.org/downloads/wwffightingillicitwildlifetrafficking_lr.pdf.
[17] Riigikogu, "National Security Concept of Estonia," 12 May 2010, p. 5, http://www.kaitseministeerium.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf.
[18] Council of the European Union, "A Secure Europe in a Better World: European Security Strategy," 2003, pp. 2 & 7, http://consilium.europa.eu/uedocs/cmsUpload/78367.pdf.
[19] NATO Science and Technology Board, "NATO Science and Technology Strategy," 2012, p. 6.
[20] Colin S. Gray, *Another Bloody Century: Future Warfare,* London: Weidenfeld & Nicolson, 2005, p. 178.
[21] Estonian Ministry of Defence, "National Defence Strategy," February 2011, p. 7, http://www.kaitseministeerium.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf.

17. In a similar vein, international intervention and conflict management (or 'out-of-area' operations in NATO's jargon) are not limited to the military domain. Experience from the campaigns in the Balkans, Iraq and Afghanistan amply demonstrates that the addressing of root causes in the political, economic and societal spheres plays an even more crucial role in reaching sustainable long-term resolutions. According to the NATO Strategic Concept, 'the lessons learned from NATO operations, in particular in Afghanistan and the Western Balkans, make it clear that a comprehensive political, civilian and military approach is necessary for effective crisis management.'[22]

18. It is therefore obvious that effective solutions to national security challenges cannot come from separate organisations or even nations. This applies equally to the activities at the stages of threat prevention, active counter-activities and the management of their consequences. The same logic also extends to complex emergencies or crises, to wars and to operations on home soil and abroad. National agencies responsible for managing various security aspects have to reach out beyond their organisational and national boundaries in order to succeed. Concerted efforts by governmental, non-governmental (including the private sector and the academia), inter-governmental and supra-national actors are often the key to resolving national, regional and global security issues. This underlying philosophy is labelled in security studies as 'comprehensive security';[23] in 'out-of-area' crisis management it is commonly referred to as the 'comprehensive approach';[24] and in Estonia's homeland defence discourse it is known as 'broad-based defence'.[25]

19. Even when the management of a security situation falls within the area of responsibility of a particular organisation, its resources might not be sufficient to cope with adverse circumstances. This necessitates the marshalling of the resources of other organisations – be they governmental, public or private, foreign (allied) or national. This whole-of-government, whole-of-society and whole-of-alliance imperative is particularly strong in small states, both in the case of large-scale emergencies or crises and in wartime. In this regard, there must be a leading agency that has to have assured access to resources, capabilities and services of other organisations and to act as an intelligent customer for those organisations: a necessary degree of technical, organisational and human interoperability as well as familiarity with those organisations and their capabilities must be achieved.[26]

20. A paramount implication of all this is that the tasks of various security and defence organisations have become convergent, with the armed forces having to perform some roles of the civil security sector and vice versa. According to an EU-funded study, this is not the case at the higher (i.e. war-fighting) and the lower (i.e. law enforcement and policing) ends of the mission spectrum, but the trend is very strong between these two extremities – it covers crisis management and peace support

[22] North Atlantic Council, "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation," Lisbon, 19–20 November 2010, p. 19, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

[23] See Ann Fitz-Gerald and Don Macnamara, "Comprehensive Security Requires Comprehensive Structures – How Comprehensive Can We Get?" Strategic Studies Working Group Papers, March 2012, http://www.cdfai.org/PDF/Comprehensive%20Security%20Requires%20Comprehensive%20Structures.pdf.

[24] See Crisis Management Initiative, Kristiina Rintakoski and Mikko Autti, "Comprehensive Approach: Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management," Seminar Publication, Helsinki: Ministry of Defence, 2008, http://www.defmin.fi/files/1316/Comprehensive_Approach_-_Trends_Challenges_and_Possibilities_for_Cooperation_in_Crisis_Prevention_and_Management.pdf.

[25] See Estonian Ministry of Defence, February 2011.

[26] See Michael Hallett and Oke Thorngren, "Attempting a Comprehensive Approach Definition and Its Implications for Reconceptualizing Capability Development" in Derrick J. Neal and Linton Wells II (eds.), *Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Interactions,* Washington: NDU Press, 2011, pp. 35–50, http://mercury.ethz.ch/serviceengine/Files/ISN/142718/ipublicationdocument_singledocument/f6211158-d4b8-4e9b-ae68-c719f6e3a404/en/full+text.pdf; Luc van de Goor and Claudia Major, "How to Make the Comprehensive Approach Work?" CPU Policy Brief, No. 21, March 2012, http://www.clingendael.nl/publications/2012/20120404_cru_policy_brief_21.pdf.

operations, the fight against terrorism, border protection, counter-piracy, non-proliferation, responses to natural and industrial disasters, critical infrastructure protection, etc.[27] The same report identifies functions that are shared by agencies involved in high-end security and in defence: (1) detection, identification and authentication (e.g. of vessels, aircraft and individuals); (2) situational awareness, including surveillance (from multiple sources); (3) risk assessment, modelling and impact reduction; (4) communication; (5) information management; and (6) positioning and localisation.[28]

21. The blurring of tasks and the sharing of functions mean that military and civil security organisations have a degree of common interest in similar areas of knowledge and technology, even though the applications derived from those areas may differ. (After all, knowledge and technology are not inherently military or inherently civil security-related, only their applications are.)[29] Even when the nature of missions is divergent, the same equipment and systems could be employed to support military or civil security tasks – either with some customisation or, indeed, without any major modifications (space technology and unmanned aerial systems (UASs) are prime examples of such dual use). In some cases, technology (e.g. communications) serves as a key enabler for inter-agency interaction in managing security threats.

22. While interests are shared, their realisation through R&T and capability programmes is often still stovepiped. At the European level, for instance, R&T projects of relevance to both military and civil security end-users have been run separately by the EC Framework Programme (Security Theme), EDA and ESA. A similar picture emerged, and often continues to emerge, at national level. According to a TNO (Dutch Applied Research Organisation) study, 'while the mutual interests and capability deployments in the defence and security sectors are increasingly converging, the development of common research agendas and programmes is still haphazard.'[30] All this leads to duplication, lack of critical mass and impact as well as financial inefficiency. In times of budgetary austerity, however, financial pressure is becoming a significant driving force for pooling R&T investments and sharing their results between civil security and military organisations. As pointed out by Krzysztof Lisek, a member of the European Parliament, 'the growing impact of the financial crisis in Europe means there is a growing need to hike the complementarities between security and defence.'[31]

23. The overall trend dictated by strategic and financial imperatives is towards a stronger inter-agency/inter-organisational approach in security and defence R&T. At the European level, the EU Commission and EDA build closer links between their research agendas within the European Framework Cooperation for Security and Defence, while EDA and ESA work together on a number of areas of common interest based on an administrative arrangement[32] (see Chapter III for particular co-operation areas). The

[27] See *Istituto Affari Internatzionali* (IAI), Manchester Institute of Innovation Research and *Insitut de Relations Internationales et Stratégiques* (IRIS), "Study on the Industrial Implications in Europe of the Blurring of Dividing Lines between Security and Defence," Final Report, June 2010, http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf.
[28] Ibid, pp. 53–61.
[29] Ecorys Netherlands, p. 24.
[30] TNO, "Development of a European Defence Technological and Industrial Base," Final Report, 2009, p. 146, http://ec.europa.eu/enterprise/sectors/defence/files/edem_final_report_en.pdf.
[31] European Commission DG Enterprise and Industry, "EU, National and Industry Officials Mull How to Promote Stronger R&D Links between Civil Security and Defence Sectors," News, March 2013, http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=6511&lang=en.
[32] See "European Framework Cooperation for Security and Defence Research," EDA Factsheet, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede301109factsheetefcsecuritydefence_/sede301109factsheetefcsecuritydefence_en.pdf; European Commission DG Enterprise and Industry, "European Framework Cooperation in the Field of Research," News, 20 September 2011, http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5413&lang=en; and "EDA & Space," EDA Factsheet, http://www.eda.europa.eu/docs/documents/factsheet_-Defence_space_final.pdf.

practice of defining common knowledge, technology and capability needs is taking root at national level in various countries: the Netherlands,[33] the United Kingdom,[34] Slovenia,[35] Poland[36] and Canada across the Atlantic.[37] Even in countries where traditions and long-standing policies previously dictated a strict separation of military and civil security activities (e.g. Ireland)[38] or the dominance of one sector over the other (e.g. the military sector, as in Finland),[39] there is a clear trend towards a stronger inter-agency approach to R&T.

