#71

DEFENCE INNOVATION: NEW MODELS AND PROCUREMENT IMPLICATIONS

The Estonian Case

Tomas JERMALAVIČIUS

HEAD OF STUDIES,
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY (ICDS)

Martin HURT

RESEARCH FELLOW,
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY (ICDS)

September 2021

The views expressed here are solely those of the author.
They do not reflect the views of any organisation.

Policy Paper

ARES
Armament Industry
European Research
Group

ABSTRACT

As a small country, Estonia cannot afford to pursue defence innovation through large, complex, and expensive programmes that entail high risks and uncertainty. Its land-centric and reserves-based defence forces also have limited demand for cutting-edge innovative solutions and prefer cost-effective innovation procurement through the products and services already available in the competitive market. However, Estonia draws on its vibrant start-up culture and some "niche" strengths in its national S&T base (such as ICT, cybersecurity, AI, robotics, health technology) to advance enterprise-led and MoD-supported innovation that also benefits from its "broad-based" defence model and whole-of-society approach. This innovation is primarily focused on enhancing the export potential, but it also provides the means to engage the Defence Forces in activities that eventually stimulate military interest to incorporate more high-tech solutions into capability development. Despite a strong transatlanticist orientation in its security and defence policy, Estonia has also been highly successful in exploiting the opportunities to manage financial and technological risks as well as in integrating its security and defence innovation ecosystem into multinational networks that emerged with the new European instruments, particularly the EDIDP/EDF.

Keywords: *Estonia, defence innovation, procurement, start-ups, military requirements, European defence cooperation.*

INTRODUCTION

The Estonian approach to defence innovation has been shaped by several major factors in the recent years. Its threat assessment has been long focused on Russia's threat to its sovereignty and territorial integrity, but such focus has been further reinforced by Moscow's aggression against Georgia in 2008 and against Ukraine since 2014. This necessitated focusing the defence investments on the development of national capabilities for territorial defence and to support credible allied deterrence posture in the region. However, since the threat is multifaceted and not just singularly military, efforts to build capabilities in new domains such as cyber have also been significant. Estonia's defence strategy has long called for a broad and holistic perspective on national defence, or so-called 'broad-based' defence, that incorporates various non-military aspects and capabilities from other agencies, public and private sectors as well as the broader society (Estonian Ministry of Defence, 2010).

At the same time, Estonia seeks to support other NATO allies and EU member states in addressing their security challenges, thus acting as a security producer and not just a consumer. Its participation in French-led Operation *Barkhane* and the *Takuba* Task Force in the Sahel region, and Estonia being the only Baltic state to join the European Intervention Initiative (EII) are two examples of this policy. Just like strengthening collective defence and deterrence, this requires close attention to the imperative of maintaining interoperability with key allies and partners – an imperative that is becoming ever more challenging at a time when those allies and partners are racing ahead to harness various emerging and disruptive technologies (EDTs) for military purposes.

A new momentum after the efforts to strengthen the European defence cooperation – particularly through instruments such as the Permanent Structured Cooperation (PeSCo), the European Defence Industrial Development Programme (EDIDP), and now the freshly launched European Defence Fund (EDF) – has also offered new opportunities for Estonia not only to contribute to cutting edge innovation but even position itself among the leading nations in certain areas. While still somewhat held back by a degree of caution over the potential impact of this cooperation on the transatlantic relations or ability to deliver actual capabilities, Estonia seeks to leverage these instruments to stimulate defence innovation, manage financial risks, and strengthen the competitiveness of its high-tech sector.

The aim of this paper is to provide an overview of the state of play in the Estonian defence innovation and procurement, as well as to highlight how Estonia is using the European instruments to advance its priorities and contribute to collaborative efforts.[1]

POLICIES

The key elements of the Estonian defence innovation policy are reflected in two principal documents of the Ministry of Defence (MoD) – Research and Development (R&D) Policy and Defence Industrial Policy. The newest iteration of the former was approved in June 2021 to cover the period until 2030, while the latter currently covers the period of 2013-22 and is undergoing a review for the next period (also until 2030) (Kaitseministeerium, 2021; Kaitseministeerium, 2013). Both these policies operate on a basis of a clear-cut recognition that Estonia's financial and human resources – both in the defence sector and nation-wide – are very limited and restrict the possibilities in terms of scale and impact of innovation. Financially, even though Estonia has been consistently among those spending 2% or even more of their GDP on defence for the last decade, its annual defence budget in actual terms is less than a billion euros (€630 million in 2020, 569 in 2019) (North Atlantic Treaty Organisation, 2021), with €77.9 million spent on equipment procurement and just €3.1 million on R&D in 2019 (European Defence Agency, 2021).

This naturally calls for a clear focus, smart ways of investing into innovative solutions, and effective organisation in planning and allocating scarce resources. For instance, the R&D Policy of the MoD echoes the general concept of 'smart specialisation' promoted by the EU and seeks to focus investments into the areas where Estonia has developed some strengths in its civilian R&D sector, such as information and communication technology (ICT), cybersecurity, artificial intelligence (AI), sensors, robotics, or health technologies. It also recognises that most of those investments will be of dual-use and strongly encourages this approach, even if their ultimate purpose, from the MoD's perspective, is to strengthen national defence capabilities and enable international defence cooperation.

