DAIO Defense AI Observatory

Caught Between Today and Tomorrow

Defence AI in Estonia

Tomas Jermalavičius

DAIO Study 23|20

Ein Projekt im Rahmen von
dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr
Finanziert von der Europäischen Union
NextGenerationEU

About the Defense AI Observatory

The Defense AI Observatory (DAIO) at the Helmut Schmidt University in Hamburg monitors and analyzes the use of artificial intelligence by armed forces. DAIO comprises three interrelated work streams:

- Culture, concept development, and organizational transformation in the context of military innovation
- Current and future conflict pictures, conflict dynamics, and operational experience, especially related to the use of emerging technologies
- Defense industrial dynamics with a particular focus on the impact of emerging technologies on the nature and character of techno-industrial ecosystems

DAIO is an integral element of GhostPlay, a capability and technology development project for concept-driven and AI-enhanced defense decision-making in support of fast-paced defense operations. GhostPlay is funded by the Center for Digital and Technology Research of the German Bundeswehr (dtec.bw). dtec.bw is funded by the European Union – NextGenerationEU.

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und
Technologieforschung der Bundeswehr

Finanziert von der
Europäischen Union
NextGenerationEU

Caught Between Today and Tomorrow

Defence AI in Estonia

Tomas Jermalavičius

DAIO Study 23|20

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

About the Author

Tomas Jermalavičius is Head of Studies at Estonia's international Centre for Defence and Research (ICDS) in Tallinn. His work focuses on defense policy and strategy, regional security and defense cooperation in the Baltic area, the impact of emerging disruptive technologies on security and defense as well as energy security and societal resilience. Prior to joining ICDS in 2008, he worked at the Baltic Defence College, where he was also the editor of the Baltic Security and Defence Review. He also worked in the Defence Policy and Planning Department of the Lithuanian Ministry of National Defence. He holds a BA in political science from the University of Vilnius, an MA in war studies from King's College London, and an MBA degree from the University of Liverpool.

Acknowledgments

The author is grateful to all the interviewees from the Estonian Ministry of Defence, Defence Forces, National Defence Academy and defense companies, who agreed to share their insights and perspectives on this paper. The author is solely responsible for any errors in fact, analysis or omission.

Design

Almasy Information Design Thinking

Imprint

Tomas Jermalivičius, Caught Between Today and Tomorrow. Defence AI in Estonia. DAIO Study 23/20 (Hamburg: Defense AI Observatory, 2023).

Defense AI Observatory | Chair of Political Theory | Helmut Schmidt University
Holstenhofweg 85 | 22043 Hamburg | T +49 40 6541 2776
www.defenseai.eu | contact@defenseai.eu | @Defense_AIO

ISSN (online): 2749-5337
ISSN (print): 2749-5345

Content

1 Summary

Artificial Intelligence (AI) is recognised by the Estonian defence leadership as an increasingly important suite of technologies that will transform society, economy, and defence sector. It is seen as a force multiplier in defence as well as an enabler of better and faster decision-making and greater economy of force. Building upon its solid track record and competence in cybersecurity and cyber defence as well as vibrant ecosystem of AI start-ups, Estonia seeks to integrate into multinational collaborative efforts to develop defence applications of AI. There is a clear understanding that Estonia must remain part of this technology's wave, not least because its defence forces will have to interact and remain interoperable with the allies who are racing forward to embrace AI-enabled capabilities. At the same time, it must avoid costly mistakes of AI adoption and learn from the allies and partners rather than lead.

Concurrently, Estonia's national defence development faces a major challenge of addressing significant capability gaps and building stocks of munitions within the compressed timeframes, given the assessments that the reconstituted Russia's capabilities will pose a direct and existential threat to Estonia by the end of the decade, if not earlier. Combined with resource constraints and inherent scepticism of the military about emerging technologies that so far hold more promise than they deliver, this rapid capability build-up is pushing investments into defence AI development down the list of priorities. Relatively weak internal structure for defence innovation and its incorporation into capability plans, along with absent formal national military doctrine as well as a void in operational analysis and concept development and experimentation, make it even more difficult to mainstream defence AI and prepare better conditions in the defence forces for its successful use.

Great progress in digitalising and preparing public services for the upcoming AI era does not necessarily translate in matching progress on the military side. However, the burgeoning Estonian security, defence and space industry, dominated by agile start-ups and small or medium enterprises, is emerging as a major driver of defence AI development, assisted also by government's support grants. The industry has been particularly successful in exploiting the European level funding opportunities for multilateral collaborative technology development, with two Estonian enterprises also leading large consortia of partners to develop robotic solutions for land and maritime domains. Enterprises in Estonia are quickly emerging as important sources of concepts of AI applications in defence and security, even though their products and services based on those concepts are often likely to reach foreign customers sooner than the Estonian ones.

On the other hand, war in Ukraine is increasingly supplying insights into what effects the use of AI can have in a battlespace when combined with old technologies and pique interest in how small states such as Estonia could employ this technology to offset imbalances vis-à-vis a numerically superior enemy force. The interest of the Estonian military in defence applications of AI is furthermore stimulated by the demonstration of those applications by the allied forces stationed as well as exercising in Estonia. Some of the in-house development projects aimed at digitalising ‘kill webs,’ enabling better information sharing and enhancing common battlespace awareness are also emerging as important vehicles for introducing AI. The need to provide feedback and consultation to the Estonian enterprises developing innovative AI-based solutions is further enhancing the military’s awareness and may potentially lead to future capability requirements better cognizant of the AI’s role and impact – provided it finds a way to effectively link bottom-up interest with top-down planning.

Most importantly, a wave of procurement of state-of-the-art weapon systems and equipment is bringing the Estonian military into close contact with advanced technologies that will include, as part of the package, elements of AI, further necessitating increasing knowledge and competence in AI technology. In this regard, Estonia will have to strengthen its military training and education system and find ways of more effectively leveraging conscription and reserve training for enhancing AI competence. It will have to attract and retain more hardware and software engineering talents – with multiple implications to strategic personnel policies and human resources management – produced by the world-class Estonian education system where such disciplines as robotics and coding from early age are a new normal.

2 Thinking About Defence AI

As for many nations, Estonia's journey into defence applications of AI started in the civilian sector, where its main strengths lie in information technology, digitalisation of public services, cybersecurity and, increasingly, semi-autonomous robotics. AI, defined as 'a system based on an autonomous software algorithm capable of learning, allowing it to perform tasks that typically require human intelligence,'[1] is making its way into the civilian applications through these key areas, with the national strategy providing the overall direction for the public and private stakeholders. Under the lead of the Ministry of Economic Affairs, the second iteration of this strategy is about to be released by the end of 2023, thus giving a better conceptual basis, context, and coherence to the overall effort.[2] It is important to note, however, that the level of digitalisation – fairly high in various international indices[3] – and AI proliferation in the civilian public and private sectors of Estonia may not necessarily be a reliable indicator of the level of digitalisation and AI adoption across the defence sector, where several factors discussed in this paper conspire to slow the process down.

Of course, defence is an integral part of the overall national endeavour through the inter-agency process, although in the Estonian context 'defence' must be treated not as a unitary player but rather as a quadriptych of interacting – usually mutually supporting but occasionally discordant – systems: policy and administration (Ministry of Defence, MoD), military (Estonian Defence Forces, EDF), industry and science, and the volunteer sector (e.g. Estonian Defence League, EDL). Each of these systems may have their own set of views, understanding, assessments and ideas about various issues such as the future applications of AI in defence that would normally be harmonised through a national defence policy or strategy.

2.1 Estonia's Strategic Culture of Pragmatism

Estonia's strategic culture shapes its defence AI approach in important ways.[4] First and foremost, Estonia relies on NATO and the EU to ensure national security and particularly in managing a persistent, multifaceted, and overwhelming threat posed by Russia. This key tenet rests on clear-eyed understanding of how small Estonia is and how large the power asymmetry with Russia is, that Estonia needs to offset to survive as a sovereign nation. Reliance, however, is not seen as a one-way street. Rather it requires both maximising Estonia's contribution to the

[1] The strategy, however, more resembles a roadmap and catalogue of practical measures rather than a full-fledged comprehensive strategy that one may expect to be labelled as "strategy." See: Estonia's national artificial intelligence strategy 2019-2021.

[2] "State to make ready AI strategy by year-end."

[3] Estonia ranked 9th in the EU in 2022 according to the Digital Economy and Society Index (DESI); 8th in the UN's E-Government Development Index in 2023, and 18th in the World Digital Competitiveness Index 2023.

[4] For more on the Estonian strategic culture, see: Salu/Männik, "Estonia," pp. 99-112; Atmante/Kaljurand/Jermalavičius, "Strategic Cultures in the Baltic States: The Impact of Russia's New Wars," pp. 53–82.

collective enterprise wherever possible and being an active and involved member of these organisations. Therefore, Estonia wants to act as a security producer and not only a consumer. This also entails continuously investing into credible national defence capabilities and allocating the necessary financial resources to this end. Since re-establishing its independence after 1990, Estonia has never diminished the value and importance of military defence in national security, despite the fact it had to be rebuilt from scratch.

Second, Estonia's security culture reflects the understanding that developing national military defence and further focusing it on homeland (territorial) defence is confined neither to national boundaries – thus requiring close interaction (and interoperability) with allies and ability to effectively integrate their contributions – nor solely to the defence sector. Thus, it requires the ability to draw upon inputs from broader society, including the corporate sector and science. Estonia therefore follows a whole-of-society approach. Third, its strategic culture is focused on practical solutions that deliver concrete results, preferably within a relatively short period of time. In general, Estonia shies away from slow-motion conceptualisations and over-strategising, even though in such sectors as cybersecurity the value of multi-stakeholder strategy-making to bring together all relevant experts and sustain common understanding is well appreciated.[5]

This pragmatic and practical mindset is important as it shapes how defence AI is approached – with a high degree of uncertainty-induced caution in the military mixed with sufficient space for entrepreneurial attitude on the industry and policy side 'to get things done'. It also reflects the military's general approach to technology adoption that is underpinned by a thorough understanding of Estonia's narrow margin of error in initiating (or not initiating) major change and limited resources to pursue any new high-flying ambitions.[6] This approach also trickles down to the doctrine level, whereby Estonian military regards itself as just too small and lacking the critical mass for developing a general national military doctrine or specialised doctrines. Thus, Estonia directly relies on NATO's doctrines and publications.[7] Such pragmatism means it cannot and will not be a trailblazer of defence innovation until and unless the evolving nature of military threat from Russia makes a rapid introduction of some unique solution – that no one else in the Alliance has yet adopted at scale – a clear and urgent imperative.

[5] The fact that the national AI strategy is named kratt – after a mythical character in the Estonian folklore that simply gets things done if there is a problem – is a good reflection of such a practical approach to problem-solving. For more information, see: "What is a kratt?"

[6] A good example of this cautious, cost-conscious, and risk-averse attitude is a recent interview by the commander of the Estonian Navy, in which he stated that, due to resource constraints, Estonia could not afford developing unmanned alternatives for mine countermeasures (MCM) while at the same time maintaining and improving crewed platforms. In his view, the country should stick with what works well. Unmanned solutions could be integrated as add-ons thus enabling gradual evolution. This would provide time to observe and analyze if and to what extent more radical concepts developed by other Allies materialize in the long term. See: Suurkask, "Mereväe ülem: laevastike ühendamine on olnud edukas [Merger of the fleets was successful]," p. 10.