24. In Estonia, the need for an inter-agency approach to tackle a range of security challenges is well-appreciated at the policy level. The National Security Concept calls for the improvement of 'joint planning for situations which require efficient co-operation between state authorities and other parties. This requires clarity in management and planning, prompt decision-making, specified competencies of state authorities as well as their readiness to draw on the capabilities and resources regardless of their affiliation.'[40] It is clearly stated in various sectoral strategies and policies, such as the Cyber Security Strategy, the Main Guidelines of Estonia's Security Policy until 2015 (an internal security policy document), the National Defence Strategy, the Emergencies Act and the Fundamentals of Counter-Terrorism in Estonia, that the threats and risks that they address are not matters to be dealt with by a single organisation. Comprehensive security and broad-based defence, enshrined in Estonian strategic thinking, constitute an unassailable strategic rationale for governmental agencies in civil security, public safety and national defence to work together in fulfilling their functions.

25. In practice, as our research and workshop revealed, the picture is mixed. On the one hand, there are many positive common activities such as mutual involvement in exercises and operations, the exchange of information and mutual support with capabilities:

25.1 Cyber security is perceived as a veritable success story from highly effective inter-agency and public-private defence actions against the 2007 cyber-attacks to current routine interactions (e.g. exercises and simulations), involving military, civil security, public research and private organisations;

25.2 Civilian agencies successfully participate in military-run host nation support exercises (e.g. Baltic Host) and, vice versa, military personnel take part in crisis management/emergency response exercises run by civilian authorities. Police authorities routinely use the modelling and simulation capabilities of the military;

[33] See Pieter J. Keuning, "R&T for Defence, Security and Safety: Experiences from the Netherlands," Seminar Presentation, Tallinn: Academy of Sciences, 20 September 2010, http://icds.ee/fileadmin/events/2010-09-20-interagency/Pieter%20J%20Keuning-Director%20R%26D-Netherlands%20MOD.pdf.
[34] See UK Ministry of Defence, "National Security through Technology: Technology, Equipment, and Support for UK Defence and Security," White Paper, London: The Stationary Office Limited, February 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf.
[35] E-mail interview with Davor Kozmus, Slovenian Ministry of Education, Science, Culture and Sports, 15 January 2013.
[36] Marek Kalbarczyk, "Polish Defence and Security R&T System: Structures, Financing, Projects, Lessons Learned," Seminar Presentation, Tallinn: Academy of Sciences, 20 September 2010, http://icds.ee/fileadmin/events/2010-09-20-interagency/Col%20Marek%20Kalbarczyk-NATO%20RTO%20coordinator-Polish%20MOND.pdf.
[37] Robert Walker, "Interagency Approach to R&T for Defence, Security and Safety: NATO and Canadian Perspectives," Seminar Presentation, Tallinn: Academy of Sciences, 20 September 2010, http://icds.ee/fileadmin/events/2010-09-20-interagency/Dr%20Robert%20Walker-Chairman-NATO%20RTB.pdf.
[38] Telephone interview with Michael Murphy, Enterprise Ireland, 21 January 2013.
[39] Mika Hyytiäinen, "Dual Use in R&D: Some Finnish Experiences," Workshop Presentation, Tallinn: Academy of Security Sciences, 21 February 2013.
[40] Riigikogu, p. 9.

25.3 Radar data from the network of civilian radars is used by the military for their air surveillance tasks. There is also co-operation between the military and the border guard in maritime and air surveillance;

25.4 Assets of the EDF (e.g. pioneer equipment, logistics trucks, boats and helicopters) and the National Defence League are often deployed to assist civilian authorities in rescue/emergency response operations (e.g. fighting forest fires and responding to floods);

25.5 There have been several instances of co-operation that have demonstrated that civilian and military authorities can respond to the operational needs of each other and are able to act together when necessary (e.g. the response to the 2007 riots and public disturbances; security operations related to a NATO ministerial meeting and the delivery of euro notes to Estonia; an operation involving a cargo airplane that crash-landed on a lake in Tallinn; and the evacuation of hundreds of people stranded on a highway during a severe snow storm– all in 2010).

26. On the other hand, capability planning and development are still very much stovepiped in various agencies, despite some tentative efforts to broaden the number of external stakeholders. For instance, when the latest ten-year National Defence Development Plan (2013–2022) was prepared – which was done well in the spirit of broad-based defence – civilian agencies did participate, but only in the initial stages. Later on, differences in their approach to capability planning, the lack of a common methodology and other factors led to back to the defence/military stovepipe. (Conversely, civilian agencies such as the Police and Border Guard Board and the Rescue Board hardly ever involve the military in their capability planning processes.) Indeed, security and defence agencies have very limited awareness of each other's needs, plans, priorities and ways of implementing them. There is no culture or established practices or processes for integrated (inter-agency) capability planning – or at least for co-ordination and harmonisation – to ensure that unnecessary duplication (or capability gaps) is avoided and a high degree of inter-agency interoperability is achieved.[41]

27. In general, it is thought that 'some segments of the security sector are characterised by weak demand side capacity to identify their capability requirements and/or to understand the capabilities that a particular technology can deliver or to recognise the benefits of innovative approaches.'[42] In Estonia, this observation rings true not only in relation to civil security organisations but to defence end-users as well.[43] It is therefore difficult to expect the two groups of end-users – military and civilian – to come together for joint capability planning, technology roadmapping and innovation (thus creating a demand-side pull for R&T), while both groups have their own difficulties in this area. On the other hand, this opens opportunities for joint building of necessary competence and capacities (e.g. in technology management, planning methodologies and innovation management).

28. Nonetheless, instances of inter-agency interaction at the stage of national security and defence capability development are already emerging not only in

[41] A reasonable argument can be made that, in terms of resources, domestic inter-agency co-operation often competes with international (military-to-military, security-to-security) co-operation that involves the fulfilment of EU and NATO benchmarks and collective requirements (the latter form of co-operation is easier because it engages similar organisations from different nations). Inevitably, a small administrative apparatus (i.e. an agency) frequently gives priority to international co-operation. The true art of comprehensive security and broad-based defence is to achieve a situation where the international (whole-of-alliance) and domestic inter-agency (whole-of-government) dimensions effectively supplement each other.

[42] ECORYS, p. 87.

[43] See Jermalavičius, pp. 50–51.

operational sharing and mutual support, e.g. the EDF's (more specifically, the Navy's) participation in the development of a maritime surveillance system, led by civilian authorities. The new Estonian Defence Industrial Policy 2013–2022, unveiled by the Estonian MOD in February 2013, envisages the MOD's, the MOI's and their subordinate agencies' co-ordinated input into the development of new technology, products and services by the Estonian industry.[44] Thus industry initiatives might open the gates for progress in adopting the inter-agency approach also to capability planning and development because governmental organisations will have to respond to those initiatives in a co-ordinated manner.

29. By extension, a similar situation in terms of inter-agency interaction emerges in the field of R&T, which is further aggravated by R&T-specific issues:

29.1 Among the ministries and agencies that are of key interest to us, only the MOD has an institutional (and by now long-standing) R&T strategy, a dedicated budget for its implementation[45] and a central co-ordinating authority. Indeed, the MOD puts a strong emphasis on the dual-use principle during the implementation of the strategy.[46] The MOD processes for the definition of R&T needs and for project launching, however, do not include specific points for informing, consulting or co-ordinating with other ministries or civil security and safety agencies (with the exception of co-ordination with the MER and the Estonian Research Council on competence-building projects with universities). If information is exchanged or consultations conducted, it is mostly done on an ad hoc basis.[47]

29.2 The MOI has a fairly rudimentary policy which encourages private companies to demonstrate their ideas, but they have to bear project costs and risks themselves, while the MOI tests and evaluates results and provides feedback. The EASS, however, adopted its research and development strategy in March 2013 which is as close to an institutional R&T strategy for the MOI's entire area of government as it gets. The strategy also captures the knowledge and skill requirements for the agencies under the MOF (the Tax and Customs Board) and the Ministry of Justice (the Estonian Forensic Science Institute and the Prisons Service).