In the meantime, the Defence Industrial Policy is focused on supporting the development of new innovative products and services by the private sector that would have military

[1] For the paper, in May-June 2021, the authors have interviewed 14 experts and officials from the MoD, Defence Forces, defence industry and other sectors, with the condition of non-attribution applied.

utility and application, but its key criterion is the export potential and international competitiveness of those products and services. This is mainly achieved through an annual grants competition with a budget of €600,000, in which enterprises can bid for the MoD's support grants of up to €200,000 in order to develop innovative solutions between Technology Readiness Levels (TRL) 4-7. The proposals are evaluated by a board that includes representatives of the defence forces who provide end-user perspective, representatives of national agencies promoting entrepreneurship, and start-ups who assess the business plans of the proposals. Although the MoD first struggled to attract enough proposals to have a truly competitive selection, by the end of the 2020s their number grew to the extent that it has become a very competitive process where only the best proposals are awarded the grants (see Table 1 for the grant-awarded projects).

2021	• Intelligent Decision Support System (IDSS) • Pyrotechnical training round (PTR) for 84 mm recoilless rifle Carl Gustaf • Universal Drone Detection Platform DefEST • Modular tooling interface development for an underwater robot • Development project application for pop-up target HARDY • UP6K Tactical – 6 kW fuel cell electric generator
2020	• Full-Duplex Radios for Defence and Security • Multi-Flex Maritime Platform • Integrated Intelligence, Surveillance and Reconnaissance system development based on Unmanned Ground Vehicle • Digital Armoury • Development of ProDot 1x25 Military-Grade Red Dot Sight • Prototype of Unit of an automated mini-drone-station with 'search & find' AI detection model software • Silent Hunter UAV
2018-19	• Multi-purpose Loitering Munition (MPLM) • 76mm Training Smoke Round • Anti-UAV missile autopilot and computer vision system • Smart mine trigger system development • Development of high-quality high performance semi-automatic and full-automatic 9mm Pistol Calibre Carbine (PCC) rifles calibre 9x19 Parabellum • Mine clearance training device development for both military and peacekeeping operations • Mined tank obstacle for infantry squads

2017	• Patient information and registration system for military field use (MIL HIS) • Enhanced technology for camouflage in NIR-range • Development of high quality semi-automatic and bolt-action long-range sniper rifles in calibre 338 Lapua Magnum • Blank firing system for Browning M2 • SecureChat communication system and redesign to Android operating system • Airframe development of low-cost attack multicopter UAV • Reinforcing substructure for ultra-lightweight universal extremity fixation device
2016	• Intuitive control system and virtual learning environment for autonomous unit supporting multi-purpose unmanned ground vehicle • Supercapacitor-based starter module in NATO 6T format • Signal intelligence sensor for unmanned aerial vehicles (UAVs) • Creating a platform for tracking and interfering with LSS (Low, Slow & Small) type drones
2015	• Development of an automated cyber defence training platform
2014	• A selective sensor to detect the movement and type of military heavy equipment on land and, if necessary, for starting a destruction device • Development and testing of an unmanned hybrid vehicle with increased off-road capacity • Development of a backpack version of an extended frequency mixing device for radio-controlled bombs • Development of a prototype of a modern field switch • Autopilot development for unmanned aerial vehicles
2013	• Development of a mobile modular trauma centre, including triage and medical storage • Development and testing of a multirotor UAV prototype into a product • VHF communications solutions for headquarters and communications units based on maritime communications solutions • Bomb cellar prototype development

Table 1. Projects awarded financial support grants in the framework of the MoD Industrial Policy during 2013-21 (Kaitseministeerium, 2021a).

However, successful development of the products and services by the grant-winning enterprises does not necessarily translate into the MoD or the Defence Forces actually purchasing the outcomes – even if some contracts could be awarded in order to serve as a 'reference customer', which is often required in order to build an international sales portfolio. There is no formal MoD procurement policy in place at all, but the informal guiding principle is that free market competition rather than "strategic partnerships"

should determine the outcomes of procurement projects and programmes. Indeed, some defence procurement officials even argue that the way Estonia invests in defence innovation is through the acquisition of weapons, equipment and systems already containing innovative but well-tested solutions developed by domestic and international suppliers, instead of spending scarce resources on long and risky development programmes. Commercial and military off-the-shelf procurements remain the preferred paradigm in Estonia's defence procurement, but with the share of procurement of new (as opposed to second-hand) armament and equipment growing, the need for technology awareness, absorption, and management capacities is also increasing.

Still, there is also a growing pressure for the defence organisation to incorporate innovative solutions developed by the Estonian national science, technology, and industry sector into defence planning and capability development. R&D is currently not well integrated into the routine capability planning process and is more ad-hoc, often relying on personalities and personal connections. The problem does not really come from a lack of understanding of how innovation should feed into capability development but is more related to the deficiencies in the organisational processes and capacities. According to the R&D Policy 2021-30, the MoD should work to ensure proper coherence between R&D, defence industrial policy and defence capability development (Kaitseministeerium, 2021b), which will require reviewing, better describing, and formalising the defence innovation framework and processes as well as strengthening the innovation capacities of the defence organisation.