[7] Interview with a defence planning staff officer from the EDF HQ, 14 July 2023.

2.2 The Current Defence AI Strategy Void

Estonia does not yet have a dedicated defence AI policy. This reflects to some extent the state of affairs in which even the overall national defence strategy is no longer drafted and published as a separate document (the last iteration was 2010).[8] Yet, given that AI is likely to become one of the major drivers in transformation of defence capabilities and conduct of warfare, this formal policy void in defence is unlikely to persist in the long-term. This is not least the case because there should be some clear definition of defence AI articulated and agreed upon to guide the future efforts in this field, which is currently lacking and could be one of the factors hampering further progress. Different players in the Estonian defence sector then express different understanding, ranging from views that AI is a very broad field (or suite of technologies) with a yet unclear impact on defence to views that AI is mostly about autonomy in weapon systems.

The MoD is gradually rising to the challenge of drafting a formal defence AI policy or strategy, while the current approach tantamount to informal policy on AI-related issues is shaped not only through its R&D and defence industrial policies, but also by the developments in the framework of NATO, the EU and minilateral initiatives that the MoD is keen to participate in. As a member of NATO, Estonia subscribes to the Alliance's AI Strategy of 2021, and as a member of the EU, it participates in defence cooperation frameworks that have elements of AI technology and AI-enabled capabilities (e.g. PESCO, European Defence Fund, European Defence Agency, etc.). Furthermore, it joined the US-led AI Partnership for Defence initiative – a 'coalition of the willing' that reinforces, amplifies, and benefits from the US leadership in the field.[9] This is seen as recognition of Estonia's strengths in cybersecurity – a field where synergies with AI are particularly important.

The MoD's key strategic message is that AI is pivotal to future military capabilities and that Estonia must keep abreast of the developments in this field and contribute to them in the areas of its technological excellence and expertise. Although the understanding of what capabilities will be transformed or created as a result of AI's use is still lagging in the wider Estonian defence establishment, the basic principles that the MoD follows in relation to AI projects for defence are:[10]

1. They must add value.
2. They must simplify rather than complicate employment of military capabilities.
3. They should be dual-use technologies.

[8] Elements of it are now dispersed between the National Security Concept and the Long-Term National Defence Development Plan, a 10-year planning document which is classified. See: Eesti julgeolekupoliitika alused [Fundamentals of national security].
[9] "AI Partnership for Defense (AI PfD)."
[10] Roundtable discussion with the MoD representatives, 2 September 2022.

There is also strong determination at the policymaking level to get Estonia involved in a web of multinational collaborative initiatives that will allow tapping into the results, ensuring interoperability and avoiding early (and often costly) mistakes made by 'first movers' in the field. Such involvement also compensates for the lack of critical mass – in terms of human and financial resources – that hampers small nations such as Estonia in their technological and capability development ambitions.

Just as many other fields, AI in defence is seen in Tallinn as a field for collaborative efforts rather than as a solo undertaking. The greater this international involvement, the more likely it becomes that ideas, concepts, and principles that circulate in those fora will be transferred to the national setting and coalesce into a more coherent formal defence AI policy in the future. In this regard, two key partners emerge as pivotal for Estonia's followship. First, the United States are a global leader in AI technology and a strategic partner of immense importance for fiercely transatlanticist Estonia. In addition, the UK is as another long-standing and trusted strategic partner in military affairs.[11] The UK is a framework nation for both the Joint Expeditionary Force (JEF) in which Estonia participates alongside other ten nations and NATO's enhanced Forward Presence (eFP) battlegroup deployed in Estonia. It has recently committed a high-readiness brigade for Estonia's defence to be integrated into with the EDF for regular exercises and deployments, when necessary, thus making interoperability with the British forces a key consideration for Estonia.[12] The UK also happens to be among the leading technological powers in the Alliance, further boosting its relevance to Tallinn's defence AI thinking.

The pivotal role of these two nations does not imply that other partners do not matter. Estonia participates in the French-led European Intervention Initiative and hosts French troops as part of NATO's eFP, so the evolution of the French defence AI strategy and technology leadership will certainly be of interest to Tallinn. Likewise, collaboration with Germany – a relative laggard in defence AI but a source of military technology and equipment of growing importance to Estonia – will shape Estonia's defence AI agenda and thinking. Last, but not least, some of the like-minded small allies with similar strategic outlook such as Finland with whom common defence procurements (e.g. of air surveillance radars, self-propelled howitzers and anti-ship cruise missiles) became a routine as well as Latvia and Lithuania with whom long-standing trilateral defence cooperation across a very broad range of issues is a permanent fixture of Estonian defence policy are likely to be among partners of first choice in keeping up with the defence AI trends in the Alliance.[13] In terms of co-operating with small Allies, successful co-operation with the Nor-

[11] See: Jermalavičius/Billon-Galland, British Power in Baltic Weather.

[12] "Eesti ja Ühendkuningriik allkirjastasid pikaajalise kaitsekoostööleppe [Estonia and the United Kingdom signed long-term defence cooperation agreement]."

[13] "Regional cooperation."

wegian partners in implementing practical projects focused on cybersecurity and e-governance have also positioned it as an important partner for Estonia in future AI-related endeavours.[14]

2.3 Defence AI Ethics: Yes, But…

In terms of general thinking about defence AI, Estonia seeks to subscribe and adhere to the overall principles of its responsible and ethical use, although remaining sceptical of the normative regulation (e.g. arms control treaties in relation to lethal autonomous weapon systems) and advocating instead norms-building approach – something that also defined its approach to international legal norms in cyber domain.[15] According to defence officials, ethical aspects of AI are high on the MoD agenda whenever technology policy and support to the specific projects are discussed.[16]

The government's thinking – including how it defines autonomous weapon systems and their governance framework – is best reflected in the joint Estonian-Finnish paper presented to the working session of the GGE CCW[17] in 2018.[18] In particular, the paper articulates that 'autonomy should be understood as a capability to perform the given task(s) in a self-sufficient and self-governing manner' and argues that 'humans must retain ultimate control over decisions of life and death,' while adding that, as a minimum legal standard, 'humans must exercise such control over a weapon system as may be necessary to ensure the operation of that weapon system consistently with international law.' Crucially, it sets a baseline for the human operator competence in the armed forces that the EDF will have to consider in its training and education requirements. According to the paper, human operators must possess, 'as a minimum, an understanding of the performance characteristics of the system and of the operational environment' and, consequently, 'if the operator lacks such an understanding, or based on that understanding has no confidence as to compliance with the law, he/she must not permit the weapon to deliver force.'

Some influential Estonian voices from the technology community, however, are pressing for more urgent action to establish a robust international AI governance framework. Among them is Jaan Tallinn, one of the founders of Skype and the

[14] "Norwegian university, Estonia begin cyber cooperation talks;" "Open Cyber Range."

[15] Crandall/Allan, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," pp. 346-368.

[16] Roundtable discussion with the MoD representatives, 2 September 2022.

[17] Group of Governmental Experts [on Lethal Autonomous Weapons] to the Convention on Certain Conventional Weapons

[18] "Categorizing lethal autonomous weapons systems – A technical and legal perspective to understanding LAWS (Submitted by Finland and Estonia)."

Cambridge Centre for the Study of Existential Risk that focuses, among other issues, on the risks posed by AI. He is one of the signatories of the open letter of March 2023 which stated that 'powerful AI systems should be developed only once we are confident that their effects will be positive and their risks will be manageable' and called for an immediate 6-month pause in developing AI systems more powerful than GPT-4.[19] Reflecting on the outcome later in 2023, he argued:

> We wanted to see how people responded, and the results were mindblowing…People are justifiably alarmed that a handful of companies are rushing ahead to build and deploy these advanced systems, with little-to-no oversight, without even proving that they are safe. People, and increasingly the AI experts, want regulation even more than I realized. It's time they got it.[20]

At the same time, however, members of Estonia's government and the business community are concerned that multinational and the EU efforts (e.g. the upcoming EU's AI Act) will stifle development of innovative AI-based solutions in defence and will stall the emerging vibrant ecosystem of AI industry enterprises that are potential suppliers of such solutions.[21] Given the focus of Estonia on promoting these ecosystems, restrictive international and EU regulation seems to pose a distinct risk to its future ability to contribute to collective defence AI endeavours. Policy-wise the MoD and other relevant government organisations are bound to continuously balance between nurturing the Estonian AI start-ups ecosystem and responding to the pressures from various directions to constrain the development of technology seen as posing unacceptable level of risk.

2.4 Industrial Push and Military Caution

Estonia's defence, security, and space industry has indeed been one of the key drivers of defence applications of AI in Estonia – not only through adoption of AI in cyber defence, but also in developing unmanned systems, counter-UAV capabilities, and digital battlefield management solutions. It has also been, thanks to the industry-funded studies and CD&E efforts, at the forefront of thinking about the future of warfare where AI-enabled autonomous military systems are dominant in the battlespace.[22] Some of the enterprises working with AI-enabled solutions are in direct contact with the armed forces and industrial partners in Ukraine, seeking to harness their insights and experience from the ongoing war and leverage them towards new concept and product development. There is natural self-interest of

[19] "Pause Giant AI Experiments: An Open Letter."
[20] "As Six-Month Pause Letter Expires, Experts Call for Regulation on Advanced AI Development."
[21] "Tehisintellekti võimalustest ja mõjudest [On the opportunities and impact of Artificial Intelligence]."
[22] Interview with a defence industry representative, 20 December 2022.

the industrial players to promote such concepts and secure the buy-in of their customers, but it seems that, in Estonia, they have more success in securing state support by virtue of representing the start-up nation culture – unafraid to take bold risks, experiment and build new markets abroad – rather than through captivating and compelling visions of future war and warfare.

The military, on the other hand, is supposed to play a major role in envisioning the future warfare and capability requirements that it will bring about. In Estonia's case, however, such visionary thinking has been limited by the realities of defence development, whereby the EDF has had to address most basic capability gaps and needs first, before turning their eyes to more advanced capabilities and emerging disruptive technologies. This pivot is at its infancy but already underway, with parts of the military establishment already considering future scenarios – building upon NATO's work such as 'The NATO Warfighting Capstone Concept (NWCC)',[23] but also alarmed by the developments in the technology sector of the main adversary, Russia, and inspired by certain elements of war in Ukraine. For these military thinkers, AI will be a major part of capabilities in most of the military functions – from ISTAR[24] to indirect fire support and armoured manoeuvre to combat service support and military administration – in the coming decades.[25]

In line with most of the thinking among Western military, AI is viewed as an enabler of dense 'kill webs' characterised by compressed OODA[26] loops and associated with greater effects on the battlefield.[27] In some of the most progressive thinking, compartmentalised parts of the future battlespace (e.g., absorbing and delaying first waves/echelons of assault by the enemy along particular axes of advance) would be fully unmanned, even though always with human operators 'on the loop.'[28] Most relevant for small nations like Estonia, AI-enabled capabilities such as unmanned systems are regarded as a means to limiting manpower losses that even a reserve-based wartime organisation such as the EDF would struggle with, and, furthermore, as a compensator for the lack of human resources.[29] Concerning the latter, it is estimated that headquarters staff at various levels could be reduced several times by introducing AI tools for planning and decision-making, thus freeing up manpower for other functions. For example, one military planner contended in an interview for this study that a division's planning staff could be cut down from 200 to about 20-50 or even fewer if advanced AI tools are introduced and jobs shift from drawing charts to judging AI-generated courses of action.[30] In

[23] NATO Warfighting Capstone Concept.
[24] ISTAR: Intelligence, Surveillance, Target Acquisition, and Reconnaissance.
[25] Interview with a defence planning staff officer from the EDF Headquarters, 14 July 2023.
[26] OODA: Observe, Orient, Decide, and Act.
[27] Interview with a senior leader of the National Defence Academy, 21 December 2022.
[28] Allik/Fahey/Jermalavičius/McDermott/Muzyka, The Rise of Russia's Military Robots.
[29] Interview with a defence planning staff officer from the EDF HQ, 14 July 2023.
[30] Interview with a defence planning staff officer from the EDF HQ, 14 July 2023.

these assessments, smaller command staffs will, in turn, mean greater survivability as the footprint of command posts will be smaller.

