Ponder the Improbable since 1996

MILITARY ARTIFICIAL INTELLIGENCE AND ISRAEL'S NATIONAL SECURITY: A STRATEGIC GAME CHANGER?

Policy Report
May 2022

Leehe Friedman

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

MILITARY ARTIFICIAL INTELLIGENCE AND ISRAEL'S NATIONAL SECURITY: A STRATEGIC GAME CHANGER?

Leehe Friedman

May 2022

TABLE OF CONTENTS

Executive Summary

In Israel, where techno-scientific leadership is a key pillar of national security, Artificial Intelligence (AI) is acknowledged as a strategic technology – "an infrastructure of infrastructures" – with the potential to reshape military affairs, the global economy, and the distribution of power within the international system. To guarantee its national security, operational autonomy, economic growth, and the well-being of its citizens, Israel strives to establish itself as one of the top five countries in the world in the field and in related technological areas of the fourth industrial revolution (4IR). The Israeli security sector plays a central role in this endeavour and in the national AI-ecosystem. Though AI and the 4IR are globally acknowledged as major military innovations of our era, and possibly even the precursors of a new revolution in military affairs (RMA), how they are about to shape future warfare and battlefields is perceived differently by different players. Israel's interpretation of the technology's transformative potential is reflected in the Israel Defense Forces' (IDF) New Operational Concept for Victory, the Momentum Multiyear Plan, and the newly announced Data and AI strategy. Given the IDF's advanced operational experience in the field, the Israeli approach makes an interesting case study for the ongoing strategic learning competition.

Introduction

Artificial intelligence (AI) is recognised worldwide as a general-purpose technology that is expected to affect every field of human activity, incite further innovation, and thus shape the rules of the game in economics and security for years to come. The global acknowledgement of AI as a strategic technology, and a means of exerting power and influence at the international level, has ignited a global race for supremacy - both economically and militarily. In the military context, the concept of a revolution in military affairs (RMA) as a disruptive form of military innovation provides a theoretical framework for the exploration of how AI and related technologies can affect future warfare and to what extent they might revolutionise it.[1]

RMA is a radical military innovation that transforms the way wars are conducted by triggering radical change(s) in the capabilities, organisational structures, and operational conduct of military forces. Since RMA indicates a turning point in the continuum of the character of warfare, strategic and military institutions must identify it in time to adjust themselves accordingly. Those who are slower or less accurate in this process may risk a significant decrease in military effectiveness, which can have weighty operational consequences and even lead to strategic disasters with overwhelming implications for national security.[2]

Nevertheless, history shows that upon the emergence of new military technologies, different players have developed varying operational concepts and strategic perceptions regarding the integration of the technology into the development, organisation, and operational conduct of their military forces. This divergence stems from various factors such as differences in the militaries' available resources, technological capabilities, and strategic cultures. Therefore, to understand the current state of play in the global AI race, conceptual and perceptual clarifications are in order with regard to the national approaches that the participating states develop towards the technology and its applications.

---

[1] See Raska, M. (2021). *The sixth RMA wave: Disruption in military affairs?. Journal of strategic studies,* 44(4), 456-479.

[2] Adamsky, D. (2010). *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Redwood City: Stanford University Press. pp.1-2.

Against this background, Israel's evolving strategic approach to AI capabilities and applications in the security context makes an interesting case study for several reasons. First, Israel presents an ambitious goal to establish itself as one of the top five countries in the field within five years.[3] Second, the Israeli security sector is renowned for its advanced technological capabilities, qualified human capital, and for its effective collaborations with industry and academia, which has established a leading defence-tech ecosystem.[4] Third, facing various security threats at the country's borders and in more distant circles, Israel is in a constant state of operational friction with its adversaries. This friction creates demand for advanced technological solutions (bottom-up), and enables fast and concrete feedback from the field regarding the applications that are being developed and their integration into operational activities. Such operational experiences provide Israel with a substantial advantage in the global learning competition regarding the development and integration of military AI. Thus, Israel can serve as a case study for military technological capacity building in the age of AI, allowing the revisitation of issues in the theory of military innovation, the art of operations, and even ethics and regulation of the future battlefield. Additionally, it enables exploration from the perspective of Western democracy.

[3] Ben-Israel, I., Matania, E. & Friedman, L. (Eds.). (Sep. 2020). *The National Initiative for Secured Intelligent Systems to Empower the National Security and Techno-Scientific Resilience: A National Strategy for Israel. Special Report to the Prime Minister.* p.11.

[4] Dougherty, G. M. (2020). Accelerating Military Innovation: Lessons from China and Israel. *Joint Force Quarterly,* 98. Retrieved from https://www.dasadec.army.mil/News/Article-Display/Article/2342531/accelerating-military-innovation-lessons-from-china-and-israel/

Israel's Perceptions of AI and the Role of the Security Sector

There is no one formal definition for AI in Israel. Yet, most operational definitions refer to AI as the technology which grants computers the ability to perform tasks that would have required thinking capability or skills generally attributed to humans. At the same time, it is worth noting that the term AI is also widely used in Israel as a synonym for the "fourth industrial revolution" (4IR) and entails ancillary technological areas such as big data, IoT, automation, robotics, swarms, and more. As such, AI is acknowledged in Israel as a strategic technology – "an infrastructure of infrastructures" – with the potential to reshape military affairs, the global economy, and the distribution of power within the international system.