STRUCTURAL CHANGES

In 2017, in order to streamline processes and increase its capacity to manage complex projects, Estonia consolidated its entire defence organisation's procurement management functions – previously scattered between various structural units of the MoD and Defence Forces – in a newly created Estonian Centre for Defence Investment (ECDI) under the MoD. Its mandate, which spans from the acquisition of major weapon systems to infrastructure development projects and other investments, also includes executing defence investments into the development of innovative solutions. With this,

Estonia addressed the need to enhance its technology management capacity and created the framework to better integrate defence innovation and procurement processes.

A similar centralisation took place on the end-user side in the Defence Forces concerning feedback and end-user perspective on the innovative ideas and solutions proposed by the academia and industry. In the framework of the MoD's 2014-22 R&D Policy, the Applied Research Department of the National Defence Academy (NDA) has become a single point of contact for those outside the Defence Forces seeking to engage military end-users early in the innovation projects, to assess the relevance of innovative solutions to military needs, and to organise tests that could generate feedback data on performance in real military operational and tactical environment. It is also a focal point in advancing cooperation between the civilian and military research communities, and as an organisational base for the military personnel who are enrolled in the PhD programmes of the civilian universities.

As part of its mission, the department also performs Operational Research / Operational Analysis (OR/OA) for the Defence Forces, whereby providing crucial input necessary for the military to define its own requirements and to assess the potential value and impact of various innovative solutions. However, many officials recognise that there is a need for more extensive OR/OA and that the absence of dedicated field units or similar structures for battle experimentation with new technologies might become a shortcoming in the future, especially when it comes to expanding Concept Development and Experimentation (CD&E) efforts. Coordination with the civilian security research organisations – primarily the Estonian Academy of Security Sciences in the area of responsibility of the Ministry of the Interior (MoI) – is also somewhat lacking, with the two organisations often engaging in similar but parallel research of dual-use nature that would benefit from a more coherent and sustained inter-agency approach.

On the supply side, a number of Estonian and foreign enterprises participate in the Estonian Defence Industry Association (EDIA).[2] The association is increasingly effective in providing a platform for interaction between all three parts of the so-called 'triple helix', with the representatives of the industry, R&D organisations, and government

[2] Contrary to the usual practice for national associations to include only indigenous firms, the EDIA membership is open to foreign security and defence enterprises that work with Estonian customers. The EDIA currently has European companies in its members, such as SAAB, MBDA, and BAE Systems, as well as Raytheon Technologies from the US, and Japan's Fujitsu.

coming together in 11 working groups formed to advance mutual understanding and explore cooperation opportunities in different areas (AI, C2 and cyber, UAV/C-UAV, weapon systems and maintenance, manoeuvre and maintenance, training and simulation, personal equipment and clothing, military medicine, space, etc.). The EDIA also provides a platform for the Defence Estonia Cluster launched in 2019 that currently has 14 members and seeks to promote innovation in the defence and security industry in order to develop new and highly competitive products and services for export, with the aim of increasing the export volume of Estonian defence and security industry tenfold by 2029 (EDIA, 2021). As the cluster is co-funded by the European Development Regional Fund and is part of a group of similar clusters under the auspices of Enterprise Estonia, it creates important links to the European and national innovation and entrepreneurship promotion efforts.

While the above are rather 'conventional' frameworks to manage defence innovation, a far more interesting and consequential structural development took place in the field of cyber defence. Since 2008, Estonia has been a host nation for NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and has generally acquired a solid reputation for its robust approach to cybersecurity. Yet, despite the recent creation of Cyber Command in the Defence Forces on the one hand, as well as a vibrant cybersecurity start-up scene and enterprise ecosystem on the other, it has lacked an open and flexible platform for the experimentation of new concepts and the development of new products and services in cybersecurity and cyber defence.

Such a platform was created by the MoD in 2020 when establishing the CR14 – a non-profit organisation that is developing and managing a cyber range used by the Defence Forces Cyber Command, the Cyber Defence Unit of the Estonian Defence League (voluntary territorial defence organisation), and NATO CCDCOE for training, exercises (e.g. multinational cyber defence exercise Locked Shields), R&D, as well as CD&E. Together with ist Estonian and Norwegian partners (Norwegian University of Science and Technology), it is currently working on the project of Open Cyber Range – an arrangement whereby cyber defence and cybersecurity innovators (enterprises, start-ups, even individuals such as conscripts of Cyber Command) would have access to the CR14 capabilities to conduct exercises as well as test and further develop their new ideas and technologies (Estonian Ministry of Defence, 2021). It is also emerging as a hub through

which the adoption of certain advanced digital technologies is being channelled into the Estonian defence, as exemplified by the recent introduction of a solution to enhance its capabilities as a platform for simulations and exercises, in cooperation with local partners such as the University of Tartu, CyberExer Technologies, Elisa and Thinnect, or Nokia's 5G Digital Automation Cloud (DAC) (Kaitseministeerium, 2021c). The CR14 is likely to become an important player for Estonia to engage other EU partners – governmental, public, and private – in collaborative innovation projects, as well as to advance the MoD's vision for Estonia's future role in advancing the military applications of AI.