The military, however, remains cautious and reserved about AI and AI-enabled capabilities so far and does not have an overarching vision for it. In some discussions, they question the degree to which this will really be transformative, as the nature of war and warfare are unlikely to change and will entail violence, uncertainty, and chance. They readily admit that AI is already playing havoc with and opening new opportunities in the information warfare domain. However, this is regarded as affecting the political layer of defence more than the military directly and therefore the understanding and management of the associated risks should be a matter for the political and policy-level attention in the first place.[31] In general, they remark that AI will first transform the societies before it transforms defence and that the latter will not be in full swing in the coming decade or so anyway. Such remarks justify the focus of the Estonian thinking and planning on the challenges of more immediate future such as building greater mass and reserves – especially in the light of Russia's war against Ukraine and its repercussions for Estonia's security.[32] Some military planners contend that, due to technology developments, some form or degree of AI-enabled and assisted man-machine teaming might become possible by the end of this decade.[33] However, the overall sentiment is that the entire field of emerging disruptive technology is too unpredictable beyond a time horizon of 5-10 years and that the main line of effort must be focused on addressing more immediate capability gaps in Estonian defence system.

Still, at the most senior levels of defence command, there is already a understanding that something profound is afoot. In some regards, the Allied presence in Estonia is a catalyst of a gradual change in perceptions and – at least – the rhetoric of the military. The protracted period of experimenting with various iterations of the indigenous Estonian platform unaccompanied by any serious conceptual work on the military side about its potential seems to have created a blind zone in the perspective of the Estonian military. However, the British forces bringing unmanned ground vehicles (UGV) to the exercises in Estonia served, according to one interviewed expert, as an 'eye-opener' to some of the military leadership about the pace and potential impact of such systems on the capabilities of Estonia's key allies.[34] Given the importance of maintaining interoperability with these allies and the capacity to act together, this is a major consideration for envisioning Estonia's future capabilities and the role of AI in them. As the same analyst observed, the AI-driven world of the future will be divided into 'haves' and 'have

[31] Interview with a senior EDF leader, 6 July 2023.
[32] Interview with a senior EDF leader, 6 July 2023.
[33] Interview with a defence planning staff officer from the EDF HQ, 14 July 2023.
[34] Interview with a researcher from the National Defence Academy, 9 May 2023.

nots,' so Estonia must start thinking about how to remain among the former, and the military should be part of this process.

Likewise, Russia's war against Ukraine is serving as a source of insights about elements of warfare based on the adoption of various new technologies (including commercial-of-the-shelf) that is prompting some progressive thinking – even though data from primary sources on the use of these technologies by Ukraine remains very limited and, according to one senior Estonian officer, does not even provide enough material for lessons identified, let alone learned.[35] Nonetheless, the war in Ukraine is accelerating ongoing efforts to prioritise defence capabilities like ISTAR, that requires greater reliance on ubiquitous and interconnected sensors, or digitised command and control (C2) processes to accelerate information sharing and decision-making. Long-range stand-off fires integrated with comprehensive sensor webs also receive greater attention in the Estonian military thinking, as does the role of loitering munitions. These preferences reflect that Ukraine's superior situational awareness and its ability to quickly share a comprehensive battlespace picture vertically and horizontally have been particularly noted by the Estonian high command.[36] With the Estonian defence development entering a more ambitious and high-tech phase, discussions about the emerging role of AI in those and other next generation capabilities – some of which Estonia has never possessed before – will become more pertinent and urgent.

At the same time this view will be tempered by the observation made at the highest command level that there is no single 'silver bullet' in the war in Ukraine, despite some advanced weapon systems being 'elevated to the podium' at various points in time. Rather it is the combined and coordinated use of different systems that is seen as most impactful in delivering the desired effects. Commander of the EDF General Martin Herem, in his interview to the Estonian military journal, was quite blunt by saying that Ukraine would have performed even better if, contrary to the conventional wisdom that generals always prepare for the last war and therefore fail to prepare for the future one, it had been indeed preparing for such a 'last war,' when mass and firepower played a decisive role.[37] As a consequence, he argued, Estonia should invest in more mass and firepower, while adopting technologies (including, presumable, AI-enabled) that make their application more efficient and effective.

This perspective is further reinforced by some influential military views from outside Estonia according to whom many things to be learned from the war in Ukraine for instance, are related to the importance of the neglected old domains

[35] Interview with a senior EDF leader, 6 July 2023.
[36] Jäärats, "Kaitseväe juhataja: kõik algab tahtest oma riigi kaitsta [Chief of defence: everything starts with the will to defend one's country]," pp. 6-13.
[37] Ibid.

such as electronic warfare or large-scale use of well-established capabilities such as engineering, artillery or armour.[38] The phrase by the UK Chief of the General Staff Sir Patrick Sanders that 'you can't cyber your way across the river' resonated with the Estonian top military brass particularly well.[39]

Moreover, future efforts to develop AI-enabled military capabilities will also have to contend with a high degree of caution in the Estonian society. A public opinion survey conducted in late 2021 revealed that 62% of the respondents agreed that AI can become more dangerous than nuclear weapons, while 85% did not trust the application of autonomy in military capabilities and 89% were against delegating 'life or death' decisions to autonomous military systems.[40] Partly reflecting this sentiment, but also to meet high standards sought at the EU level for the EU-funded projects and hedge against potential liability risks in a more distant future, companies such as Milrem Robotics have been instituting clear and robust ethical AI governance policies that reflect the current state of thinking in Estonia about corporate responsibility and accountability in developing and fielding defence AI applications.[41]

[38] "Key Conversation: General Christopher Cavoli."
[39] "General Sir Patrick Sanders, Chief of the General Staff, opens the RUSI Land warfare conference with his speech."
[40] Idarand, Reining in autonomous weapons: Impact on military innovation – An Estonian perspective.
[41] "Policy of Ethical Development of Systems with Intelligent Functions."

3 Developing Defence AI

Developing AI-enabled solutions is not consciously prioritised by the Estonian MoD when selecting and supporting R&D projects. For instance, in the framework of the defence industrial policy, the MoD provides annual grants to enterprises for developing solutions that are highly innovative, contribute to enhancing capabilities, and have export potential. But the inclusion of AI may not always warrant success in the selection process. Some of those successful projects may indeed contain elements of AI and, with time, are more likely to do so given the overall trajectory of technological development in the commercial sector, but there is currently no deliberate demand pull from the defence organisation to do so. There is some expectation though that the number of such projects will grow and, at some point, will reach critical mass, perhaps warranting the establishment of a formal policy or strategy to guide increasingly AI-centric development efforts.[42]

This 'bottom up' approach at the policy level is echoed by military practice. The EDF is quite open to testing new solutions such as robotic platforms with various units in the field and providing feedback to the developers. However, it does not place any special emphasis on those solutions being AI-aided or AI-enabled. The focus is firmly set on whether they resolve any specific technical, tactical, or operational problem and address an existing capability gap rather than on laying ground for introducing new paradigms and concepts of future warfare. The capacity of the EDF to define generic requirements for future capabilities and develop concepts for their employment remains very limited, further constraining the demand pull for AI-based solutions.

This is not to say that the ground is not being laid for such solutions. As an example, the efforts to stand up the Estonian Division (ESTDIV) – a formation that will serve, among other things, as a 'plug and play' environment for NATO Allies deploying to Estonia – require addressing various shortcomings in the C4I[43] systems. For instance, three national defence communication systems with related databases are not able to interact and exchange data, necessitating data transfers by human operators. ESTDIV development is leading the EDF towards a fully integrated system that will, in essence, become an equivalent to a 'digital backbone' for the entire defence force.[44] Such integration and further digitisation of command and the resource management process is a prerequisite for future AI-based applications, including those of the allies whose units will become part of the ESTDIV. This will have to overcome the proclivity of national contingents contributed by various Allies to limit information sharing across national lines – a procedural and policy rather than a technical problem besetting the already deployed eFP battlegroups and requiring the extensive use of staff liaison officers.[45]

[42] Roundtable discussion with the MoD representatives, 2 September 2022.
[43] C4I: Command, Control, Computers, Communications, and Intelligence.
[44] Interview with a senior EDF leader, 6 July 2023.
[45] Briefing by the command staff of the eFP battlegroup, 28 September 2023.

In addition, the EDF has been making steady progress with two in-house development projects that form the basis and core of its digitalised battlespace management:

- **KOLT (Kaitseväe olukorra ja lahinguteadlikkuse süsteem)**
  KOLT is a Defence Forces Situational and Combat Awareness System that was initiated in 2014-15 by conscripts and reservists with IT background and has since become an EDF-wide solution used by various units and tested during major exercises such as Kevadtorm (Spring Storm).[46] Some small development projects to use AI to facilitate its various functions (e.g. mapping, handwriting recognition, etc.) are being pursued by the EDF, showing how a major technological step forward opens opportunities for more AI-related "bottom up" ideas and add-ons that may not necessarily have been part of the original intent and design.

- **TOORU**
  TOORU is a fire support system that seeks to combine fire managers, fire control centres, calculation points, weapon systems, fire support officers, logistical components, and aerial fire control elements into a single digitalised "kill web." Conceived as one of the modules of KOLT, it already generates datasets from various fire systems (e.g. K9 self-propelled howitzers, FH70 towed howitzers, M252 and M41D mortars, etc.) and is envisaged as an excellent platform for introducing AI solutions aiming to reduce the workload of human operators in preparing fire missions (e.g. performing calculations).[47] Thus, it has already been designed from the start as a system that will both generate data for training AI algorithms and integrate new capabilities based on AI.

Overall, however, there is a sense that the defence organisation needs take a step back and assess the potential and need for AI across a range of capabilities. The MoD is providing funding for a study project by the Estonian National Defence Academy who set out, together with Germany's Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), to examine the potential requirements and narrow down the broad spectrum of AI applications to more specific priority areas.[48] This should lay the ground for stronger demand pull and the defence AI strategy with a degree of top-down guidance as well as facilitate greater coherence in selecting, encouraging, and supporting development projects in the future.