29.3 Our survey suggests that most civil security and safety agencies subordinated to the MOI or the MEAC do not have their own R&T strategies and they allocate assets for this field only on an ad hoc basis (often without any co-ordination between themselves, let alone with the military).[48] Accordingly, the R&T culture is underdeveloped and the same applies to deep expertise and structured processes for the definition, harmonisation and implementation of R&T requirements (which is quite typical of many civil security agencies across Europe).[49]

[44] See Estonian Ministry of Defence, "Defence Industrial Policy 2013–2022" (in Estonian), February 2013, http://www.kmin.ee/files/kmin/img/files/Eesti_kaitsetoostuspoliitika_2013-2022.pdf.
[45] It falls considerably short of the NATO and EU target of 2% of defence costs: as of 2012, spending was at the level of 0.37% (although not all R&T activities performed by defence organisations are reflected in the defence investments area, so the actual figure is somewhat higher).
[46] For instance, the dual-use principle guides the decisions on participation in the R&T projects of the EDA. See Ministry of Defence, "Principles of Participation in Research and Technology Activities of the European Defence Agency" (in Estonian), Minister's Decree No. 332, 1 November 2012.
[47] For example, the MOD consulted with the Rescue Board's demining experts on their knowledge requirements when it started to participate in the EDA project which included research in the field of munitions toxicology.
[48] For this reason, it is impossible to provide a clear figure on how much the MOI and the MEAC spend on security and safety-related R&T on a year-to-year basis.
[49] See IAI, Manchester Institute of Innovation Research and IRIS, pp. 107–109.

29.4 None of the organisations covered in this paper view R&T as a matter of strategic importance, unlike, for instance, the UK government which regards it as a means to avoid strategic surprise, to enable the adoption of an intelligent customer posture, to retain technological advantage and to maintain strategic and operational sovereignty.[50] However, our survey reveals that Estonian organisations still considered R&T to be crucial in at least two fundamental respects (a perception that is not really backed by policies and funding commitments): (a) for the acquisition of new knowledge and increasing their organisational competence; and (b) for the enhancement of existing capabilities, the acquisition of new ones and the prevention of their obsolescence. The significance of R&T is also underlined in the new Estonian Defence Industrial Policy 2013–2022.

30. Even in this disjointed environment characterised by R&T's undeservedly marginal role, there have been quite a few dual-use R&T projects, implemented by the defence side or by the civil security side (sometimes duplicating one another) or conducted under enterprise support schemes run by Enterprise Estonia. In some cases, the results produced successful spin-offs from the defence sector to the civil security side. Furthermore, there are projects that are being launched with extensive participation by civil security, safety and defence stakeholders (e.g. the BIAS LIFE project on underwater acoustics monitoring). However, as one workshop participant noted, 'there is a clear recognition both at the political and the expert levels that an inter-agency approach to R&T is necessary; yet something happens to this goodwill between the two levels.'

31. The situation should be greatly facilitated by a fact that almost all governmental organisations involved in civil security, public safety and defence draw upon a common R&T supply base – Estonian civilian universities, research centres and enterprises – as opposed to their own in-house research establishments (with the exception of some research carried out at the EASS and the Estonian National Defence College (ENDC), but even these research efforts are often linked with competences and activities at civilian universities). The exploitation of the same supply base means – at least in theory – that: (a) military and civil security applications are derived from the same sources of national expertise (the same people, and their networks, who do not specialise solely in military or solely in civil security R&T) and (b) the range of these applications will always reflect (and will be constrained by) the underlying strengths of the Estonian civilian R&T sector in particular areas of knowledge and technology.

32. It is unclear whether or not the demand side will be able to organise itself in order to sustain, strengthen and harness this common base in a co-ordinated, effective and efficient manner. A similar question – will the end-users be able to organise themselves properly and 'pool' their demand? – arises in cases where they cannot draw upon national expertise (due to its absence) and need to contract foreign R&T suppliers.[51] The answer largely depends on whether or not the end-users manage to identify the areas in which they have shared interests (which is the subject of the next chapter) and whether or not they deploy suitable mechanisms to pursue these interests nationally or internationally (which is discussed in Chapter IV).

[50] See UK Ministry of Defence, pp. 26–28 & 34.

[51] Indeed, mechanisms for tapping into the knowledge and technology base of foreign allies and partners are crucial – they should receive much more attention, given that Estonian experts cannot possibly cover in-depth all key areas in national defence, civil security and public safety. End-users should remain open-minded about the sources of supply, instead of regarding Estonian R&T organisations as their exclusive demand-side partners.

III. Potential areas for dual-use R&T

33. The success of the inter-agency approach to R&T partly hinges on the achievement of a consensus between defence, civil security and public safety stakeholders regarding the areas of focus.[52] We combined several methods to determine the potential breadth of dual-use R&T in Estonia. Each of the following thrusts has various limitations if taken individually, but their combinations allowed us to develop a reasonably comprehensive picture of which R&T areas could be regarded as candidates for inter-agency measures by Estonian defence, civil security and safety organisations. Our activities were the following:

- We examined the findings of various EU-funded studies about dual-use R&T trends in Europe;
- We looked into the agenda of co-operation between the EC, EDA and ESA and examined NATO's R&T priority objectives;
- We considered national dual-use R&T agendas and experiences in various EU and NATO countries;
- We extracted clues about R&T areas of relevance from Estonian national security and defence policy documents;
- We reviewed past and present dual-use R&T investments/projects in Estonia;
- We examined the very few existing institutional R&T strategies and policies in the civil security and national defence sectors;
- We captured national expert perspectives through interviews, a survey questionnaire and a workshop.

34. The study on the industrial implications of the blurring of dividing lines between security and defence has identified the following technologies on which the interests of military and civil security end-users coincide (and which are indeed the technological drivers for blurring):

- Structural materials/technologies and structural effects analysis, with an underlying shared interest for military, civil security and safety end-users in strengthening physical installations against the impact of explosions;

- Photonic/optical materials and device technology, given their numerous applications in infra-red (IR) sensors, navigation, search and rescue, mine laying/detection and Command and Control;

- Sensor (esp. hyperspectral/multispectral, IR, acoustic and optical) technology and components, driven by shared civil-military interest in their application for border/area/point surveillance, CBRN-E substances detection, etc.;

- Electronic components as a generic technology with multiple applications across the civil security and defence sectors;

- Signal processing, information, computing and communication technologies, which are critical for interoperability in comprehensive security and broad-based defence missions;

[52] Raffaele Esposito, "Interagency Research and Technology Strategy for Defence, Security and Safety: The Industrial Point of View on Problems and Opportunities," Seminar Presentation, Tallinn: Academy of Sciences, 20 September 2010, http://icds.ee/fileadmin/events/2010-09-20-interagency/Dr%20Raffaele%20Esposito-Honorary%20Chairman-NIAG.pdf.