Non-profit entities that create a trusted, flexible, and stimulating environment for interactions between the innovation stakeholders overall seem to be an overlooked trend. Another example from Estonia is Garage48, an organisation that conducts competitive 'hackathons' involving experts from academia, government, and industry from Estonia and abroad – particularly from the Nordic-Baltic region. The NDA has been a keen participant in these annual events, and in 2018 a 'hackathon' specifically dedicated to pitching innovative ideas for the defence sector, the Garage48 Defence Makeathon, was held at the University of Tartu – a leading university of Estonia – in cooperation with the MoD, EDIA, and the NDA, which attracted 170 participants from 20 nations (Garage48, 2018).

MID-TECH END-USER?

However, the changes and initiatives mentioned before may have a limited impact on the uptake of innovative solutions by the Defence Forces. With the land component being dominant in the overall structure but comprised of just two brigades and oriented mostly towards building personnel reserve for wartime structure, the military are often focused on addressing fairly conventional needs and requirements rather than experimenting with innovative capabilities. Indeed, some officials argue that despite some advance, for instance in the digitalisation of the Defence Forces by implementing indigenous solutions such as situational awareness and the battle management system KOLT, it is necessary not to become too dependent on expensive high-tech instruments. In this line of argument, the force and its capabilities would become too complex for the reservists, too

vulnerable to the adversary's countermeasures, too exposed to cutting-edge technology failures, and too expensive to maintain.

In essence, this represents a mid-tech posture, or a combination of some high-tech, if not cutting-edge, elements in some key areas such as C3 or cyber defence with lower tech yet robust capabilities that could be employed by a mobilised army of reservists. In this posture, significant attention must be paid to researching, understanding, and managing the human and organisational factors – and advancing related innovation – over technological aspects. Also, innovation that cuts costs and complexity becomes a much more attractive proposition than the constant pursuit of some cutting-edge technology through high-cost and high complexity programmes.

On the other hand, it is sometimes argued that conscripts and reservists provide opportunities for the Defence Forces to tap into a broader base of knowledge and skills in the society and benefit from innovation in the civilian sector. Although this often remains a rather theoretical possibility without effective mechanisms in place to harness this potential, it is often acknowledged in Estonia that the conscript and reserve service is one of the factors that help, to some extent, enhance the awareness of the civilian S&T community, start-up creators, and enterprise managers about the real-life military challenges and environment. Service in the Cyber Command that partly relies on the conscripted manpower is regarded as a particular case in point, as the growing digital skills of the society have become valuable assets for the defence organisation, and vice versa, insights into the military cyber domain inspire innovative development and entrepreneurial pursuits. The aforementioned KOLT system, for instance, is a product developed by cyber conscripts and reservists (Eesti Kaitsevägi, 2019).

Yet, as the Estonian society and digital economy constantly experience insufficient numbers of highly skilled IT professionals and rely increasingly on the imported foreign workforce, this fluid circulation of knowledge between civilian and military sectors has its limits. It will be afflicted by trust issues, as there is some reluctance to allow foreign talents (especially from non-NATO and non-EU nations) who represent a significant portion of the digital innovation ecosystem to come close to the very heart of the digital society – its cybersecurity and cyber defence. Since the Defence Forces reservists become creators of cybersecurity start-ups but have to partly rely on foreign talents in their development, this may become an important constraint on the cybersecurity ecosystem

when it comes to interactions with the Cyber Command that even strict security vetting protocols may not be able to overcome.

Furthermore, given that military experience as a conscript is usually confined to the lowest tactical levels, the value of it in advancing large-scale transformative innovation should not be overstated, even if it contributes to interesting bottom-up ideas. Estonia maintains a relatively large reserve component compared to its active component, and the officials admit that this is not ideal for innovation. Using conscripts limits the possibility to experiment, as exercise time is always limited, and the focus is set on certifying units, not on innovation. Still, unit commanders are generally willing to provide the NDA and its industrial partners with opportunities to test new solutions within their units – and often give valuable feedback on their performance. There are some examples of extensive testing of new technology even on international missions, but they focused more on technical aspects than on the identification of operational strengths and weaknesses.

At the strategic level, innovation is constrained by the fact that Estonia's basic defence strategy, force design, and concepts for its employment have remained largely unchanged since 2010, when the last official National Defence Strategy was published. Furthermore, even the scope that is available and possible is not fully exploited due to the lack of wider interest in cutting-edge innovative solutions, the absence of long-term strategic foresight, as well as a relatively poor ability to identify deep problems for R&D-based solutions, or sometimes even to articulate effective military requirements. Although the competence of the MoD and the Defence Forces Headquarters in planning has considerably grown over the years, they still have major weaknesses when it comes to incorporating R&D-based inputs into those plans, identifying the need for innovative solutions in capability development, and coordinating their implementation.

As the military still often struggles with defining military requirements that could drive innovation, the efforts are initiated by the MoD's Defence Investments Department and EDIC, as well as the industry, and these efforts focus more on technical innovation than on satisfying the operational requirements. Nevertheless, all stakeholders realise the vital need for the Estonian defence companies to have the Defence Forces as a reference customer. This both offers opportunities and presents some risks: the MoD and the industry may be able to push the military to embrace innovative technology developed by

the Estonian companies and their international partners, but the operational requirements might not be sufficiently considered, thus potentially leading to the acquirement of technology that solves non-existing operational problems.