[46] "Kevadtormil arendavad küberväejuhatuse ajateenijad IT-lahendusi [Cyber Command's conscripts develop IT solutions during the Spring Storm]."
[47] Dieves, "Kiirema tulelöögi nimel – TOORU projekt [For the sake of faster fire support – TOORU project]," Academia Militaris, pp. 12-16.
[48] Interview with a researcher from the National Defence Academy, 9 May 2023.

It should not come as a surprise, though, that Estonian enterprises take a lead not only in thinking about, but also developing AI-enabled solutions, often in close collaboration with the University of Tartu and Tallinn University of Technology (TalTech), two leading universities, whose R&D work provided basis for several successful spin-offs and start-ups, and the National Defence Academy. A vibrant innovation ecosystem has helped set up several companies that also develop defence products with AI applications such as

- Milrem Robotics developing UGV[49]
- Threod Systems developing unmanned aerial vehicles (UAV)[50]
- DefSecIntel Solutions working on sensors and surveillance systems[51]
- SensusQ focusing on data sharing and intelligence management platforms[52]
- Marduk Technologies focusing on Counter-UAV solutions[53]
- Rantelon working on Electronic Warfare and communication systems[54]
- Krakul providing Internet of Things for defence[55]
- Wayren working on digital communication platforms[56]
- Vegvisir developing mixed reality situational awareness systems[57]

The Estonia cybersecurity sector also has several enterprises – some well-established and some in the start-up phase – that work on AI-enabled solutions. Chief among them are Cybernetica (encryption technologies),[58] CybExer Technologies (cyber range technology and services),[59] Guardtime (data security and blockchain technology applications)[60] and others. Many of them are collaborative partners of the Foundation CR14[61] as well as Estonia-based NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE)[62] – important players in the defence AI development ecosystem.

Inevitably, given that the defence AI ecosystem is populated by many small start-ups and young enterprises, this is a very dynamic scene, with many new entrants appearing each year, while other enterprises migrate in and out of the defence field or disappear entirely. Still, companies like Milrem Robotics, Cybernetica, DefSecIntel Solutions, Threod Systems or Rantelon have been around for quite

[49] For more information, see: https://milremrobotics.com/ (last accessed 23 November 2023).
[50] For more information, see: https://threod.com/ (last accessed 23 November 2023).
[51] For more information, see: https://www.defsecintel.com/ (last accessed 23 November 2023).
[52] For more information, see: https://www.sensusq.com/ (last accessed 23 November 2023).
[53] For more information, see: https://www.marduk.ee/ (last accessed 23 November 2023).
[54] For more information, see: https://rantelon.ee/en/ (last accessed 23 November 2023).
[55] For more information, see: https://krakul.eu/ (last accessed 23 November 2023).
[56] For more information, see: https://wayren.ee/ (last accessed 23 November 2023).
[57] For more information, see: https://www.vegvisir.ee/ (last accessed 23 November 2023).
[58] For more information, see: https://cyber.ee/ (last accessed 23 November 2023).
[59] For more information, see: https://cybexer.com (last accessed 23 November 2023).
[60] For more information, see: https://guardtime.com/ (last accessed 23 November 2023).
[61] For more information, see: https://www.cr14.ee/ (last accessed 23 November 2023).
[62] For more information, see: https://ccdcoe.org/ (last accessed 23 November 2023).

some time and grown into significant players with international reach. Some of them are R&D-intensive in their business model as well. Most of the companies involved in developing products and services for defence are members of the Estonian Defence and Aerospace Industry Association, an umbrella organisation that provides a framework for international networking, represents the industry's interests in relation with the government, and assists with the development of various business capacities and competencies.[63]

In addition, two well-established Estonian companies, Milrem Robotics and Baltic Workboats, are coordinating major pan-European consortia financed within the framework of the European Defence Fund:[64]

- **iMUGS**
  Launched in 2020, iMUGS strives 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).'[65] It heavily builds on TheMIS UGV platform that, in turn, draws upon the results of the MoD-funded R&D project conducted during the 2000s. The consortium also incorporates an Estonian producer of UAVs, Threod Systems, as well as the National Defence Academy. Although TheMIS is perhaps the most famous and versatile Estonian UGV platform, Milrem Robotics is now setting its eyes on developing a robotic combat vehicle (RCV) called Type X for a more specialised 'wingman' role in armoured units.[66] In either case, these platforms are supposed to be part of a broader system of systems where AI in C2 as well as AI-enabled autonomy will be major pillars of the new capabilities.

- **EUROGARD**
  Launched in 2022, this project is less ambitious than iMUGS and has set out to 'build a vessel capable of a range of different autonomous operations in coastal areas.'[67] In this case, Estonian leadership of the consortium draws heavily on the expertise in developing autonomous maritime surface platforms for civilian applications that has already seen through deployment of a research vessel capable of autonomous operations at sea in collecting various data.[68]

[63] For more information, see: https://defence.ee/ (last accessed 23 November 2023).
[64] For companies from a small country, coordinating large multimillion euro consortia with members across Europe marks a significant proof of their achievements in pursuing technologies that underpin the ambitions of these teams.
[65] "iMUGS – Integrated Modular Unmanned Ground System."
[66] "Type-X RCV."
[67] "EUROGUARD – EUROpean Goal based mUlti mission Autonomous naval Reference platform Development."
[68] "Scientists launch Estonia's first autonomous maritime research vessel."

Robotics, of course, is but one of the areas in which Estonian industry is integrating AI solutions. With cybersecurity being a significant part of the defence and security industrial ecosystem, the interest in AI applications in this domain is growing exponentially. More importantly, cybersecurity is viewed as a pivotal element of future secure, safe, and trustworthy AI systems, allowing Estonian companies to leverage their competitive advantages and competence in larger projects led by their Allies. As an example, Estonia's Cybernetica signed a contract to develop cryptographically secure AI with US Office of Naval Research. According to the company's press release, 'the PAI-MACHINE project will optimise algorithms for collaborative AI applications so that allies can share work together for the common good without having to share their confidential data in full.'[69] Projects such as this will potentially address the abovementioned issue of information sharing between national contingents (e.g. in ESTDIV).

The opportunities related to the European Defence Fund are also pursued in this field. In the cycle of proposals for 2023, Foundation CR14 is leading a consortium of 15 nations and 28 organizations named AIDA (Artificial Intelligence Deployable Agent). The consortium aims to develop a set of TRL7[70] level software agent prototypes that rely on AI algorithms for their operation in the cyber incident management cycle. The proposal puts a strong emphasis on AI trustworthiness and facilitated adoption, both from a cultural, ethical, and organizational perspective, but also through technical methods such as the use of synthetic data for efficient machine-learning and implementation of appropriate technical frameworks to ensure resilience against adversarial AI. The project is expected to improve protection of the EU's critical infrastructure (e.g. satellite communications), alleviate human resource availability problems in cybersecurity, and enhance military mobility through securing operations of autonomous vehicles and aircraft. The decision of the European Defence Fund is anticipated in 2024.[71]

[69] "Cybernetica signs contract to develop cryptographically secure artificial intelligence with US Office of Naval Research."
[70] TRL: Technology Readiness Level.
[71] E-mail communication from Foundation CR14, 1 December 2023.

4 Organising Defence AI

Estonia's approach to organising defence AI reflects its overall organisation for defence innovation. The system is quite decentralised and rests on the 'bottom up' initiative from within the defence organisation as well as stimulating and facilitating the innovation ecosystem outside the government structures – in the civilian universities and enterprises. It also focuses on enhancing relations with foreign partners. This ensures that ideas for development and experimentation are relevant to national and international end-users, while also staying connected to wider trends in the transatlantic and European arenas. At the same time, however, this approach lacks overall strategic coherence, continuity in projects, and momentum in harnessing such disruptive technologies as AI.

4.1 A Broad Alliance for Defence AI…

Estonia's defence policy has always placed strong emphasis on the so-called 'broad national defence,' whereby all national stakeholders – public and private – ought to have a role in ensuring the nation's defence and provide capabilities for the common efforts.[72] When it comes to defence technology and innovation, this whole-of-society and whole-of-government approach in practice often means that the MoD spends portions of the defence budget for the projects of civilian research establishments or companies that have potential or clearly identified military applications. In addition, the MoD representatives are included in various interagency working groups (e.g. on the development of government 'cloud' services) and councils (e.g. Research Council that drafts the national science and technology strategy).

Overall, the AI-related efforts at the national level – just as digitalisation of governance and cybersecurity – are coordinated by the Ministry of Economic Affairs and Communication, through the office of the undersecretary for digital development. The MoD, in turn, has consolidated numerous activities within a single department of defence innovation, even though other departments such as those overseeing NATO and the EU affairs or national defence information systems, contribute to its mission from their respective roles. The department is responsible for defining R&D and defence industrial policies and managing the committees that oversee implementation of certain aspects of these policies. It has recently established a position for coordinating all AI-related matters and, eventually, coordinating development of the Estonian defence AI policy.

[72] National Defence Strategy.

On a working level, however, the MoD must draw upon the expertise and contribution of state agencies and other entities outside its formal structure but within its area of governance. One such agency is the Estonian Centre for Defence Investment, where management of most procurement programmes was centralised in 2015.[73] The centre draws technical requirements of equipment acquisition and has specialised managers for various categories of equipment. AI will inevitably become part of these requirements across a range of capability projects, thus necessitating a certain level of competence and the capacity to incorporate impartial external advice from the national and allied S&T base.

Moreover, the MoD area of governance includes organisations that offer maximum flexibility in combining various sources of funding such as the European Defence Fund, the Defence Innovation Accelerator for the North Atlantic Alliance (DIANA), and the NATO Innovation Fund to incorporate national and foreign public and private sector partners into common projects and serving as hubs for testing various practical solutions. Foundation CR14, established and supervised by the MoD, is key to the Estonian efforts to advance cybersecurity and cyber defence solutions, with AI rapidly becoming an important part of this effort.

CR14 operates cyber ranges that are used by various stakeholders (including NATO Cooperative Cyber Defence Centre of Excellence) to conduct exercises and test new solutions.[74] These cyber ranges also help to generate datasets that can be used by the data owners (e.g., nations that provide 'blue teams' at Exercise Locked Shields[75]), for example, to train AI algorithms in cyber defence. In a clear acknowledgment of the key role of CR14 in channelling Estonia's national expertise in cybersecurity to its foreign partners and representing the country in collective AI policy development endeavours, the foundation's CEO has also been appointed to represent Estonia in NATO's Data and Artificial Intelligence Review Board (DARB).

The MoD also provides support for non-governmental entities and programmes initiated by other stakeholders. One such particular programme is CyberNorth, a cybersecurity AI accelerator, launched by Start-up Wise Guys, a major Estonian technology start-up accelerator, in cooperation with the Estonian Defence and Aerospace Industry Association in 2019.[76] Since then, it has become an accelerator within NATO's DIANA network, in which Estonia-based accelerators also provide a launchpad for start-ups focused on AI, cyber, space and green-tech (energy and propulsion).[77] This not only brings the Estonian entrepreneurial expertise in start-

[73] For more information, see: https://www.kaitseinvesteeringud.ee/en/ (last accessed 23 November 2023).
[74] "Cyber Ranges."
[75] "Locked Shields."
[76] "Estonia invites new cyber security startups – a unique cyber security and AI accelerator to be opened."
[77] "Tallinn, Tartu science parks to operate NATO innovation accelerator DIANA;" "Accelerator programme."

up creation and growth as well to bear on developing AI-powered solutions for defence, but also enhances Estonia's profile as a multi-spoke hub and integrator of such innovation benefiting the entire Alliance.