- Information security technologies, which are crucial in protecting both civilian and military networks;

- Simulation tools and software, particularly those applied in tactical/crew training systems, command and staff training systems and synthetic environments. Military, civil security and safety end-users increasingly rely on such tools to cut their training costs;

- Human sciences, particularly technologies that can be applied for human behaviour analysis and modelling, which are relevant to both civil security (e.g. in anti-terrorism, riot control and other functions) and military (e.g. in peace support operations) organisations;

- Biotechnology, especially technologies that allow for the rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques – all of which are essential for military operations in hostile areas and for the protection of civilian populations.[53]

35. The same study also outlines a number of emerging technologies which will be additional drivers for blurring between civil security and military functions and which will be exploited by civil security, safety and defence organisations. These are concentrated in the fields of nanomaterials (for applications in CBRN-E detection, force protection, computing, imaging, etc.) and nanotechnologies; communications (wired/wireless, secure, etc.); semantic web technologies (to harness the internet for actionable intelligence and to support decision-making); autonomous self-organised networks of smart sensors (to build a comprehensive picture of an operating environment); and energy storage and distribution (e.g. miniaturised energy sources).[54] This adds a valuable forward-leaning perspective to the potential R&T agenda, which is necessary for preventing strategic surprises and for gaining the technological edge in a dynamic threat and risk environment. At a more basic research level, it also provides for the inter-agency approach to 'technologies whose applications for either civil security or defence are still unknown.'[55]

36. The ECORYS study focused on identifying the areas in which technology synergy between the civil security and defence sectors have been most frequent till now or where the potential of such spin-offs is deemed most promising by the experts. The paper concluded that these were, almost invariably, the areas of sensor technologies, C3 (Command, Control and Communications) and cyber security.[56] In addition, the study pointed out that joint R&T activities performed by civil security and defence organisations is one of the facilitating factors for future spin-offs and spin-ins (along with similar operational needs, technology maturity level and market characteristics). It allows both military and civil security end-users discuss their needs and requirements at an early stage and it helps to develop a culture of working together. According to the study's findings, joint R&D efforts across European countries were concentrated, yet again, in the fields of C3 and cyber security as well as in space and CBRN-E protection technologies.[57]

37. The EC and EDA have formally agreed within the European Framework Agreement to pursue CBRN protection as a 'mature research topic' to co-operate on.

[53] IAI, Manchester Institute of Innovation Research and IRIS, pp. 78–81.
[54] Ibid, pp. 84–86.
[55] See European Commission DG Enterprise and Industry, News, March 2013.
[56] See ECORYS, p. 75.
[57] Ibid, p. 74.

The two organisations have also declared their intention to add the topics of UASs and situational awareness (including sensors, information management and cyber security) to this agenda in the future.[58] They have also previously co-ordinated their activities in underwater research and explosives' detection technologies.[59] EDA and ESA have of their own accord agreed to co-operate in the fields of ISR (Intelligence, Surveillance, and Reconnaissance), satellite communication (in support of UASs), Earth observation, space situational awareness and critical space technologies for European non-dependence.[60]

38. After performing an analysis of Priority Shortfall Areas in the Alliance's capabilities, NATO Allied Command Transformation has identified a set of R&T objectives in those areas. Although the analysis clearly kept military applications in mind, it can be argued that the results of R&T efforts in those areas would be highly relevant to civil security and public safety end-users. These include:

- Novel training systems, techniques, tools, technologies, strategies and organisation;
- Language translation technologies and training;
- Non-kinetic effects in the human environment and information domain (protection and consequences management);
- Kinetic effects of ballistic missiles, CBRN-E, Improvised Explosive Devices (IEDs) and natural and man-made disasters (protection and consequences management);
- Situational awareness (intelligence) in all domains and information sharing;
- Collaboration culture and expertise management;
- Adaptive systems and capabilities;
- Energy consumption efficiency;
- Low-cost autonomous solutions (platforms, sensors, effectors and system integration).[61]

39. Individual nations pursue dual-use R&T within a rather narrow circle of themes (which are difficult to compare due to major differences in levels of detail available about particular technologies of interest).[62]

39.1 In the Netherlands, defence, security and safety R&T has five focus areas: (1) Observation Systems (radar and electronic defence, electro-optics and sonars); (2) Information and Operations (operational analysis, purchase and exploitation; Modelling, Simulation and Gaming; Network Enabled Capabilities; and surveillance, maintenance and training); (3) Protection, Munitions and Weapons (weapons systems, personal protection and survivability, high performance energetics); (4) CBRN-E Protection (threat and protection, chemical and biological detection, identification, diagnosis and therapy, physical protection and tests); and (5) Human Factors (intelligent interfaces, perception and simulation, human in command, human performance, traffic behaviour, training and instruction).[63] Although some R&T elements mainly support defence or civil security applications, the use of the integrated approach means

[58] See European Commission DG Enterprise and Industry, News, 20 September 2011.
[59] See European Commission DG Enterprise and Industry, News, March 2013.
[60] European Defence Agency, "EDA and Space," EDA Factsheet, 17 June 2011, http://www.eda.europa.eu/docs/documents/factsheet_-Defence_space_final.pdf.
[61] NATO Allied Command Transformation, "From PSAs to S&T Objectives," presentation in the possession of the authors.
[62] The ECORYS and the IAI, Manchester Institute of Innovation Research and IRIS studies covered a number of EU member states, some of which are also listed in this paragraph.
[63] See Keuning, 2010.

that benefits flow in both directions (from defence to civil security and from civil security to defence). Examples of defence spin-offs to civil security include extending new knowledge about soldier effectiveness to the functioning of first responders; using the design of combat operations centres to design security and safety control rooms; and applying knowledge about explosives detection techniques. Civil security research also benefits the military, the examples being: public area camera surveillance in urban operations; new materials in compound and vehicle protection; new communication technologies in the protection of military C3 networks; sensor concepts in military UAV (unmanned aerial vehicle) and space applications; and fireworks safety research helping to improve munitions storage.[64]

39.2 Finland's examples of dual-use (or multi-use, as is the preferred term in Finland) R&T and capability development investments include C3 (VIRVE TETRA-radio communications for all homeland security actors; Software Defined Radio), situational awareness (the Maritime Environment Tri-Authority Operations system) and information management projects. Potentially, UASs could be added to these, although presently only the military can purchase, own and operate them.[65] In addition, the Scientific Advisory Board for Defence (MATINE) funds projects at TRL 1-2 the outcomes of which can be applied in civil security or public safety. The areas include: sensors and environment; electronics; software and telecommunications; materials and production; machine building and structures; system analysis; CBRN and medicine; social sciences; health and human factors.[66]

39.3 Norway's examples of harnessing defence research and technology expertise (concentrated mainly in its Defence Research Establishment (FFI)) for civil security and safety purposes include: CBRN; Critical Infrastructure Protection (vulnerability assessments for the telecommunications, energy and transport sectors; critical information systems protection); Crisis Management (including scenarios and emergency preparedness assessments); and space technology for Earth observation.[67] However, FFI's R&T competences in such areas as information management (e.g. C3, modelling and simulation), air systems (e.g. UAVs), maritime systems (e.g. unmanned undersea vehicles, sonars, undersea surveillance and surveying the marine environment) and protection technologies (e.g. environmental and physical protection) could equally be exploited for civil security and safety objectives.

39.4 In Ireland, it is not definitively clear whether or not the results of R&T projects are largely dual-use or not ("we are 'agnostic' in this regard", as the interviewee put it), as the respective decisions are mostly driven by opportunities in civil security or defence markets and the availability of EU funding. However, the projects undertaken usually reflect the inherent strengths of the country's research and industry base (mainly information and communication technology (ICT)) and the expertise of end-users (e.g. CBRN-E, especially explosives). Technologies that make it possible to tap social media for

[64] Ibid.
[65] Hyytiäinen, 2013.
[66] Presentation by Pekka Appelqvist, Secretary General of MATINE (Helsinki: Ministry of Defence), 3 June 2013.
[67] Paul Narum, "Defence and Security R&T in Norway," Seminar Presentation, Tallinn: Academy of Sciences, 20 September 2010, http://icds.ee/fileadmin/events/2010-09-20-interagency/Dr%20Paul%20Narum-Director%20General-FFI.pdf.

intelligence data gathering have also been flagged as being of interest to civil security and defence end-users.[68]

39.5 Slovenia's potential for dual-use R&T is mostly concentrated in fields that have received the largest amount of national and international support and that represent the country's scientific and technological strengths. These lie in machine engineering, micro- and nanotechnologies, ICT and biotechnology.[69]

39.6 Across the Atlantic, Canada's inter-agency defence, security and safety R&T agenda encompasses four themes: (1) CBRN-E; (2) Critical Infrastructure Protection, including vulnerability assessments and monitoring, resilience, disaster alert and mitigation and cyber security; (3) Surveillance, Intelligence and Interdiction (SII), including integrated communications, intelligence and surveillance, maritime/border/transportation SII and forensics; and (4) Emergency Management Systems and Interoperability, including risk and vulnerability assessments, interoperability, standards, modelling and decision support and human factors.[70]