One possibility to mitigate this risk is to strengthen the link between innovation and the National Defence Development Plan (NDDP), a 10-year plan that is revised every four years. The purpose of the NDDP is to determine the priorities for defence capability development based on operational requirements. One of the benefits of the NDDP is that it is relatively flexible in allowing innovative solutions to meet operational requirements.

There are some encouraging signs that the Defence Forces might take a more systematic and anticipatory view of the EDT challenges and of their military effects. There is an ongoing work to set up an autonomy programme to centrally coordinate all the work from the Defence Forces HQ – maintaining technology awareness, assessing implications to military capabilities and operations, defining corresponding military requirements, and evaluating innovative solutions – in a broad area of autonomy technology. If this programme goes forward and receives the necessary resources (which is still an open question given the defence budget cuts enacted as a result of the Covid-19 pandemic and its economic repercussions), it may become a pivotal element in future-proofing the Defence Forces and adopting high-tech solutions in the development of the Estonian defence capabilities.

AREAS OF FOCUS

Autonomy is inevitably a very broad field that encompasses a multitude of technologies. There is clear recognition that Estonia, due to its small size and lack of critical mass in many S&T disciplines, cannot excel in all of them and must build excellence in particular niches that draw upon its existing strengths. First and foremost, this means cybersecurity, an area in which a vibrant innovation ecosystem has emerged over time in Estonia allowing it to be ranked third globally and first in the EU in the Global Cybersecurity Index 2020 (International Telecommunication Union, 2021), and an area which is pivotal for modern societies and their armed forces and which will certainly retain its fundamental importance in the upcoming age of the Internet of Things. Cybersecurity is an area where governmental agencies such as Start-up Estonia working to advance national

entrepreneurship are giving much attention and resources and have high expectations about the future R&D-intensive growth.

More recently, some of Estonia's cutting-edge innovation efforts have also been directed at addressing the cybersecurity challenges in maritime and space domains as new frontiers. Estonian cybersecurity companies are working with the European Space Agency (ESA) to deal with space cybersecurity issues (Guardtime, 2019, 2020), and as part of the OCEAN2020 consortium within the framework of the Preparatory Action for Defence Research (PADR) managed by the European Defence Agency (EDA) (Cybernetica, 2018). Furthermore, over-horizon challenges such as quantum technologies are coming into the focus of attention, with the Estonian enterprises and academia beginning to grapple with the potential of quantum cryptography (Paulus, 2020).

AI-related innovation is also becoming a major area of interest, with the MoD undertaking efforts to position Estonia within NATO and the EU at the forefront of policy initiatives that seek to advance this innovation and harness it for defence purposes. Part of this effort is dedicated to ensuring that small nations have access to sufficiently large data pools to train machine learning algorithms, and that policy, legal, ethical, and technical challenges are addressed by nations in a coherent manner in order to maintain interoperability of their future capabilities. There are some particular concerns among the policymakers in Tallinn that the EU may adopt AI policies which will severely impinge upon the development of military AI in the future and will thus undermine the collective ability of NATO/EU to maintain military technology edge over adversaries such as Russia.

One of the areas which could potentially be hampered but which has already been emerging as a success story in Estonia is military robotics. While some applied research and initial development work funded by the MoD in the mid-2000s seemed inconsequential at the time, it laid the groundwork for breakthroughs during the 2010s in designing and producing both unmanned aerial and unmanned ground vehicles. UAVs developed by Estonian companies such as Threod Systems have been successfully introduced to support units of the Defence Forces and have shown very strong export potential as well as further development opportunities both for civilian and military uses. For instance, Estonia and Finland performed a UAV flight experiment across the Gulf of Finland in 2019, which was 'the world's first over-sea international drone delivery under UTM control' [UTM – unmanned aircraft system traffic management] (Estonian Aviation

Cluster, 2019). Potential application of unmanned aerial systems in lethal military missions is also being explored by using the MoD grants to develop loitering munitions and swarming technologies.

Estonia also strives to become a European centre of excellence when it comes to military ground robotics. Its unmanned ground vehicle (UGV) developed by Milrem Robotics, TheMIS, is considered for a variety of combat support and combat service support functions in several armed forces, with the Netherlands set to deploy it with its contingent in Lithuania as part of NATO's enhanced Forward Presence Battlegroup, by 2022. The platform is also marketed for a broad range of civilian applications, from rescue works to mining operations, while the competences acquired to develop it enabled the company to secure a contract with the ESA to start applying its autonomy capabilities towards planetary rovers (Milrem Robotics, 2021b). Even though the Estonian Defence Forces have extensively tested this platform in Mali and in the conscript-manned units at home, those tests have been focused mainly on technical aspects, while the vision for its integration into the Tactics, Techniques and Procedures (TTPs) seems to be still lacking.

The innovators involved in this area admit that while Estonian developers where among the trailblazers in this area, the country is unlikely to stand out for long, as other (and much more resourceful) European nations have recently caught up and begun directing serious investments into military ground robotics. Nonetheless, the Estonian industry is already looking ahead, with a larger and more capable platform (Type X) under development (Milrem Robotics, 2021a). The future prospects of the sector received a strong vote of confidence from the European industry peers after Krauss-Maffei Wegmann (KMW) became a minority shareholder of Milrem Robotics in 2021 (Milrem Robotics, 2021c).