4.2 …Meets Defence Forces that Are About to Get AI Ready

While the MoD appears reasonably well organised and prepared to pursue defence AI-related ambitions, the EDF has a poorer organisational preparedness. For a start, there is no centralised innovation management function at the EDF headquarters, and the office of the Chief of Defence no longer has a position of chief scientific or innovation adviser to provide advice on what should be included in the top-level defence planning and capability development guidance to the services and commands. If there is any substantive consideration given to the EDTs, and AI in particular, it is supposed to be included through the long-term planning processes managed by the defence planning department of the HQ (J5). In reality, however, as demonstrated by the failure to stand up an autonomy programme initiated to provide centralised coordination from the HQ for this particular area of technology, it is all too easy to abandon organisational measures if they are not regarded as a strategic priority and do not have a powerful high-level advocate in the organisational hierarchy.[78] Interest in and initiatives to advance innovative solutions that include AI thus basically reside at the level of individual units and communities of practice (e.g. military intelligence, signals and communications, or electronic warfare).

The EDF, however, has attempted to centralise its interaction with the civilian S&T community and defence industry via the Applied Research Centre of the National Defence Academy. This has proven a useful measure to provide a hinge between external innovators and end-users within the EDF.[79] But it has not been able to build the capacity that is quite central for the military's ability to define the need for innovative solutions – operational analysis / operational research (OA/OR). It is also pushed into too many directions such as securing funding from the EU sources through consortia, supporting the educational mission of the academy and addressing the requirements for research in social sciences, thus diluting its ability to focus on the application of the EDTs, including AI, in defence.[80] It is also too far removed from the centralised planning processes at the EDF headquarters,

[78] Interview with a defence industry representative, 20 December 2022.
[79] Jermalavičius/Hurt, Defence Innovation: New Models and Procurement Implications – The Estonian Case.
[80] Interview with a researcher from the National Defence Academy, 9 May 2023.

making it less impactful than it should be in future-proofing long-term defence development plans.[81]

Existing challenges notwithstanding, long-term planning may undergo some important changes soon. The ongoing project to redesign planning methodology will open some important opportunities to consider EDTs in the future capability mix. Some of the upcoming or already introduced elements are as follows:[82]

1. The methodology will identify points in time when various external (e.g. defence industry) or internal (e.g. the National Defence Academy) stakeholders will have a possibility to engage defence planners in a discussion on technological aspects of the capabilities, with a view of incorporating their ideas into the plans.
2. There will be a clearer segmentation between several different sets of forces along the time axis. The current set of forces is driving short-term investments to address the existing capability gaps. The medium-term set is a force vision for the next 10 years, and the long-term force set looks at a time horizon of up to 20 years.
3. Services will be provided some funding to experiment with the technologies and capabilities that may become part of their capability mix in the future, in the expectation that their analysis and lessons will inform their views about investing into EDTs and shape their inputs into the defence plans.
4. As a guiding principle, introducing and operating a new capability to replace obsolescence will have to fit within the cost ceiling set for each unit at a certain level, thus preventing 'cutting edge' technology adoption from driving ever increasing operating costs that come with the ever more complex and sophisticated (but often 'gold-plated') capabilities.

Additionally, some of the more recent new force structure elements need to pursue new technological solutions within a very dynamic threat environment due to their core mission. Estonia's Cyber Command established in 2018 is one example. It brings together various previously disparate elements such as the Signals Battalion, the ICT development centre, the strategic communications unit, and others with the mission to conduct operations in cyberspace, including information operations, making it one of the domain-specific combatant commands alongside land, air, and naval forces. It is also providing support to other EDF services and commands as well as agencies in the area of the MoD's responsibility when it comes to information technology, infrastructure, and services, thus also making it akin to a C3I agency or combat service support organisation.[83] By virtue of this

[81] Interview with a senior leader of the National Defence Academy, 21 December 2022.
[82] Interview with a defence planning staff officer from the EDF HQ, 14 July 2023.
[83] "Küberväejuhatus [Cyber Command]."

dual role, but particularly due its exposure to the domain where AI applications are emerging very fast, it thus potentially becomes a major gateway for AI diffusion into the military organisation, especially given the synergies and overlaps between cyber operations, ISTAR, electronic warfare, information operations, and C3I management. This will be contingent on greater acceptance of its role and mission across the EDF: one very senior military commander from the Land Forces is known to have complained that the Cyber Command's birth was akin to a 'workplace accident' – implying that this was rather unfortunate and should not have happened. Furthermore, its success will also rest on how well it will be able to combine its various tasks. Currently its cyber and information operations, for example, are quite poorly integrated.[84]

The Cyber Command, however, frequently represents the EDF in the interagency setting where digital governance architecture is developed, giving it access to and possibilities to advance civil-military synergies in cyber domain and harness dual-use nature of AI technology applied in this domain. Uniquely among the EDF services and somewhat contrary to efforts to centralise EDF's R&D coordination at the Applied Research Centre of the Defence Academy, it is also tasked with R&D work in its domain, thus linking it with CR14 and NATO CCDCOE as well as external partners in the wider defence innovation ecosystem.

This is, to some extent, mirrored by the Estonian Defence League (EDL) – a paramilitary organisation for territorial defence manned by volunteers. Its Cyber Defence Unit was stood up in 2010 and provides a platform for the volunteer members of the EDL from all walks of life to exchange their knowledge, train together and act when required.[85] The unit extends its remit into information operations as well, and it would be natural to expect that, with the proliferation of AI tools in the civilian cyber and strategic communication sectors, members of this unit will bring ideas and solutions from these sectors to bear on their military tasks in the EDL. As Ukraine's example shows, this pathway of spinning-in technologies into the military domain can be as impactful as the classical defence innovation and technology acquisition pathways.[86]

Contrary to these new elements, the discipline of long-term defence planning seems to have been put on the backburner recently. This will most likely also affect its interplay with defence innovation. Currently, Estonian defence development is driven by the fundamental assumption that Russia – a primary and existential threat to Estonia – will reconstitute most of its lost capabilities by the end of this decade if not sooner, necessitating a steep increase in Estonia's national defence

[84] Interview with a Cyber Command's reservist, 30 November 2023.
[85] "Kaitseliidu koosseisus luuakse küberkaitseüksus [Cyber defence unit is being created within the Defence League]."
[86] Champion/Safronova, "From Robots to Recycled Vapes, Ukraine's War Effort Gets Inventive."

capabilities. As one defence expert remarked, the country is now basically trying to compress a ten-year cycle into four years or even less to arm and prepare itself as much as possible ahead of what it regards as a quickly approaching point of a direct military confrontation with Russia.[87] In this mindset, there is little space left for considering long-term implications of various EDTs – including in terms of interoperability with Allies. Only innovative solutions that are mature enough and readily available – and therefore can be quickly introduced into the capability mix or adapted to military uses from their civilian origins – draw attention of the planners and military leadership. Interoperability, in the meantime, is becoming narrowly focused – at least in some minds – on a question of interchangeability, i.e. whether munitions (e.g. artillery shells) of one producer can be used on platforms of another producer.[88]

[87] A senior Estonian defence official at the Toom Kooli Strategic Talks, 15 November 2023.

[88] For more on the notion of interchangeability, see: Landrum/Gleason/Corrado, "Turning standard ammunition into sharable ammunition."

5 Funding Defence AI

For several years, Estonia has been one of the few NATO Allies spending more than two percent of its Gross Domestic Product (GDP) on defence. Russia's full-scale war against Europe has shifted the terms of the spending debate within NATO, whereby this level is being advocated by Tallinn as a floor rather than ceiling – with the national effort matching the political rhetoric. While the defence budget of 2021 was €749M (2.2% of GDP), it grew to €1.1bn (2.73% of GDP) in 2023 and is expected to reach €1.3bn (3.2% of GDP), despite the struggle with the economic slowdown and growing budget deficit.[89]

Such growth, however, does not deliver a very large pool of funding in absolute terms (in which Estonia's budget is among the smallest in NATO) or create too much additional space for funding R&D/R&T. The needs for capability development and stockpiles build-up are considerable and, along with the need to compensate the impact of inflation on personnel pay, crowd out more long-term requirements. As a senior military official said in a closed door briefing to media and think-tank representatives in September 2023, the overriding principle in budget allocation – reflecting the aforementioned assessment of the military threat from Russia – currently is whether a programme or project is likely to deliver tangible results within the next 4-5 years.[90]

As the defence organisation essentially resides in the emergency mode, spending on long-term technology and innovation pursuits becomes, to a large degree, a luxury item. Moreover, Estonia's defence R&D spending has been below the EDA's target of 2% of the defence budget already for years, reflecting different priorities and a degree of scepticism in the defence establishment towards these kinds of investments. As of 2021 (i.e. before the war in Ukraine), Estonia was spending just €5.1M on R&D and only €1.1M on R&T (using EDA's definitions).[91] However, it seems that the bonanza of fresh funding for defence is spilling over into the R&D investments, despite the long-standing scepticism and the pressure of current events. According to the MoD figures, its R&D investments were €5.6M in 2022 and €7.8M in 2023. Surprisingly, they are projected to more than double in 2024 and reach €12.1M.[92] This, however, is only about half of the EDA's benchmark of 2% of the defence budget.

Given current R&D/R&T budgeting methods, no data is available to identify specific spending priorities such as defence AI, for example. This makes it very difficult to gauge the MoD's funding levels for it. Nonetheless, some defence industry

[89] "2024. aasta riigieelarve eelnõu [Draft budget of 2024]."
[90] A senior EDF leader during the closed door briefing to foreign think-tankers and journalists in the framework of the Annual Baltic Conference on Defence 2023, Ministry of Defence of Estonia, 28 September 2023.
[91] Defence Data 2020-2021: Key Findings and Analysis
[92] E-mail communication from the MoD of Estonia, 20 November 2023.

support grants go to the projects the title of which explicitly or implicitly suggest inclusion of at least some elements of defence AI:[93]

- In 2021, for example, the MoD supported a project entitled 'Prototype of Unit of an automated mini-drone-station with "search & find" AI detection model software' by DefSecIntel Solutions.
- In 2022, the MoD supported an Intelligent Decision Support System (IDSS) by Sensus Septima and Vegvisir Mixed Reality Situational Awareness System by Defencesphere.
- In 2023, Wayren and Defencelab received MoD support for a project called 'Tactical Data Exchange Platform with Armoured Troops Awareness System Integration'.

Overall, however, the financial MoD support for these and similar projects remains very modest, ranging between €72,000 and €200,000. Despite the lack of a more aggregate budget total for defence AI spending, these grants are an important element of stimulating the industry's interest in defence markets, including defence AI development and especially among young enterprises and start-ups.

In contrast, Estonia receives far larger sums related to AI projects from the private financial sector or external sources. The OECD AI Policy Observatory estimated that Estonia's overall AI start-up ecosystem received a cumulative investment inflow worth USD437M as of 2023, which has almost tripled in size since 2021.[94] Although this dwarfs anything that the MoD can offer to finance defence AI development, the benefits of such investments in the broader AI sector are bound to seep into defence-related projects at some point, given that defence increasingly attracts technology entrepreneurs eager to exploit new opportunities and benefits from EU and NATO funding sources.