40. We have analysed a number of policy documents that govern Estonia's national security and defence, including the National Security Concept (2010), the National Defence Strategy (2010), the Main Guidelines of Estonia's Security Policy until 2015 (including implementation reports), the Cyber Security Strategy (2008) and the Fundamentals of Counter-Terrorism in Estonia (2006). Although none of them explicitly refers to specific priority areas of R&T, they still contain a number of clues about scientific knowledge and technology of relevance to various national security objectives and functions.[71] We have derived the following areas in which civil security, public safety and national defence end-users could have shared interests in Estonia:

- Command, control, communications, computer and information (C4I) devices, systems and networks, their integration/interoperability and protection/security (cyber security);
- Surveillance devices, platforms, systems and their integration for maritime/air/land(area)/point monitoring and object detection, localisation, identification and tracking;
- Crisis/emergency modelling, simulation, gaming and training, software solutions, data collection and management, human-machine interfaces, etc.;
- CBRN-E, especially the 'C', 'R' and 'E' parts of it, for substance monitoring, detection, analysis and decontamination/neutralisation;
- Physical protection of personnel and infrastructure;
- Human factors – physical, mental and psychological performance and resilience, behavioural science and sociology, organisational behaviour and management, human source intelligence gathering, social networks, etc.;

[68] Murphy, 2013.
[69] Kozmus, 2013.
[70] Walker, 2010.
[71] Most of these documents come up for review in 2013–2014. It is, however, quite unlikely that this will lead to the inclusion of more coherent and elaborate principles on technology policy or R&T priorities. In our view, it is also unlikely that these reviews will radically alter our analysis of the directions and areas of (dual-use) R&T.

- Risk assessment and management, resource and capability planning methodologies.

41. As we have pointed out earlier, the EASS is one of the very few genuinely inter-agency hubs for education, training, research and technology in Estonia.[72] It has set out to advance its R&T competence in a number of areas, some of which could also be of relevance to defence end-users, such as:

- Crisis management;
- Preventive surveys, high-risk behaviour and information measures;
- Risk management and civil defence;
- Effectiveness of in-service training;
- Financing models and resource planning;
- Innovative educational techniques;
- Development of professional terminology and language technology;
- Development of human resources and personnel management.[73]

42. Safety and security (prevention of emergencies, crisis management and communication, maritime safety and the protection of citizens) constitute one of the key priorities of Estonian space policy.[74] Although the MOI has been tasked with leading the development of applications to address this priority, defence end-users could benefit from them as well. Such applications will most likely concentrate in three areas:

- Surveillance, monitoring and geo-information (related to the Earth observation initiative 'Global Monitoring for Environment and Security', which has a security and defence dimension);
- Positioning, localisation, tracking and navigation (related to the forthcoming European satellite navigation and positioning system 'Galileo' and associated functions aimed at improving the accuracy of positioning systems);
- Access to and use of meteorological information (related to the services provided by the EUMETSAT via the Estonian Meteorological and Hydrological Institute).

43. The Estonian MOD's Research Council has produced a rather extensive list of technological competences of interest to defence (including a total of 35 competences). These are grouped into three larger areas: (1) situational awareness, systems, system integration, information management (including information assurance) and decision-making; (2) force protection and sustainment; and (3) human factors and medicine.[75] It is planned to formally identify these areas in the new defence research and development strategy as priorities and as specialist niches within NATO and the EU, with a strong emphasis on the dual-use principle. These three broad areas and the technological competences within them evidently include what we have derived from

[72] The EASS educates and trains police, border guard and rescue personnel (who work for agencies under the MOI), customs personnel (under the Ministry of Finance) and prison services personnel (under the Ministry of Justice). In the early 1990s, it was called the State Defence Academy and thus it also offered training to military officers.
[73] See Estonian Academy of Security Sciences, *Research, Development and Innovation Strategy of the Estonian Academy of Security Sciences till 2015* (in Estonian), 4 March 2013, p. 3, http://sisekaitse.ee/public/Teadus-_ja_arendus/SKA_TAL_strateegia_kinnitatud.pdf.
[74] See Ministry of Economic Affairs and Communications, *Strategy for Estonian Space Affairs 2011–2013,* 2012, p. 21, http://www.eas.ee/images/doc/ettevotjale/innovatsioon/kosmos/estonian-space-strategy-2011-2013-booklet.pdf.
[75] Jermalavičius, pp. 25–26.

the national security and defence policy documents and listed in the previous paragraph.

44. Our survey tested to what extent civil security and safety organisations are keen on those technology competences that are of interest to defence. Although imperfect (and revealing a rather techno-centric attitude that focuses on hard sciences), the results still give us an indication of the convergence points between the interests of end-users in the civil security and safety sectors and in defence organisations. Having received the highest grades for current and future relevance and the highest number of 'hits' from the respondents, the top five technology competences are:

- Sensors (radio-frequency, optical, sounder, pressure, seismic, magnetic, electrical, chemical and biological);
- Radars;
- Sensor networks, cognitive signal processing and data fusion;
- Communication systems (including their interoperability);
- Network-enabled capabilities.

45. Many past and current R&T projects funded by the MOD – the ministry with the most advanced policy and record of R&T investments – are of a dual-use character. Indeed, the results of those investments have already been successfully deployed for civil security and safety uses (e.g. sensors for border surveillance, jammers for countering IEDs and simulation software for defence against cyber attacks). Furthermore, the MOD remains very positive about the use of the results of other past projects by other ministries and agencies. In our view, there are numerous past projects that could yield new knowledge and technology useful not only for defence but also for civil security and safety end-users. These projects involve:

- A universal Unmanned Ground Vehicle;
- An UAV;
- A portable analyser of chemical agents;
- Protection against radiation;
- Adaptive camouflage;
- Light armour panels for transportation vehicles;
- UAV observation data processing;
- Network-based capabilities and spontaneous networks;
- Radio communication technology;
- A digital radar;
- GPS (Global Positioning System) usage for obtaining meteorological data;
- Personnel performance in chronic heat conditions;
- Psychological tests for personnel selection.[76]

46. Finally, our interviews with experts and planners, together with the expert workshop, re-affirmed that there are overlapping interests in C4I, surveillance, sensor, cyber security, CBRN-E, modelling and simulation technologies. It also transpired that civil security, safety and defence end-users shared interests in new knowledge, technology and applications related to the use of UAVs (e.g. enabling their introduction into managed airspace) and space-based assets (e.g. in geo-information systems). As one workshop participant noted, 'space technology is inherently dual-use.' Last but not least, a less techno-centric side of the end-user community emerged, with indications of

[76] The full list of the MOD's past R&T projects is available in Jermalavičius, pp. 23–24. It should be noted that even projects with very clear military applications (e.g. assessing the soil crossing ability of heavy military vehicles) could have yielded knowledge relevant to civilian users as well, although this might not always be evident straight away.

a strong shared interest in human factors, in methodologies for supporting better planning and decision-making (e.g. resource and capability planning, foresight, risk and impact assessment, system and operational analysis) and in novel approaches to training and education.