The maritime domain is also emerging as an important area for Estonia to innovate with unmanned solutions. As the navies of the Baltic states will be retiring much of their maritime mine countermeasures (MCM) capability in the 2030s, there have been efforts underway to agree on a new common vision for the shape of the future naval capabilities of Estonia, Latvia, and Lithuania. One of the options of this vision envisages a transition to more multifunctional capabilities enabled or even embodied by unmanned surface and underwater platforms and systems. In line with this, the Estonian MoD, ECDI, and industry (Baltic Workboats) began exploring the possibilities for a project that could deliver a

prototype suited for this vision. Still, the potential end-user, the Estonian Navy, remains cautious and regards this as a high-risk technology area in which environmental, legal, technical, and operational issues are far more challenging than in the land or air domains. Therefore, its expectations from the potential project are different from those of the MoD Defence Investment Department or the involved enterprises – to stimulate technological awareness, competence, and capacity rather than deliver a complete solution to meet future military requirements.

A natural extension of the Estonian interest in robotics – and of a general trend where unmanned platforms are set to pose a significant threat to future operations of the Defence Forces and allied forces – is the interest in systems to counter these capabilities and provide smart surveillance solutions. Estonia's past R&D investments in sensor and electromagnetic spectrum (EMS) technologies are already bearing fruit in the form of competitive commercial products such as the Shark C-UAV system by Marduk and a suite of electronic warfare (EW) equipment by Rantelon, as well as AI-driven multi-domain surveillance systems by DefSecIntel Solutions. It is entirely to be expected that this area will continue to rapidly evolve in Estonia, and in the case of EMS perhaps also converging with the innovation in the cyber domain. Electronic Warfare (EW) Live, an annual international event launched by Estonian and international partners in 2017, has already become a venue for showcasing the latest advances in EW systems and equipment.

Last but not least, since the value of soldiers and human operators – particularly in small countries with small armed forces – has never been higher, the ability to save lives on the battlefield that builds upon Estonian national competence in medicine, human factors research, and health technology has become another important direction. The innovative modular military hospital facility Golden Hour Mobile Modular Hospital (MMH), developed by Maru, has already been deployed by the Defence Forces nationally to support the civilian health system overwhelmed by the first wave of the Covid-19 pandemic in 2020 (ERR News, 2020). As health data technology and industry is rapidly taking shape in Estonia, it can be expected that digital solutions allowing to monitor and manage the physical and mental performance and the health of soldiers on the battlefield will emerge as a significant area of interest for defence innovators.

While the outline given here is far from comprehensive and exhaustive in describing various defence innovation ecosystems clustered around particular technology areas –

training and simulation technology, space technology, or new materials being among those not covered – Estonia has made significant progress in advancing R&D intensive start-ups and enterprise innovation where national excellence meets international market opportunities. The question is whether the European defence cooperation instruments and initiatives will provide a further boost to this progress.

USE OF THE EUROPEAN INSTRUMENTS

Estonia's general attitude towards the EU defence cooperation has always been rather cautious and seeking to steer it away from a competition with or a duplication of NATO. Tallinn has also been sceptical of the degree to which this cooperation will be able to deliver actual and affordable capabilities. It is therefore not a surprise that Estonia is involved only in four PeSCo projects at the time this was written – Military Mobility; Cyber Rapid Response Teams and Mutual Assistance in Cyber Security; European Medical Command; and, as a lead nation, Integrated Unmanned Ground System (UGS) – all of which align well with the fundamental strategic concerns and interests as well as with the defence innovation priorities of Estonia.[3] As an ardent transatlanticist, it has also been fully supportive and welcomed the decision to open PeSCo projects to third parties, particularly the United States, whose role in defending Europe from external military threats is regarded by Estonia as pivotal. However, the recent reports that most of the PeSCo projects are behind the schedule or face major obstacles (Barigazzi, 2021) are bound to reinforce this deeply rooted scepticism and cautious stance, while the relations with the US based on such bilateral instruments as the defence research cooperation agreement of 2016 (US Department of Defence, 2016) or the pursuit of opportunities in the US security and defence market and technology ecosystems for the Estonian enterprises will remain at the heart of Estonia's policy.

Theoretically, if the transatlantic relations severely deteriorate in the future, or if the European and American defence industrial competition leads to ever higher degrees of protectionism on both sides, this may cause some practical dilemmas and challenges for the Estonian defence innovation ecosystem seeking to forge strong links both within

[3] A caveat must be made here: some of the EDIDP projects are run in the context of PeSCo. Therefore, the actual number of PeSCo-related projects in which Estonian enterprises are involved is higher.

Europe and across the Atlantic. To avoid these challenges, Tallinn is bound to continue insisting on complementarity, non-duplication, and openness of the European initiatives in defence innovation within the framework of its broader policy position that the EU and NATO should seek greater synergies and continue intensifying their cooperation. At the same time, as it is likely that the Estonian policymakers will keep relying on the principle of open market competition in defence procurement, Estonian investments and efforts encouraging and promoting European cooperation in defence innovation are not going to translate into a default preference for European defence products and services (just like the strategic partnership with the United States is not going to lead to a default preference for US products and services).