In fact, multinational sources of funding like the European Defence Fund (and one of its precursors, EDIDP) as well as Horizons Europe (Horizons 2020 in the previous cycle) have emerged as pivotal in advancing AI-related developments in Estonia. The latter is still something that defence research and innovation projects are not eligible for (those are addressed via the European Defence Agency's instruments) but given the dual-use nature of AI and the reliance of the Estonian defence innovation on the civilian S&T base, this restriction eventually becomes trivial. A cursory look at the websites of many Estonian enterprises involved in defence projects reveals that many of them also run projects funded by Horizon Europe.

[93] "Kaitsetööstuse arendusprojektide konkurss 2023 [Defence industry development projects competition 2023]."
[94] "AI in Estonia."

The European Defence Fund (and EDIDP prior to it), on the other hand, has direct relevance and significance to the Estonian enterprises involved in the defence sector, as highlighted in Chapter 2. Estonian enterprises have been particularly successful in tapping into this source, with 16 international projects that involve companies from Estonia receiving an overall total of almost half a billion euros of funding. Six of those projects also receive Estonian MoD co-funding.[95] Again, it is hard to isolate the Estonian share of the funding without additional research or identify what share is devoted to AI-related projects. Some of the MoD co-funded projects, however, are bound to include AI one way or another and may even source this technology from Estonia,[96] judging from the participating companies such as Milrem Robotics, Cybernetica, Cafa Tech[97] or Criffin,[98] which are involved in incorporating AI into their products and services.

If and how these projects will deliver tangible capability gains for the EDF, however, is an open question. For now, the military is fully satisfied with the arrangement that minimally taxes the defence budget and shifts the financial and technological risks to industry and the EU, while drawing upon the military end-user's knowledge and feedback. That is also the reason why it is possible that EU or NATO funded development projects will eventually become a stimulant of interest and demand from the EDF when formulating their capability requirements, thus accelerating adoption of technology that those projects seek to advance.

[95] "Estonia achieves unprecedented success with European Defence Fund projects."

[96] Cyber and Information warfare toolbox (EUCINF), Collaborative Combat for Land Forces (LATACC), Naval Collaborate Surveillance (E-NASCOS), Modelling, Simulation and Simulator Integration Contributing to Decision-Making and Training (FEDERATES)

[97] For more information, see: https://cafatech.com/ (last accessed 23 November 2023).

[98] For more information, see: https://criffin.com/ (last accessed 23 November 2023).

6 Deploying and Operating Defence AI

In a country without a formal defence procurement policy in place, it is difficult to assess whether AI-enabled capabilities are prioritised in any way – this would require analysis of technical requirements of each procurement on a case-by-case basis. However, as an informal matter, the Estonian MoD and its procurement agency adhere to the principle that past support to the development projects does not warrant procurement of the outcomes. Rather tenders evaluate all offers and select the best match with the requirements while remaining agnostic about the source of technology (as long as it is not China, Russia, or other similar originators) or whether it has domestic roots and has drawn upon investments by the Estonian taxpayers.[99]

Despite this, officials insist that most projects supported with MoD grants within the defence industrial policy successfully secure sales with the domestic customer.[100] This is partly the result of a close consultation process between military end-users and project teams in ensuring continuous feedback to best meet military customer needs. At the same time, those procurements serve to provide a reference for export markets, as international defence customers often pay attention whether the home country of the product, service or technology is among its buyers. Thus, the development projects described earlier are almost certain to make their way – or have already been included – into the EDF's mix of capabilities.

In addition, the defence forces also gain experience in operating, for example, robotic systems as part of field tests and on missions. The THeMIS UGV by Milrem Robotics was operated by the Estonian contingent in French-led Operation Barkhane in Mali, where three EDF platoons used the platform for patrols and transportation of supplies. This deployment provided the producer with valuable insights into the performance of the platform under harsh conditions (e.g. desert terrain, hot temperature) and enabled the military to gain experience in operating these systems to better understand their added value and the challenges in operating them.[101]

Assessing the actual deployment of AI-enabled capabilities, however, remains complicated as they often constitute the most sensitive part of the package, especially in such domains as ISR or cyber, thus making them subject to high levels of classification. It can only be inferred that procuring ISR UAVs from Estonian producer Threod Systems for tactical and operational level combat service support functions could potentially feature in-built AI elements – if not yet currently then definitely in the future. Likewise, the ongoing implementation of the in-house

[99] Jermalavičius/Hurt, Defence Innovation: New Models and Procurement Implications – The Estonian Case.
[100] Roundtable discussion with the MoD representatives, 2 September 2022.
[101] "Milrem Robotics' THeMIS UGV completes first deployment in Mali proving its effectiveness and reliability."

projects, KOLT and TOORU (see chapter 3) are opening possibilities for deploying AI tools to assist the processes in these systems.

However, the major ongoing shift in the nature of defence procurements will be a game changer for future AI-enabled capabilities. During the first two decades or so since restoring the independence the EDF had to rely mostly on donated equipment or purchases of second-hand systems with some notable exceptions such as long-range air surveillance radars or short-range air defence and guided anti-tank missile systems. But over the last few years we are witnessing a surge – undoubtedly driven by the threat assessments and increased defence funding – in acquiring brand-new equipment and weapon systems with cutting edge technology.[102] Many of these systems like

- Blue Spear (5G SSM) land-to-sea cruise missile system
- Blocker PM16 naval mines
- M142 HIMARS multiple rocket launchers
- K9 Thunder 155mm self-propelled howitzers
- Iris-T SLM medium range AD/MD system
- Long-range loitering munitions (LMs)

will already include AI or provide possibilities for incorporating it through upgrades or connectivity with AI-assisted battle management systems. Interestingly, some of these procurements (e.g. anti-ship missiles) have not been part of the long-term development plan discussed in the previous section but resulted from a strong political push accompanied by additional funding decisions by the government.[103] This demonstrates that, in some cases, technology can make its way into the Estonian defence capabilities mix without a methodical and complex long-term process underpinning that plan.

It is obvious that the EDF will have to find a way of integrating the AI elements that come already as part of the purchased systems with its in-house development projects that may come to feature such elements as well. So far, this has not emerged as a matter of concern. For instance, the TOORU module has been installed on K9 Thunders without any major difficulty, but the former does not yet possess AI-enabled features that would require complex integration with the built-in systems. This is bound to change, and therefore participation of the national developers in the multinational end-user clubs and their interaction with the suppliers will play a crucial role in avoiding costly integration problems in the future.

[102] Gosselin-Malo, "Estonia's global arms buying spree seeks drastic combat gains."
[103] "Rannakaitse täisvõimekuse saavutamiseks kuluks paar aastat [It would take a few years for the coast guard to reach its full capacity]."

At the same time, the fact that some of these procurements are already undertaken jointly with foreign partners – such as Blue Spear and K9 Thunder with Finland and Iris-T with Latvia – opens opportunities for collaborative technology adoption pathways as envisaged by the emergent defence AI policy principle articulated by the MoD. Herein lies a risk that the Estonian end-users will just not make sufficient effort to fully and comprehensively understand the AI technology packaged in the acquired cutting-edge systems, as it will primarily be examined, understood, and vouched for by the lead partners in joint procurement projects. This may not result in the outright adoption of a black-box solution that would contravene Estonia's position which holds that operators need to understand built-in AI. Rather it might create a grey-box situation, whereby EDF operators will probably have some understanding, but will depend upon the explanations of more irregular AI behaviour from their foreign military partners. In any case, these procurements will inevitably bring AI-related issues to the very core of the EDF's future capability mix, requiring changes in such aspects as training and education or personnel management policies.

7 Training for Defence AI

A decade and a half ago, in the wake of the cyber-attacks on Estonia that followed the relocation of the Soviet military statue and the street riots instigated by Russian agents,[104] a commonplace lament in the Estonian security debates was how limited the awareness of cybersecurity and cyber defence was in the society at large and among the military in particular. As the AI era is dawning, a similar observation – that the military chain of command has very limited insights into what AI is or will be capable of – is sometimes resurfacing.[105] It took just a decade to overcome the cyber ignorance and establish a dedicated command, which demonstrates that a learning and adoption curve of similar duration may well occur when it comes to AI.

Doctrinally, the EDF is not well prepared to advance force-wide learning outside the whole-of-alliance framework, as there is no formal national military doctrine in place and the entire system often directly relies on Allied Joint Publications (AJP) and Allied Tactical Publications (ATP).[106] Without the national process to think through and develop ideas as well as to establish them as part of the Estonian doctrine, the EDF becomes highly dependent on the progress of NATO in incorporating AI into its AJP/ATP family of documents. This may serve as an opportunity, given that a small country alone can hardly address the challenge of drawing an overarching doctrine for joint multidomain operations, for example.

Many of the preconditions for effective learning about AI, however, could be laid in the professional military education (PME) system, with the National Defence Academy and the Baltic Defence College playing a pivotal role. [107] For the time being, however, AI is addressed as a fairly minor subject within larger technology and innovation modules and courses, even though air and naval officer training provides some more extensive exposure to this particular technology. Likewise, the training of non-commissioned officers (NCO) for the land component – by far the most dominant service in the EDF – does not provide any significant skillset in managing AI as part of the military capabilities and tactics, techniques, and procedures (TTP).[108]

As the Estonian defence system relies heavily on the mobilisation reserve, conscript, and reserve (re-fresher) training programmes naturally constitute the core of the training activities undertaken by the EDF. These programmes undergo continuous modifications and adaptation, depending on, among other factors, when the defence acquisition programmes and projects deliver new weapons systems and

[104] Juurvee/Mariita Mattiisen, The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict.

[105] Roundtable discussion with the MoD representatives, 2 September 2022.

[106] Interview with a senior leader of the National Defence Academy, 21 December 2022; Interview with a defence planning staff officer from the EDF Headquarters, 14 July 2023.

[107] The Academy covers levels 1 and 2 of the PME and awards graduate and post-graduate degrees, whereas the College covers levels 3 and 4 and provides (as an option) a post-graduate degree from the Latvian National Defence Academy.

[108] Interview with a defense planning staff officer from the EDF Headquarters, 14 July 2023.

equipment or their upgrades. In most cases, conscripts – and the units manned by conscripts – must demonstrate their ability and be certified to use these systems before being transferred to active reserve after 8-11 months of service, while the EDF's professional core needs to gain deep understanding of those systems well ahead of its actual fielding. This gives a head-start of a few years before any major influx of AI technology takes place – including potentially together with the joint procurement partners (e.g. Finland and Latvia), given that pooled training and logistics are often touted as key benefits of collaborative procurement projects.