This perception, the derived national goals in the field, and Israel's approach for achieving them are shaped mainly by three factors. First, techno-scientific leadership is a central pillar of Israel's national security concept. Thus, identifying in time and preparing at a national level for the emergence of new strategic core technological areas is a top priority in Israel, especially given its restrictions as a small country with limited resources.[5] Second, the race for AI supremacy is at the techno-scientific forefront of the great power competition. It is crucial for Israel to establish itself as a leading player with independent capabilities to guarantee its national security, strategic autonomy of operation, economic growth, and the well-being of its citizens. This rationale led former Prime Minister Benjamin Netanyahu to launch in 2018 the "National Initiative for Secured Intelligent Systems" with the mandate to generate a national strategic plan that will place Israel front and centre in the field.[6] Third, it is believed that Israel has the potential to become a leading player in the field. This notion is derived from some base strengths of the 'startup nation', such as its culture of innovation; leading high-tech ecosystem; qualified human capital; relevant areas of academic excellence; the volume of AI companies; and the large-scale investments they attract.[7]

The Israeli security sector plays a central role in the Israeli AI landscape. It is developing AI capabilities through the Directorate of Defense Research & Development (MAFAT) in the Ministry of Defense and its counterparts within the (Israel Defense Forces) IDF and other security agencies. However, it is also employing technologies from the private sector, where most

[5] Adamsky. *The Culture of Military Innovation*. p.113-115. | Ben-Israel et al. *The National Initiative*. p.8.
[6] Ibid. pp.11-12.
[7] Ibid. p.17.

scientists, engineers, and executives are veterans of the IDF, and many are familiar with the military's needs. Furthermore, one of the core strengths of the Israeli high-tech sector is its ability to translate military advances to civilian commercial uses. Thus, the security sector has a triple role within the Israeli innovation ecosystem: it increases the demand for technological solutions, contributes to the development of new technologies, and trains highly qualified human capital to be integrated into the tech ecosystem.

AI and the Future Battlefield

Like its counterparts around the globe, the strategic community in Israel is occupied with how AI and related technologies of the 4IR can transform the character of warfare, and whether they should be viewed as an AI-driven RMA. Some see AI as an evolutionary phase in which the new technologies will complement and contribute to the fulfilment of the IT-RMA's full revolutionary potential, which was not technically achievable until recently. On the other hand, a more "revolutionary" school argues that AI is about to revolutionise human activity in all fields of life, including security and the way we conduct wars, and hence should be classified as a new RMA. Currently, the revolutionary approach is more vocal within the Israeli strategic echelon. It is echoed in the newly developed IDF's 'Operational Concept for Victory' (*Tfisat HaHaf'ala*), in the 'Momentum (*Tnufa*) Multiyear Plan', which was released in February 2020 and meant to direct force design of the IDF until 2024, and in the IDF's recently approved 'Data and AI Strategy'.[8] These strategic documents are the result of an in-depth critical learning and evaluation process of the IDF's strategy and doctrine, which was initiated and led by Chief of Staff Lt. Gen. Aviv Kochavi in January 2019, and yielded a paradigmatic change in the way the IDF sees itself, its adversaries, and the challenges posed by them.[9]

According to this approach, the current wave of innovation has the potential to solve the most acute challenge facing the IDF (and some other Western militaries): restricted mobility in the face of fire dominance over maneuver. Since the IDF embraced the IT-RMA's reconnaissance-strike complexes several decades ago, its adversaries have gone through a learning process which led them to adopt guided missiles and target intelligence as a means to offset Israel's superiority. This conceptual development is known

[8] Brig. Gen. Dagan. A. (2022, February 8). *"The IDF's New Information and AI Strategy"* [Conference session]. AI Week 2022 Virtual Conference, Tel-Aviv University. Video available at https://aiweek2022.b2b-wizard.com/expo/vod#webinar-3041021205

[9] Ortal, E. (2020). Going on the Attack: The Theoretical Foundation of the IDF Momentum Plan. *The Dado Center Journal.* 28-30: pp.35-49. (Hebrew). p.35.

as the "Other side's RMA" (O-RMA).[10] Today, both sides have precision-fire technology that neutralises the other's tactical mobility. By holding a defensive position against Israel, whose ability to manoeuvre efficiently is limited, Hezbollah and Hamas benefit from many inherent advantages.[11] Brigadier General Eran Ortal, current commander of The Dado Center for Interdisciplinary Military Studies, has mentioned: "Denying the enemy of his fire capabilities will remove the threat he poses on Israel. Negating the threat will give Israel significant strategic freedom of action and thwart enemy rebuilding efforts after the war."[12]