On the other hand, new European instruments that stimulate the growth of competence, competitiveness, and innovation of industry and science as well as help them mitigate financial and technological risks have become a major attraction to Estonia. The MoD has laid a solid groundwork during the Estonian rotating presidency of the Council of the EU in the second half of 2017 in attuning the country's defence innovation ecosystem to the upcoming new instruments of defence cooperation, and this became a key enabler for an important success in exploiting the opportunities afforded by the EDIDP. In late 2020, a consortium led by Milrem Robotics, iMUGS (Integrated Modular Unmanned Ground System), that includes Estonian as well as German, Belgian, Finnish, French, and Spanish companies and research organisations secured €32.6 million of funding to 'develop a modular and scalable architecture for hybrid manned-unmanned systems in order to address a large range of missions and to enable easy update or modification of assets and functionalities within the system: aerial and ground platforms, command, control and communication equipment, sensors, payloads and algorithms' (European Commission, 2020).

If successful, the project will solidify Estonia's position at the forefront of innovation in this field and will also facilitate the development of its leading companies as system integrators, not just developers of stand-alone platforms or systems. It has also validated the preparatory efforts by Estonia and its European partners – to the extent that some senior European defence officials present Estonia's readiness to tap into the EDIDP and now the EDF as an example for other EU member states to follow. This proactive stance and comprehensive approach have paved the way for Estonian enterprises to be involved

in ten further successful projects (in addition to iMUGS) approved within the EDIDP framework in 2019-20 (see Table 2), securing €16 million of European funding. Among potential future projects, one is focused on maritime unmanned capabilities: Estonia is currently working on assembling a consortium and preparing an application in this area, hoping to launch and lead an EDF project by 2023.

Project	**Lead enterprise /nation**	**Consortium partner(s) from Estonia**
European Cyber Situational Awareness Platform (ECYSAP)	Indra Sistemas (Spain)	Cybernetica
European Command & Control System (ESC2)	Indra Sistemas (Spain)	GT Cyber Technologies
Persistent Earth Observation for Actionable Intelligence, Surveillance and Reconnaissance (PEONEER)	e-GEOS (Italy)	Defsecintel Solutions
Future Highly Mobile Augmented Armoured System (FAMOUS)	Patria (Finland)	Cybernetica
Deployable Cyber Defence Toolbox for Cyber Rapid Response Teams (CYBER4DE)	Baltic Institute of Advanced Technologies (Lithuania)	Talgen Cybersecurity & CR14
Virtual Reality Trauma Simulator (ViReTS)	Exonicus (Latvia)	Criffin R&D (VR Lab)
Mine Risk Clearance for Europe (MIRICLE)	Naval Group Belgium (Belgium)	CAFA Tech
Passive Acquisition by Digital Convergence (PADIC)	SAAB (Sweden)	CAFA Tech & Rantelon
European Approach of AI transversality applied of Defence Programs (AI4DEF)	Terma (Denmark)	Defsecintel Solutions
Joint European System for Countering Unmanned Air Systems (JEY-CUAS)	Leonardo (Italy)	Marduk Technologies

Table 2. EDIDP projects with the Estonian participation approved in 2020 (sources: European Commission and Estonian MoD)

It is notable that the nature of the EDIDP/EDF projects and their requirements seem to fit the Estonian entrepreneurial nature and start-up culture as well as its flexible and goal-oriented culture of public administration, and its open, internationalist outlook. These instruments also appear well suited for a small country with an innovation landscape dominated by small and medium enterprises with limited financial resources and lacking critical mass for complex and challenging programmes. Access to these instruments and

their potential benefits even help sway conservative, cautious and sceptical end-users in the Defence Forces and bring them on board, in order to provide the necessary military perspective and understanding of military capabilities and operational problems and, eventually, perhaps even adopt the resulting solutions if they meet the national military requirements. If it were not for the possibility to apply for the EDF funding in 2022-23 for instance, it is unlikely that the Defence Forces would have endorsed the idea of an unmanned maritime platform project.

CONCLUSIONS

Estonia is a good case study of how the entrepreneurial culture of a self-styled start-up nation can overcome the lack of demand for innovation from the military and, with the strong support of the MoD, lay ground for a vibrant innovation ecosystem that builds on natural strengths in national S&T. The impetus arising from this enterprise-driven innovation ecosystem not only creates new economic opportunities but is also gradually beginning to transform the military culture towards greater openness to innovation and more systematic and structured collaboration with the developers of innovative solutions. Preparing and implementing projects funded by the EDF is likely to serve as an important conduit through which military end-user of the Defence Forces will become involved in developing those solutions, even if their expectations concerning the outcomes might diverge from those of the industry or the MoD. In the end, if those projects deliver results that satisfy real military needs and provide cost-cutting solutions that are robust, reliable, and reduce complexity, there will be a strong interest from the Defence Forces to procure those solutions – with a key caveat that they must be competitive compared to other options available in the open military and commercial markets. ■

REFERENCES

Barigazzi, J. (2021, July 12). EU military projects face delays, leaked document shows. *Politico.* https://www.politico.eu/article/leaked-document-shows-delays-in-eu-military-pact/

Cybernetica. (2018, March 29). *Cybernetica partners with European Defence Agency for the first ever military research programme for next-generation naval surveillance system.* https://cyber.ee/news/2018/03-29/

Eesti Kaitsevägi. (2019, May 7). *Kevadtormil arendavad küberväejuhatuse ajateenijad IT-lahendusi.* https://mil.ee/uudised/kevadtormil-arendavad-kubervaejuhatuse-ajateenijad-it-lahendusi/

ERR News. (2020, March 31). *EDF Saaremaa coronavirus field hospital to start work Thursday.* https://news.err.ee/1070834/edf-saaremaa-coronavirus-field-hospital-to-start-work-thursday

Estonian Aviation Cluster. (2019, August 20). *First drone flew from Estonia to Finland.* https://eac.ee/news/first-drone-flew-from-estonia-to-finland/

Estonian Defence Industry Association (EDIA). (2021). *About Cluster.* https://defence.ee/cluster-and-members/.