As discussed, the policy thinking suggests that AI-enabled systems should not be used if the operators do not possess sufficient understanding of how the AI behaves in the respective systems. Therefore, readiness of individual and collective training system to deliver upon this principle becomes critical. Military leaders of the EDF acknowledge that, to be a competent end-user of sophisticated weapon systems, many of which will be drawing upon AI, the organisation will require ever growing number of soldiers-technicians – with the backgrounds and skill sets related to STEM[109] disciplines – in addition to the usual soldiers-tacticians.[110] This, in turn, shifts the onus onto the national higher education and vocational training system, whose graduates then go through the basic and advanced military training programmes. With STEM disciplines lacking popularity, the MoD and EDF are now working on co-operative arrangements with various civilian schools to give them a boost through scholarships, secure service contracts, and other incentives, in the expectation that future demand for technical skills – including those relevant to AI – will be met by sufficient supply from the national education system.[111]

In fairness, the EDF is not arriving at the threshold of the AI era being deprived of talents. Using the ProgeTiiger programme framework and tools aimed to enhance technology literacy starting as early as kindergarten,[112] the world-class Estonian education system is already dedicating attention to such subjects as coding and robotics from early age.[113] After all, this is in line with what a future highly digitalised and AI-powered society and economy will demand. The EDF can tap into this trend through conscription – which also serves as one of the recruitment tools into full-time military employment – and, as the roots of KOLT demonstrate, is even capable of encouraging, capturing, and scaling up the innovations that arise from this talent pool. However, it is a different subject, whether it is capable of motivating and retaining the best and brightest in the fierce competition for talents in a

[109] STEM: Science, Technology, Engineering, Mathematics.

[110] Interview with a senior leader of the National Defence Academy, 21 December 2022.

[111] "Kaitseressursside Amet soovib stipendiumikonkursiga suunata noori rohkem tehnikavaldkondasid valima [The Defense Resources Agency wants to direct young people to choose more technical fields with a scholarship competition]."

[112] "ProgeTiger – Estonian way to create interest in technology."

[113] Over the last few cycles, Estonian schoolchildren have consistently ranked among top ten in the world by the results of PISA tests. In 2018 (the latest available cycle), Estonia ranked 8th in mathematics and 4th in science. See: Schleicher, PISA 2018: Insights and Interpretations.

small labour market where private enterprises in the high-tech sector offer much higher salaries and benefits while not exposing their employees to the constraints and risks inherent to military service.

As it currently stands, the conscription and reserve training system, however, is not a perfect solution, as military service is mandatory only for men and voluntary for women, thus depriving the EDF of easier access to a significant part of a demographically aging and shrinking talent pool. Notwithstanding the fact that younger generations might have natural instincts for handling high-tech systems, the current approach also fits relatively poorly with the world of complex technology as the effective mastering of new technologies requires longer periods than the current duration of conscript service or the amount of reserve refresher training. It also locks many of the full-time professionals into repetitive training cycles, giving them fewer opportunities to experiment, innovate, and develop new skills or TTPs. Nonetheless, the current approach exposes the EDF to and synchronises the armed forces with the broader societal trends among which AI proliferation will inevitably be a major one, thus making it inevitable that, as far as AI adoption is concerned, the military will, sooner or later, follow where the rest of the Estonian society is heading to.

8 Conclusions

Estonia's gradual embrace of defence AI illustrates the challenges and opportunities of broader defence innovation in a country where strong entrepreneurial drive and the government's willingness to facilitate and leverage technological progress meet the conservative and cautious military focused on quick build-up of capabilities required to counter an existential threat to the nation. The lack of a strong, sustained, and systematic demand pull for AI-enabled solutions from the military side is compensated, to some degree, by the enthusiastic, dynamic, and conceptually well-versed AI innovation ecosystem that has taken root in Estonia because of its strengths in cyber and robotic technologies. Russia's war against Ukraine and emerging AI-enhanced capabilities in key allies such as the UK, United States, and France serve as additional motivating factors for the Estonian military to increasingly pay attention on how to apply AI to shape future warfare.

Despite its relative novelty, AI is not finding Estonia's defence organisation writlarge unprepared or just passively watching the incoming wave. Thanks to efforts by the MoD and industry, it is well integrated into NATO and EU fora where defence AI is a central theme. This also provides opportunities for Estonia to join leading countries in large EU-funded defence projects focusing on defence AI. The military has been open to experiments and provides feedback to developers, using the National Defence Academy as the main interlocutor. The EDF's Cyber Command and the communities of practice where AI is making major strides (intelligence and electronic warfare) are further amplifying this effort. Further development of in-house projects such as KOLT and TOORU are laying further ground for the future exploitation of AI. If successful, the reform of the long-term defence planning process will provide incentives for the military services, branches, and units to pay more attention to what longer-term future challenges might be and how to prepare for them.

Some preconditions for the successful adoption of defence AI, however, are clearly lacking. There is no vision in place for the EDF to become a data-centric organisation or how far-reaching its digitalisation will be. Without an overarching national defence strategy, AI policy and a national military doctrine, a lot of AI-related (as well as generally technology-driven) innovation might come to lack the scale, coherence with the national defence objectives, and eventual impact. The overwhelming focus on short and medium-term capability requirements and needs leave long-term foresight side-lined and marginalised. Almost entirely absent operational analysis/operational research capacity and concept development and experimentation structures in the EDF make it difficult to systematically estimate the impact of emerging disruptive technologies on warfighting and cast the existing organisational practices in a critical light. This is further reinforced by superficial coverage of AI and related technologies at all levels of the PME system.

With further growth, the above shortcomings will, sooner or later, be addressed. It is clear though that Estonia is not setting itself an ambition to be first adopter of AI in defence, but rather seeks to tread carefully and avoid costly mistakes, while remaining integrated with the efforts and networks of the allies. Further AI diffusion, it seems, will take place through

- continuous flow of ideas, concepts and practical solutions from the civilian sector into the military via industry engagement and involvement of civilian talents in national defence;
- interactions with the foreign allies and partners (including in the development of new command structures), and
- integration of new capabilities into its force structure.

Estonia will likely continue leading in some niche areas, where national strengths and civilian inputs are evident, such as AI in cybersecurity and cyber operations or software for autonomous platforms and sensors. Overall, however, the country will largely follow more resourceful allies and their defence industries. For a small nation, being a solid, competent, and active team player will be more important in AI adoption for defence than pursuing own high-flying visions or revolutionary transformations.

Literature

"2024. aasta riigieelarve eelnõu [Draft budget of 2024]," Riigikogu (The Parliament of Estonia), 18 October 2023, https://www.riigikogu.ee/fookusteemad/2024-aasta-riigieelarve-eelnou/ (last accessed 23 November 2023).

"Accelerator programme," DIANA undated, https://www.diana.nato.int/accelerator-programme.html (last accessed 23 November 2023).

"AI in Estonia," OECD, undated, https://oecd.ai/en/dashboards/countries/Estonia (last accessed 23 November 2023).

"AI Partnership for Defense (AI PfD)," Joint Statement, 15-16 September 2022, https://www.ai.mil/docs/AI_PfD_Joint_Statement_09_16_20.pdf (last accessed 22 November 2023).

"As Six-Month Pause Letter Expires, Experts Call for Regulation on Advanced AI Development," Future of Life Institute, 21 September 2023, https://futureoflife.org/ai/six-month-letter-expires/ (last accessed 22 November 2023).

"Categorizing lethal autonomous weapons systems – A technical and legal perspective to understanding LAWS (Submitted by Finland and Estonia)," Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, CCW/GGE.2/2018/WP.2, 24 August 2018, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/257/85/PDF/G1825785.pdf?OpenElement (last accessed 22 November 2023).

"Cyber Ranges," CR14, undated, https://www.cr14.ee/ranges/ (last accessed 23 November 2023).

"Cybernetica signs contract to develop cryptographically secure artificial intelligence with US Office of Naval Research," Cybernetica, 22 September 2023, https://cyber.ee/resources/news/ONR-2024/ (last accessed 23 November 2023).

"Eesti ja Ühendkuningriik allkirjastasid pikaajalise kaitsekoostööleppe [Estonia and the United Kingdom signed long-term defence cooperation agreement]," Ministry of Defence of Estonia, 11 October 2023, https://kaitseministeerium.ee/et/uudised/eesti-ja-uhendkuningriik-allkirjastasid-pikaajalise-kaitsekoostooleppe (last accessed 22 November 2023).

"Estonia achieves unprecedented success with European Defence Fund projects," Ministry of Defence of Estonia, 28 June 2023, https://www.kaitseministeerium.ee/en/news/estonia-achieves-unprecedented-success-european-defence-fund-projects (last accessed 24 November 2023).

"Estonia invites new cyber security startups – a unique cyber security and AI accelerator to be opened," Enterprise Estonia, November 2018, https://investinestonia.com/estonia-invites-new-cyber-security-startups-a-unique-cyber-security-and-ai-accelerator-to-be-opened/ (last accessed 23 November 2023).

"EUROGUARD – EUROpean Goal based mUlti mission Autonomous naval Reference platform Development," European Commission, 2022, https://defence-industry-space.ec.europa.eu/system/files/2023-06/EUROGUARD%20-%20Factsheet_EDF22.pdf (last accessed 23 November 2023).

"General Sir Patrick Sanders, Chief of the General Staff, opens the RUSI Land warfare conference with his speech," British Army, 28 June 2022, https://www.army.mod.uk/news-and-events/news/2022/06/rusi-land-warfare-conference-cgs-speech/ (last accessed 23 November 2023).

"iMUGS – Integrated Modular Unmanned Ground System," European Commission, 2020, https://ec.europa.eu/commission/presscorner/api/files/attachment/865736/EDIDP%20-%20iMUGS.pdf (last accessed 23 November 2023).

"Kaitseliidu koosseisus luuakse küberkaitseüksus [Cyber defence unit is being created within the Defence League]," Ministry of Defence of Estonia, 29 November2010, https://kaitseministeerium.ee/et/uudised/kaitseliidu-koosseisus-luuakse-kuberkaitseuksus (last accessed 23 November 2023).

“Kaitseressursside Amet soovib stipendiumikonkursiga suunata noori rohkem tehnikavaldkondasid valima [The Defense Resources Agency wants to direct young people to choose more technical fields with a scholarship competition],” Defence Resources Agency, 3 November 2023, https://kra.ee/kaitseressursside-amet-soovib-stipendiumikonkursiga-suunata-noori-rohkem-tehnikavaldkondasid-valima/ (last accessed 24 November 2023).

“Kaitsetööstuse arendusprojektide konkurss 2023 [Defence industry development projects competition 2023],” Ministry of Defence of Estonia, last updated 10 November 2023, https://kaitseministeerium.ee/et/eesmargid-tegevused/teadus-ja-arendustegevus/kaitsetoostuse-arendusprojektide-konkurss-2023 (last accessed 24 November 2023).

“Kevadtormil arendavad küberväejuhatuse ajateenijad IT-lahendusi [Cyber Command’s conscripts develop IT solutions during the Spring Storm],” Estonian Defence Forces, 7 May 2019, https://mil.ee/uudised/kevadtormil-arendavad-kubervaejuhatuse-ajateenijad-it-lahendusi/ (last accessed 23 November 2023).

“Key Conversation: General Christopher Cavoli,” CEPA, 27 September 2023, https://cepa.org/transcripts/key-conversation-general-christopher-cavoli/ (last accessed 23 November 2023).

“Küberväejuhatus [Cyber Command],” Estonian Defence Forces, undated, https://mil.ee/uksused/kubervaejuhatus/ (last accessed 23 November 2023).

“Locked Shields,” NATO CCDCOE, undated, https://ccdcoe.org/exercises/locked-shields/ (last accessed 30 November 2023).