IV. Business models

47. There are a number of different business models for implementing dual-use R&T, the choice and details of which depend on ambition and context. In their pure form, the models could be divided into four broad (and somewhat overlapping) categories:

47.1 A **fully integrated** business model for civil security, safety and defence R&T presupposes that end-user organisations do not conduct their own (stovepiped) R&T at all and totally rely on joint R&T strategies and roadmaps; on joint planning, decision-making and funding structures and processes; and on a common knowledge and/or innovation brokering hub. We did not find any examples that reflected this ideal in its entirety, but several countries came quite close through **partial integration**. For instance:

47.1.1 In the Netherlands, the MOD, the Ministry of Justice and the MOI draw up common knowledge requirements and channel them – together with the required funding – to the specialised defence, security and safety arm of the Netherlands Organisation for Applied Scientific Research (TNO). However, every ministry still has its own knowledge needs which it may address either through TNO (and not necessarily through its defence, security and safety division) or by sourcing from other (even non-Dutch) knowledge suppliers.[77]

47.1.2 In the UK, the defence and home affairs departments use the National Security Strategy and Strategic Defence and Security Reviews as a basis for a common policy on technology, equipment and support. Again, this does not exclude individual approaches if their capability needs diverge, but the aspiration is to jointly build, support and exploit the national knowledge and industrial base for defence and security purposes, with a ministerial working group ensuring adherence to the whole-of-government approach at the policy level. There has also been some progress towards integrated implementation (e.g. by extending the remit of the Centre for Defence Enterprise – the innovation brokering hub for defence – to security technology and industry).[78]

47.1.3 In Poland, security and defence R&T activities are integrated through the National Science Council (up to TRL3) and the National Research and Development Council (TRL4 to TRL9) under the Ministry of Science and Higher Education. The Ministry of National Defence and other ministries (and industry representatives) participate in the steering committees of the councils which run the so-called national projects. Instead of advancing stovepiped agendas (even though institutional projects are still possible and pursued to address purely defence-related needs), institutional R&T strategies (e.g. that of the

[77] See Tomas Jermalavičius, "Defence R&D: Lessons from NATO Allies," ICDS Report, 2009, http://icds.ee/fileadmin/failid/Report-Defence_R_D-Lessons_from_NATO_allies.pdf.
[78] See UK Ministry of Defence, 2012.

Ministry of National Defence) aim to ensure that institutional needs are properly reflected in national projects, that co-operation with the leading ministry (the Ministry of Science and Higher Education) is appropriate and that international co-operation (e.g. in EDA and NATO projects) is intensive.[79]

47.2 A **collaborative model** presupposes that organisations draft their own institutional R&T strategies and roadmaps which are implemented through separate (often in-house) knowledge brokering hubs (R&T institutes, laboratories and centres). However, the organisations come together to issue common requirements and pool resources for joint projects when inter-agency imperatives are very strong or when a national security strategy requires their close operational collaboration (or when the critical mass needed for the implementation of an R&T project has to be achieved). It is also quite common to cluster different knowledge brokering hubs (together with business enterprises) at the same location in order to facilitate their interaction. Collaboration may be temporary and ad hoc (i.e. it occurs whenever opportunities are spotted by the two sides in any field of interest, leading to co-operation for a limited period) or it may be more structured, even with elements of partial integration (i.e. it focuses on particular areas of R&T over a longer period). In our view, this model is best illustrated by Finland.

47.3 A business model focused on the **co-ordination** of separate institutional R&T strategies presupposes constant comparison and harmonisation of institutional needs, plans and roadmaps of defence, civil security and safety end-users, together with the definition of common standards in selected areas. The aim of such activities is to avoid the duplication of investments, the issuing of conflicting requirements to the same suppliers and the development of incompatible solutions for similar functions of different agencies. This is a rationalised form of stovepiping – one which allows an organisation to benefit from the expertise and results of its sister organisations, while maintaining an independent R&T agenda to serve its own needs. Although European organisations – **the EC, EDA and ESA** – have introduced elements of a more collaborative approach, they are mostly confined to the co-ordination and harmonisation of their activities (mainly due to various idiosyncrasies found at the European level of co-operation and in their institutional make-up).

47.4 Finally, at the opposite end of the co-operation spectrum from full integration, there are business models that primarily focus on **awareness and exchange**. Their choice could be determined, for instance, by reluctance to carry the additional administrative burden associated with closer inter-agency co-operation in R&T, by the lack of a cooperation tradition or by a heavy dominance of one organisation (e.g. defence) in terms of its R&T investments, the scope of its agenda and its experience with R&T matters. This model, however, implies readiness and ability to spin-in/spin-off R&T results and competences for further use (adaptation) in separate sectors (which, in turn, pre-supposes a degree of openness to such exchanges, including in intellectual property rights management and information protection requirements). In our opinion, Norway practices a version of this model.

48. It seems reasonable that elements of these four models can coexist at the same time in the inter-agency approach to defence, security and safety R&T. For instance, a joint (integrated) R&T strategy and roadmap may be drawn up only for a select area of

[79] See Kalbarczyk, 2010.

blurred functions (e.g. crisis and emergency management) or for a knowledge and technology area with the highest degree of common interest (e.g. cyber security), while other activities mostly concentrate on co-ordination or even simply maintaining awareness. In a similar vein, the co-ordination model may include projects of a collaborative nature, particularly when it turns out that end-user requirements are largely the same or when scarce financial resources can, and must, be pooled together. Last but not least, the integrated model might dominate at lower TRLs, while collaborative or co-ordinated approaches could be dominant at higher TRLs (and, vice versa, the integrated model might be applied to new product or service development on the basis of largely institutional R&T programmes).

49. In Estonia, the integrated approach is built into the design of the so-called national research and development programmes – a mechanism established by the Organisation of Research and Development Act. The criteria for launching these programmes include the following requirements: the multidisciplinary nature of activities, the involvement of several ministries and linkages with the national research, development and innovation strategy. So far, national research and development programmes for ICT, biotechnology, energy, the environment and health, together with a provisional one for materials technology, have been launched. Although the integration of the R&T interests of various security, safety and defence stakeholders by means of a dedicated national programme sounds logical and natural, such programme does not yet exist.

50. Our conversations with the managers of some national research and development programmes were quite informative as to what issues should be addressed for an integrated security, safety and defence programme to succeed:

50.1 Planning: Participating ministries and agencies have to be good at joint planning from defining their common objectives and requirements to producing a sufficiently detailed, specific and measurable technology roadmap. As we highlighted earlier, Estonian defence and civil security organisations do not have a very positive record in this respect.

50.2 Focus: The chances of success increase if a programme does not have more than two or three clear directions.[80] The findings presented in Chapter III provide a basis for agreeing on such directions in security, safety and defence sector. However, not all themes relevant to this sector can be woven together into a coherent national programme.

50.3 Funding: Sufficient funding from participating ministries and the EU is what draws the attention, and ensures the eager participation, of public R&T organisations and the industry. Given that R&T spending levels of the civil security and defence sectors taken together are rather negligible in absolute terms (or even non-existent in some agencies), it is almost impossible to meet this requirement at the present, especially without any EU funding.

50.4 Political/policy level support: A national programme has to receive sustained attention and support from the political/policy-making level. As we pointed out earlier, the political level is often supportive of the dual-use R&T idea, but the problem lies with generalist policy-makers. It may be easy to generate a sufficient degree of attention and to gain backing for the themes

[80] The same advice – to seek a clear focus – comes from countries with considerable experience with dual-use R&T (for instance, Italy). See Esposito, 2010.

which are currently in vogue such as cyber security. However, it is difficult to elicit the same degree of support to equally significant but less popular and appreciated areas of knowledge, technology and innovation in security and defence (e.g. sensorics or human factors).

50.5 Governance and administrative capacity: There is a need for sufficient numbers of qualified people to provide robust programme oversight and administration. The MOD has only two full-time R&T managers, the MOI does not have a central R&T co-ordinator and the MEAC does not have an R&T expert for the security and safety part of its portfolio of responsibilities, so this capacity is extremely limited at the ministerial level. The picture is similar at the level of subordinate agencies.

50.6 Leading ministry: The business model suitable for national research and development programmes requires one ministry to lead, with overall programme responsibility and the involvement of other stakeholders. The experience, resources and relative sophistication of its R&T policy suggest that the Estonian MOD is suitable for taking this role in an integrated security, safety and defence R&T programme. However, the circle of civil security and safety end-users is broader; their knowledge and technology needs are more immediate; they have access to EU funds (which is not the case with the MOD, as defence organisations are excluded from EU financing); they also possess experience with EU-funded projects and/or the management of existing national research and development programmes (in addition, the MEAC can channel results of R&T projects through enterprise innovation support mechanisms). This seems to favour a non-defence ministry in the lead, but it comes with a significant risk of increasing the distance between R&T and military end-users (which runs counter to the MOD's policy and efforts).

51. Another possibility related to the integrated approach is to insert joint defence and civil security end-user requirements into existing national research and development programmes. This would be in line with the reality that civil security and defence R&T in Estonia exploits the same civilian R&T base. The managers of existing programmes are quite positive about this; but, as it transpired during the workshop, the governance framework of the programmes would have to be altered to allow this – especially as the MOD and the MOI currently do not contribute their own funds to support the fulfilment of their interests through existing national programmes.