Estonian Ministry of Defence. (2010). *National Defence Strategy.* https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf

Estonian Ministry of Defence. (2021, July 21). *Open Cyber Range.* https://kaitseministeerium.ee/en/Open-Cyber-Range

European Commission. (2020, June 15). *Selected Projects – European Defence Industrial Development Programme (EDIDP) 2019: iMUGS – Integrated Modular Unmanned Ground System* [Factsheet]. https://ec.europa.eu/commission/presscorner/detail/en/fs_20_1085

European Defence Agency. (2021). *Defence Data. Data Analysis: EDA Collective and National Defence Data 2017-2019.* https://eda.europa.eu/docs/default-source/documents/eda-collective-and-national-defence-data-2017-2019-(excel).xlsx.

Garage48. (2018, September 30). *Garage48 goes BOOM*. https://garage48.org/blog/garage48-goes-boom

Guardtime. (2019, January 4). *European Space Agency selects Guardtime for Data Provenance.* https://guardtime.com/blog/european-space-agency-selects-guardtime-for-data-provenance

Guardtime. (2020, September 28). *Guardtime awarded contract for European Space Agency Cyber Safety and Security Operational center (C-SOC).* https://guardtime.com/blog/guardtime-awarded-contract-for-european-space-agency-cyber-safety-and-security-operational-center-c

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020: Measuring commitment to cybersecurity.* ITU Publications. https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

Kaitseministeerium. (2013). *Eesti kaitsetööstuspoliitika aastateks 2013–2022*. https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/eesti_kaitsetoostuspoliitika_2013-2022_0.pdf

Kaitseministeerium. (2021a). *Kaitsetööstuse arendustoetused.* Last updated on May 24, 2021. https://kaitseministeerium.ee/et/eesmargid-tegevused/teadus-ja-arendustegevus/kaitsetoostuse-arendusprojektide-konkurss-2021

Kaitseministeerium. (2021b). *Kaitseministeeriumi valitsemisala teadus- ja innovatsioonipoliitika 2021-2030*

Kaitseministeerium (2021c, July 23). *Nokia autonoomne 5G võrk tõstab Eesti küberharjutusvälja võimekust*. https://kaitseministeerium.ee/et/uudised/nokia-autonoomne-5g-vork-tostab-eesti-kuberharjutusvalja-voimekust

Milrem Robotics. (2021a, January 7). *Milrem Robotics rolls out its new Type-X RCV.* https://milremrobotics.com/milrem-robotics-rolls-out-its-new-type-x-rcv/

Milrem Robotics. (2021b, June 22). *Milrem Robotics to expand its operational theatre towards the Moon.* https://milremrobotics.com/milrem-robotics-to-expand-its-operational-theatre-towards-the-moon/

Milrem Robotics. (2021c, May 31). *Krauss-Maffei Wegmann acquires stake in Milrem Robotics.* https://milremrobotics.com/krauss-maffei-wegmann-acquires-stake-in-milrem-robotics/

North Atlantic Treaty Organisation. (2021, June 11). *Defence Expenditure of NATO Countries (2014-2021).* https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210611-pr-2021-094-en.pdf

Paulus, S. (2020). How to secure cryptography against quantum computers?. *Life in Estonia,* no. 55, 47-49. https://issuu.com/eas-estonia/docs/life_in_estonia_no55_issuu.

U.S. Department of Defense. (2016, June 22). *U.S., Estonia Sign Defense Research Agreement*. https://www.defense.gov/Explore/News/Article/Article/810138/us-estonia-sign-defense-research-agreement/

#71
Policy Paper

DEFENCE INNOVATION: NEW MODELS AND PROCUREMENT IMPLICATIONS
The Estonian Case

BY
Tomas JERMALAVIČIUS/ HEAD OF STUDIES, INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY (ICDS)
Martin HURT / RESEARCH FELLOW, INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY (ICDS)

September 2021

The views expressed here are solely those of the author. They do not reflect the views of any organisation.

ARES GROUP

The Armament Industry European Research Group (Ares Group) was created in 2016 by The French Institute for International and Strategic Affairs (Iris), who coordinates the Group. The aim of the Ares Group, a high-level network of security and defence specialists across Europe, is to provide a forum to the European armament community, bringing together top defence industrial policy specialists, to encourage fresh strategic thinking in the field, develop innovative policy proposals and conduct studies for public and private actors.

CONTACT [Pilots]:
Jean-Pierre Maulny, Édouard Simon, Olivier de France, Sylvie Matelly
ares@iris-france.org
+33 (0)1 53 27 60 60

www.iris-france.org/ares
#AresGroup