“Milrem Robotics’ THeMIS UGV completes first deployment in Mali proving its effectiveness and reliability,” Milrem Robotics, 5 May 2020, https://milremrobotics.com/milrem-robotics-themis-ugv-completes-first-deployment-in-mali-proving-its-effectiveness-and-reliability/ (last accessed 24 November 2023).

NATO Warfighting Capstone Concept (Norfolk: NATO Allied Command Transformation, 2021), https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/ (last accessed 22 November 2023).

“Norwegian university, Estonia begin cyber cooperation talks,” ERR, 29 April 2018, https://news.err.ee/827342/norwegian-university-estonia-begin-cyber-cooperation-talks (last accessed 30 November 2023).

“Open Cyber Range”, Ministry of Defence of Estonia, last updated 30 July 2021, https://kaitseministeerium.ee/en/Open-Cyber-Range (last accessed 30 November 2023).

“Pause Giant AI Experiments: An Open Letter,” Future of Life Institute, 22 March 2023, https://futureoflife.org/open-letter/pause-giant-ai-experiments/ (last accessed 22 November 2023).

“Policy of Ethical Development of Systems with Intelligent Functions,” Milrem Robotics, https://milremrobotics.com/policy-of-ethical-development-of-systems-with-intelligent-functions/ (last accessed 22 November 2023).

“ProgeTiger – Estonian way to create interest in technology,” Education Estonia, 31 January 2021, https://www.educationestonia.org/progetiger/ (last accessed 24 November 2023).

“Rannakaitse täisvõimekuse saavutamiseks kuluks paar aastat [It would take a few years for the coast guard to reach its full capacity],” ERR, 2 October 2020, https://www.err.ee/1142379/rannakaitse-taisvoimekuse-saavutamiseks-kuluks-paar-aastat (last accessed 24 November 2023).

“Regional cooperation,” Ministry of Defence of Latvia, undated, https://www.mod.gov.lv/en/nozares-politika/international-and-regional-cooperation/regional-cooperation (last accessed 22 November 2023).

“Scientists launch Estonia’s first autonomous maritime research vessel,” ERR, 30 September 2023, https://news.err.ee/1609117841/scientists-launch-estonia-s-first-autonomous-maritime-research-vessel (last accessed 23 November 2023).

“State to make ready AI strategy by year-end,” ERR, 23 August 2023, https://news.err.ee/1609054811/state-to-make-ready-ai-strategy-by-year-end (last accessed 22 November 2023).

“Tallinn, Tartu science parks to operate NATO innovation accelerator DIANA,” ERR, 27 August 2022, https://news.err.ee/1608697294/tallinn-tartu-science-parks-to-operate-nato-innovation-accelerator-diana (last accessed 23 November 2023).

“Tehisintellekti võimalustest ja mõjudest [On the opportunities and impact of Artifical Intelligence],” Riigikogu (Parliament of Estonia) on YouTube, 3 November 2023, https://www.youtube.com/watch?v=eRrFcFPXnEk (last accessed 30 November 2023).

"Type-X RCV," Milrem Robotics, undated, https://milremrobotics.com/type-x/ (last accessed 23 November 2023).

"What is a kratt?" Kratid, 2023, https://www.kratid.ee/en/mis-on-kratt (last accessed 30 November 2023).

Allik, Sten, Sean Fahey, Tomas Jermalavičius, Roger McDermott, Konrad Muzyka, The Rise of Russia's Military Robots: Theory, Practice and Implications (Tallinn: International Centre for Defence and Security, February 2021), https://icds.ee/wp-content/uploads/2021/02/ICDS-Analysis_The-Rise-of-Russias-Military-Robots_Sten-Allik-et-al_February-2021.pdf (last accessed 22 November 2023).

Atmante, Kristine, Riina Kaljurand, and Tomas Jermalavičius, "Strategic Cultures in the Baltic States: The Impact of Russia's New Wars," in Katalin Miklóssy and Hanna Smith (eds.), Strategic Cultures in Russia's Neighbourhood: Change and Continuity in an In-Between Space (London: Lexington Books, 2019), 53–82.

Champion, Marc and Olesia Safronova, "From Robots to Recycled Vapes, Ukraine's War Effort Gets Inventive," Bloomberg, 10 August 2023, https://www.bloomberg.com/news/features/2023-08-10/how-ukraine-s-innovative-military-gadgetry-is-helping-fend-off-russia-s-invasion#xj4y7vzkg (last accessed 23 November 2023).

Crandall, Matthew and Collin Allan, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," Contemporary Security Policy, 36:2 (2015), pp. 346-368, DOI: 10.1080/13523260.2015.1061765.

Defence Data 2020-2021: Key Findings and Analysis (Brussels: European Defence Agency, 2022), https://eda.europa.eu/docs/default-source/brochures/eda---defence-data-2021---web---final.pdf (last accessed 24 November 2023).

Dieves, Veiko, "Kiirema tulelöögi nimel – TOORU projekt [For the sake of faster fire support – TOORU project]," Academia Militaris, No. 2 (December 2021): 12-16, https://www.kvak.ee/files/2021/12/academia_militaris_detsember_2021_web.pdf (last accessed 23 November 2023).

Eesti julgeolekupoliitika alused [Fundamentals of national security] (Tallinn: Government of Estonia, 2023), https://www.riigiteataja.ee/aktilisa/3280/2202/3001/julgeolekupoliitika_2023.pdf (last accessed 22 November 2023).

Estonia's national artificial intelligence strategy 2019-2021 (Tallinn: Government of Estonia, July 2019), https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_27a618cb80a648c38be427194affa2f3.pdf (last accessed 30 November 2023).

Gosselin-Malo, Elisabeth, "Estonia's global arms buying spree seeks drastic combat gains," Defense News, 13 June 2023, https://www.defensenews.com/global/europe/2023/06/13/estonias-global-arms-buying-spree-seeks-drastic-combat-gains/ (last accessed 24 November 2023).

Idarand, Tõnis, Reining in autonomous weapons: Impact on military innovation – An Estonian perspective (Tallinn: International Centre for Defence and Security, February 2023), https://icds.ee/wp-content/uploads/dlm_uploads/2023/02/ICDS_Analysis_Reining_in_Autonomous_Weapons_Tonis_Idarand_February_2023-1.pdf (last accessed 23 November 2023).

Jäärats, Raiko "Kaitseväe juhataja: kõik algab tahtest oma riigi kaitsta [Chief of defence: everything starts with the will to defend one's country]," Sõdur, 128:6 (2022), pp. 6-13.

Jermalavičius, Tomas and Alice Billon-Galland, British Power in Baltic Weather: The UK's Role in Nordic-Baltic Security and UK-Estonia Defence Cooperation (Tallinn: International Centre for Defence and Security and Chatham House, 2023), https://icds.ee/en/british-power-in-baltic-weather-the-uks-role-in-nordic-baltic-security-and-uk-estonia-defence-cooperation/ (last accessed 22 November 2023).

Jermalavičius, Tomas and Martin Hurt, Defence Innovation: New Models and Procurement Implications – The Estonian Case (Paris: ARES Group, September 2021), https://www.iris-france.org/wp-content/uploads/2021/09/71-Policy-Paper-Def-Innov-Estonian-Case-Sept-2021.pdf (last accessed 23 November 2023).

Juurvee, Ivo and Mariita Mattiisen, The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict (Tallinn: International Centre for Defence and Security, 2020), https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf (last accessed 24 November 2023).

Kaska, Kadri, Liis Rebane, and Toomas Vask, "Lessons from Estonia's national cybersecurity strategy: How to succeed or fail in delivering value", in Henry Rõigas and Tomas Jermalavičius (eds.), So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation (Tallinn: International Centre fro Defence and Security, 2021), https://icds.ee/wp-content/

uploads/2021/05/ICDS_Report_So_Far_Yet_So_Close_chapter_II.pdf (last accessed 23 November 2023).

Landrum, L., Joel P. Gleason, and G. Corrado, "Turning standard ammunition into sharable ammunition," NATO Review, 10 November 2023, https://www.nato.int/docu/review/articles/2023/11/10/turning-standard-ammunition-into-sharable-ammunition/index.html (last accessed 23 November 2023).

National Defence Strategy (Tallinn: Ministry of Defence of Estonia, 2011), https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf (last accessed 30 November 2023).

Salu, Kadi and Erik Männik, "Estonia," in Biehl, Heiko, Bastian Giegerich, and Alexandra Jonas (eds.), Strategic Cultures in Europe: Security and Defense Policies Across the Continent (Potsdam: Springer VS, 2013), 99–112.

Schleicher, Andreas, PISA 2018: Insights and Interpretations (Paris: OECD, 2019), https://www.oecd.org/pisa/PISA%202018%20Insights%20and%20Interpretations%20FINAL%20PDF.pdf (last accessed 22 November 2023).

Suurkask, Heiki, "Mereväe ülem: laevastike ühendamine on olnud edukas [Navy Chief: Merger of the fleets was successful]," Sõdur, 123:2 (2023): 7-17.

Defense AI Observatory Studies

23|20 Tomas Jermalivičius, Caught Between Today and Tomorrow. Defence AI in Estonia

23|19 Nikolaos Karampekios, Konstantinos Sakalis, and Iraklis Oikonomou, Harnessing the Potential. Defense AI in Greece

23|18 Andreas Graae, Servers Before Tanks? Defence AI in Denmark

23|17 Kévin Martin and Lucie Liversain, A Winding Road Before Scaling-Up? Defense AI in France

23|16 Sami O. Järvinen, Cautious Data-Driven Evolution. Defence AI in Finland

23|15 Inbar Dolinko and Liran Antebi, Embracing the Organized Mess. Defense AI in Israel

23|14 Alastair Finlan, A Fertile Soil for AI? Defense AI in Sweden

23|13 John Lee, "Overtaking on the Curve?" Defense AI in China

23|12 Heiko Borchert, Torben Schütz, and Joseph Verbovszky, Master and Servant. Defense AI in Germany

23|11 Katarzyna Zysk, High Hopes Amid Hard Realities. Defense AI in Russia

23|10 Yvonne Hofstetter and Joseph Verbovzsky, How AI Learns the Bundeswehr's "Innere Führung." Value-Based Engineering with IEEE7000™-2021

23|09 Robert C Engen, When the Teeth Eat the Tail: A Review of Canada's Defence Artificial Intelligence

23|08 Çağlar Kurç, Enabling Technology of Future Warfare. Defense AI in Turkey

23|07 Lauren A. Kahn, Risky Incrementalism. Defense AI in the United States

22|06 Yvonne Hofstetter, Wie KI Innere Führung lernt. Wertbasierte Technik mit IEEE7000™-2021

22|05 Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini, Exploring the Benefits of a New Force Enabler: Defense AI in Italy

22|04 Kenneth Payne, Bright Prospects – Big Challenges. Defense AI in the United Kingdom

22|03 Heiko Borchert, Christian Brandlhuber, Armin Brandstetter, and Gary S. Schaal, Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense

22|02 Peter Layton, Evolution not Revolution. Australia's Defence AI Pathway

21|01 Heiko Borchert, Torben Schütz, Joseph Verbovszky, Beware the Hype. What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War

DAIO Defense AI Observatory

www.defenseai.eu