52. As mentioned earlier, there are some examples of ad hoc collaborative approaches displayed by security and defence actors in R&T. In one particular case, end-users from the national defence and border guard authorities came together to formulate and communicate their needs to the scientists of Tallinn University of Technology who participated in the EU-funded project consortium on underwater acoustics monitoring (BIAS LIFE). In a similar vein, experts from civil security and safety organisations (e.g. the Estonian Information System's Authority and SMIT) have participated in some projects and events conducted by the NATO Science and Technology Organisation thanks to the support of the MOD. However, even such ad hoc collaboration – which suits civilian agencies very well given that they mainly invest in R&T on a case-by-case basis – is the exception rather than the rule. It is hampered by the lack of communication between the ministries and their subordinate agencies about their intentions for new projects and by the absence of clear points of contact (POCs) on R&T issues on the side of civil security and safety organisations.

52.1 The adoption of the Estonian Defence Industrial Policy 2013–2022 might lay the ground for more ad hoc collaboration on various projects. The policy

envisages that a committee of stakeholders will deliberate over ideas and project proposals coming from enterprises. However, this mostly pertains to projects at higher TRLs (i.e. new product or service development and introduction) rather than lower TRLs (i.e. R&T).

53. Opportunities for more structured long-term collaboration are emerging after the adoption of the new R&D strategy of the EASS. With its areas of interest clearly articulated, it is becoming possible to engage a sister organisation on the defence side – the ENDC – to collaborate on the development of new knowledge and in-house competence in areas where defence, civil security and public safety issues strongly overlap (but do not necessarily or immediately lead to commercial development opportunities) and to support the training and education missions of the two organisations. However, research capacities and ambitions are very limited which presents significant difficulties for structured collaboration to take off and be sustained in this format.

54. R&T co-ordination between civil security, safety and defence organisations in Estonia is provided in an ad hoc fashion at best, but usually it is absent. This is despite the government's legal obligation to assume a formal role as a co-ordinating organisation for all institutional research and development programmes – civil security and defence representatives have only recently been included in the MER-led working group for renewing the national R&D and Innovation Strategy ("Knowledge-Based Estonia"). One reason for this is, of course, that the majority of actors on the civilian side of demand do not have any policies, strategies or roadmaps that can be co-ordinated or harmonised with the defence side in the first place. (Our workshop also revealed that agencies on the civilian side do not co-ordinate much between themselves either due the very same policy vacuum and the MOI's and the MEAC's failure to play a co-ordinating role in R&T matters in relation to their own subordinate agencies.) The other reason is that many civilian organisations have treated defence as a completely separate sector which has too specific requirements and which is excessively oriented towards its war-fighting mission (a perception often reinforced by the EDF itself) and therefore bears little relevance to civil security and public safety needs.

55. The workshop participants also highlighted the following issues that prevent R&T co-ordination:

55.1 The inability of end-users to formulate effective and meaningful R&T requirements tailored to broader policies, capability requirements and operational needs;

55.2 The defence side's unwillingness to share classified capability requirements and development plans with governmental civil security organisations, let alone R&T suppliers;

55.3 The absence of central POCs for R&T issues on the civil security and public safety side in the MOI and MEAC spheres of governance (also in other organisations, e.g. the MOF, the Ministry of Foreign Affairs, etc.);

55.4 No interest from, and the lack of a defined role for, the State Chancellery in co-ordinating security-related R&T issues (even though the government meets in the Security Committee and R&D Committee formats, both of which are supported by the State Chancellery).

56. At the moment, awareness building about the R&T activities of defence, civil security and safety organisations in Estonia is quite sporadic, without a defined, constantly sustained and periodically updated set of measures. There have been spin-

offs from defence-related projects to civil security uses, but these have been quite accidental, resulting from the initiative and efforts of the supply side. Towering over other civil security and safety organisations with its R&T agenda and portfolio, the MOD has a special role to play in building inter-agency awareness and it has indeed been increasingly active in this regard. However, its administrative capacity is often overwhelmed by intra-organisational challenges and international co-operation demands, while opportunities for inter-agency awareness building are too few and far between.

Conclusions and recommendations

57. There are strong strategic, operational, financial and organisational reasons for civil security, public safety and national defence organisations to co-operate in R&T. The nature of contemporary security and defence is such that organisational silos stand in the way of effective whole-of-government and whole-of-society responses to the complex and dynamic threat and risk environment. The very limited financial and human resources of a small nation such as Estonia further contribute to weighty arguments for avoiding duplication, pursuing synergy and developing the inter-agency approach to the entire value chain of civil security, public safety and defence organisations – from joint foresight, risk and threat assessment, lessons learned, concept development and experimentation (CD&E) and R&T to common development of new services/applications, their testing and evaluation, joint procurement, maintenance and operations as well as education and training. It is quite difficult to build comprehensive security and broad-based defence without the inter-agency approach, including in R&T.

58. Our civil security, public safety and national defence organisations have to co-operate to fulfil their often blurred tasks and missions – especially when dealing with large-scale emergencies, but also in routine daily operations – or, at least, to act as intelligent customers for each other's services. Their technical and human interoperability has to be high, especially in systems and skill-sets which enable operational co-operation. Indeed, there are many examples that show they are quite successful at such operational co-operation in Estonia. What is lacking here is the culture, practice and framework for inter-agency risk analysis, capability planning, concept development and, by extension, the ability to formulate and manage common knowledge and technology requirements and to invest in dual-use R&T through a common effort. Dual-use R&T – an issue of growing importance at the European level and in other nations – or even R&T as such is simply missing from comprehensive security and broad-based defence thinking and practice in Estonia.

59. European and national practices as well as our take on Estonia's security policies and Estonian expert perspectives show that dual-use R&T – one of the enabling conditions for synergy between military, civil security and public safety sectors – has a rather defined set of themes. The most recurrent ones are situational awareness (a full variety of sensor technologies, their networks and integration); information management (C4I, cyber security, network-enabled capabilities, social media exploitation, etc.); physical protection; CBRN-E detection and protection; unmanned aerial, ground and undersea platforms and systems; space technology; and decision-making support (modelling and simulation, risk assessment, resource planning methodologies, etc.). We would also strongly argue that R&T in human factors and medicine (physical, cognitive and mental performance, behavioural and sociological research, medical research, etc.) is inherently dual-use and is exploited by civil security and safety as well as military organisations.

60. Co-operation on these themes ranges from awareness building and the exchange of results to co-ordination, collaboration and integration. National and

institutional contexts and levels of ambition determine which business models or combinations thereof are accepted in a particular country or even internationally (e.g. at the European level). Despite the Estonian government's formal obligation to ensure the co-ordination of institutional research and development programmes, there is not much co-ordination – indeed, there is even little mutual awareness, not to speak of collaboration and integration – between civil security, safety and defence organisations in their R&T investments. In terms of synergy, all achievements – mainly in the form of spin-offs from the defence sector's past investments – have been largely due to the supply side's initiative.

61. At the moment, the business models described above are not suitable for Estonia in their pure form, even though some tentative steps are being made towards, and initial conditions are emerging for, more co-ordinated and collaborative approaches. However, as a small nation, Estonia can ill-afford to thinly spread its financial, material, human and intellectual resources in civil security, public safety and national defence. R&T is one of the areas where these resources could be consolidated – especially on the demand side – to achieve synergy, to save time and money, to increase national competence and its international impact and to lay the groundwork for future interoperable or shared solutions (applications).

62. A fully integrated business model for inter-agency R&T activities (let alone for the entire value chain) is clearly unattainable, just as it is not present in its pure form elsewhere. On the other hand, partial integration, supplemented by collaborative, co-ordinating and awareness building arrangements, is the right direction to go. It would take time and considerable effort to achieve, but it would produce multiple benefits for a comprehensive security and broad-based defence posture as well as for security and defence enterprise innovation (including better access to EU funding and knowledge networks). It might even catalyse greater inter-agency co-operation in other components of the value chain (such as foresight and risk analysis, concept development and experimentation or capability planning) of this particular set of public services – civil security, public safety and national defence.

63. To advance the dual-use R&T principle in Estonia's civil security, public safety and national defence, we recommend the following:

63.1 Clearly define the **role, strategic value, broad priorities and expected impact of R&T** in the course of a security and defence review (updating the National Security Strategy, the National Defence Strategy, the Cyber Security Strategy, the Main Guidelines of Security Policy, the Fundamentals of Counter-Terrorism, etc.);

63.2 Develop an **inter-agency capability planning methodology and process** to effectively bring together different civil security, public safety and national defence organisations:

63.2.1 The development of a **comprehensive methodological toolbox, ideally covering the full value chain** (from joint foresight, risk and threat assessment, lessons learned, concept development and experimentation (CD&E) and R&T to common development of new services/applications, their testing and evaluation, joint procurement and maintenance, inter-agency operations and education and training) would be an ambitious and complex, but eventually a very rewarding undertaking;

63.2.2 Alternatively, the defence side should develop methods for including civil security and public safety organisations in their existing planning processes and, vice versa, for participating in the existing planning processes of the civilian authorities. This goal is less ambitious,

but still requires mutual familiarity with planning tools on the military and civilian sides as well as some common training and adjustment of organisational processes;

63.3 In response to those strategic expectations (see the first point), produce a **common knowledge, technology and innovation agenda and roadmap** for the entire civil security, public safety and national defence sector as a separate capstone document or as an integral part of the national R&D and Innovation Strategy ('Knowledge-Based Estonia', or whatever its future iterations are going to be called). Merge, or at least link, **the Estonian Defence Industrial Policy** with this agenda;

63.4 Establish a clear and legally binding **budgetary benchmark** for the ministries responsible for civil security, public safety and national defence regarding multi-annual investments in new knowledge, technology and innovation;

63.5 Consider running **regular joint sessions** of the government's Security Committee and its R&D Committee to provide general political guidance and oversight concerning common knowledge and the technology and innovation agenda of the civil security, public safety and national defence sector, with a concomitant role for the State Chancellery;

63.6 Appoint **POCs for R&T** at the ministries and subordinate agencies dealing with civil security and public safety (including ministries not covered in this paper, e.g. the Ministries of Justice, Social Affairs and Foreign Affairs). Institute **regular meetings** of POCs (including the existing defence side's POCs) as a work format for dual-use R&T and inter-agency co-operation in this field;

63.7 Develop an **inter-disciplinary training programme** for R&T co-ordinators, capability developers, experts and policy generalists on the role, exploitation and impact of R&T in civil security, public safety and national defence, including on the methodologies for the definition of R&T requirements and on the translation of results into policy, conceptual, technical, organisational, operational or doctrinal innovation. Ideally, the programme should form part of the public service capacity development programme run by the State Chancellery and use the EASS as a platform for its organisation and delivery;

63.8 In terms of an appropriate **mix of business models** for dual-use R&T (see summarised in Figure 2):

63.8.1 As a basic awareness building measure, **enhance communication** about R&T needs, ideas, initiatives, projects and their outcomes between the ministries and their subordinate agencies that deal with civil security, public safety and national defence by means of mailing lists and newsletters, by opening meetings of the MOD Research Council for observers from other ministries and agencies, by inviting them to the EDF science days, etc.;

63.8.2 Establish a **regular and all-inclusive meeting forum** (e.g. annual conference) for all stakeholders of dual-use R&T (both the demand and supply sides) in order to foster broad awareness of R&T and innovation developments and trends in the field of security, safety and defence;[81]

[81] The seminar in 2010 and the workshop in 2013 demonstrated that such gatherings are very much appreciated by R&T experts, policymakers and R&T suppliers.

63.8.3 Consider launching a **national research and development programme** in civil security, public safety and national defence as a partial integration element of the mix, focusing on one or two knowledge and technology areas where interests of end-users are closely aligned. In our view, the key focus area for this measure should be (at least initially) **situational awareness and information management technologies**;[82]

63.8.4 As another element of partial integration, jointly develop new knowledge and technology requirements of national defence, civil security and public safety end-users for some of the **existing national research and development programmes**. The health programme (e.g. to address requirements concerning cognitive, psychological and physical performance of personnel in extreme conditions, the prevention and treatment of post-traumatic stress disorder, personnel rehabilitation, etc.) is the most obvious candidate. Other programmes (ICT, materials, energy and biotechnology) could also be considered:

- Start a dialogue with the leading stakeholders of those programmes on the necessary arrangements and adjustments to enable the acceptance and fulfilment of joint requirements.

63.8.5 As a collaborative element of the mix, advance close research collaboration between the EASS and the ENDC through a framework agreement and common projects. In particular, focus this collaboration on research on **human and organisational factors** (decision-making and leadership, personnel management, psychology and sociology, man-machine interaction, organisational behaviour, etc.), **modelling and simulation**, innovative **education and training methodologies** and various comprehensive **civil-military planning methodologies** (e.g. risk assessment, strategy, foresight, resource planning, crisis management, etc.):

- **Commit and adequately fund** the two organisations to enhance their in-house research capacities, so that they could better serve their end-users and more effectively engage in collaboration;

63.8.6 Use the inter-ministerial and inter-agency expert group (recommended above) as an instrument to co-ordinate institutional R&T initiatives and activities in **unmanned systems and platforms**, **CBRN-E defence**, **physical personnel and infrastructure protection technologies** and **space technology**. This kind of co-ordination would help avoid the duplication of investments and interoperability problems, while creating opportunities for commonly funded (ad hoc collaborative) projects:

[82] C4I devices, systems and networks, their integration/interoperability and protection/security (cyber security), data fusion, etc.; surveillance and signal processing devices, platforms, systems (including space-based) and their integration for maritime/air/land(area)/point monitoring and object detection, localisation, identification and tracking.

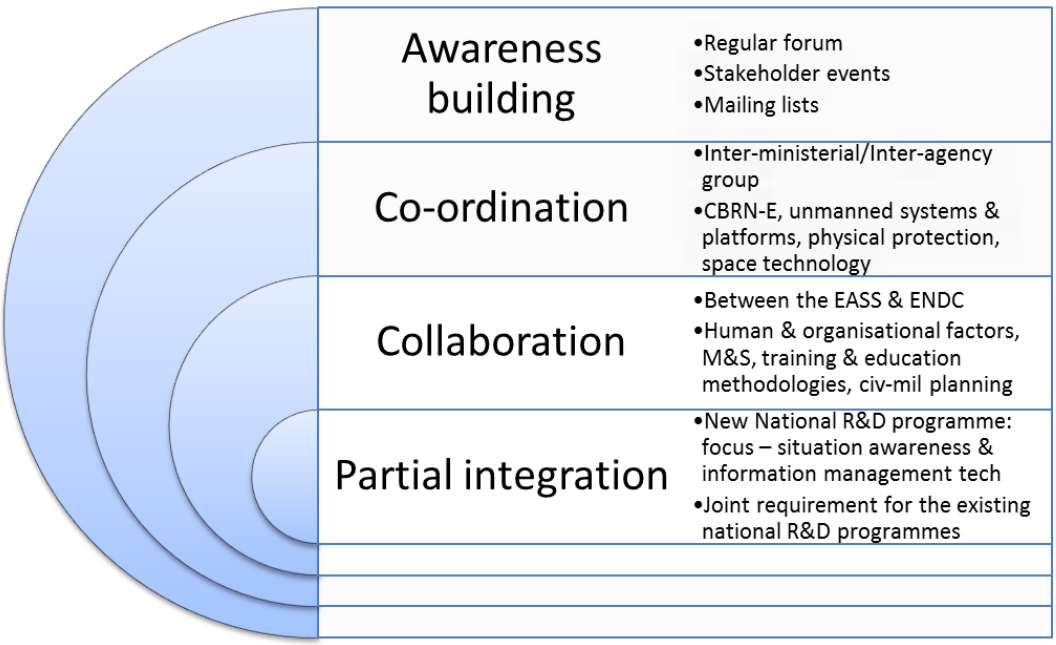

Figure 2: The recommended mix of business models for Estonia's dual-use R&T