The autonomous and 'smart' revolutions allow the IDF to reimagine warfare. The new 'Operational Concept of Victory' is inspired by the multi-domain principle, which was developed by the US Armed Forces in order to undermine the advantages of the defender and overcome the challenge of anti-access/area-denial (A2/AD). In the Israeli context, this means that the IDF is required to develop a faster and more precise ability to locate the forces of the disappearing enemy, as well as fire-suppression capability that will destroy the enemy's sources of fire upon his detection.[13] The multi-domain principle is not new or innovative in itself. The transformative potential lies in the current "age of integration", which enables the aggregation of many independent multi-domain (land, air, sensing, cyber, spectrum, etc.) tactical forces to function simultaneously under one command framework at the brigade level. This revives the IDF's ability to maneuver while confusing the adversaries and denying them the ability to adapt effectively. This is the guiding principle for developing capabilities in the 'Momentum' plan.[14]

The technological basis for the multi-domain tactical forces lies in digital superiority and "data fusion". That is, automation and advanced information processing capabilities enable the creation of battlefield sensing, processing, and rapid strikes complexes as part of the manoeuvring force. Equipping the attacking forces with data systems capable of processing and reducing the overwhelming abundance of data received in real-time from Internet of Battlefield Things (IoBT) sensors to a manageable level improves their ability to distinguish useful information from "noise" and expose the enemy's location. In certain situations, commanders might even

---

[10] Brun, I., & Valensi, C. (2012). The revolution in military affairs of the 'other side'. In Adamsky, D., & Bjerga, K.I. (Eds.). Contemporary Military Innovation: Between Anticipation and Adaption. Routledge. pp. 119-141.

[11] Ortal, E. (2019). We're Confused Too: A Historical Perspective for Discussion of 'Land Ahead. *Military Review* 99(2):82-98. p.84.

[12] Ortal. *Going on the Attack.* p.48.

[13] Ibid. pp.42-43.

[14] Ibid. p.45.

consider allowing these AI-based systems to make decisions.[15] This way, the manoeuvring forces can overcome key challenges due to the fact that the main intelligence gathering and production efforts are detached from them. The vision of the new 'Operational Concept for Victory' is "a screen-based reconnaissance on squadrons of UAVs belonging to tactical forces, a synergy of intelligence and sensing means for senior commanders, all of which are connected to joint databases and effective information extraction systems. This will allow us to locate the enemy more precisely and more rapidly, then to destroy him by fire from aircraft and by nearby ground forces."[16]

To complement the new doctrine and the Operational Concept that is based on multi-domain force buildup, as part of the Momentum Plan, the IDF underwent several organisational changes, like the formation of the Digital Transformation Administration that will lead and design the processes for the realisation of digital superiority in the IDF. Another new administration was established within the Intelligence Directorate to streamline and prioritise the target acquisition processes by integrating all the relevant elements in one centre. Additionally, following the splitting of the Planning Directorate into two directorates, the Multi-Branch Force Buildup Directorate was established based on the Planning Division, with the addition of the recently formed Warfare Methods and Innovation Division *"Shiloah"*, which is responsible for modernising combat methods and arms to enable effective multi-domain warfare.[17]

With regard to the combating forces, two new frameworks which stand out are the 99 Division "Bazak", as the first multi-dimensional division, and the multi-dimensional unit 888 "Refaim" which combines troops and capabilities from units in the infantry, combat engineering, reconnaissance battalions, artillery, air force, intelligence and more. Its soldiers will be equipped with unmanned aerial vehicles and classified combat technologies to facilitate their versatile missions, and will test new fighting techniques and tactics developed by the Shiloah unit.[18] Finally, to adjust the training environment to the changing battlefield, in recent years, massive multi-arms and multi-dimensional exercises have taken place to practise the new warfare methods and 4IR capabilities according to the new Operational Concept for Victory.[19]

---

[15] Ortal. *We're Confused Too.* p.88.

[16] Ortal. *Going on the Attack.* p.46.

[17] IDF Portal. (2020, May 11). The new Shiloah Division in the Planning Division was inaugurated. HYPERLINK "https://www.idf.il/מירמאמ/2020/תגצה-תביטח-תוטיש-המיחל-תונשדחו-סורופל-הטמה-י/

[18] Ahronheim, A. (2020, January 1). New year, new multi-dimensional combat unit in the IDF. *The Jerusalem Post.* Retrieved from https://www.jpost.com/israel-news/new-year-new-multi-dimensional-combat-unit-in-the-idf-612769

[19] For example: IsraelDefense team (2019, June 20). IDF Concludes Massive Multi-Arm Exercise in Northern Israel. *IsraelDefense* Retrieved from https://www.israeldefense.co.il/en/node/39044

In the past three years, addressing AI and the 4IR as critical enablers of the IDF's desired transformation has turned into a bon ton discourse among military and even political echelons. The technological advances allow the combat forces to be equipped with advanced sensors set up upon new layers of unmanned aerial vehicles and platforms, enabling the integration of data for fast and accurate generation of intelligence and targets, essential in connecting all-to-all in the battlefield. This unprecedented connectivity and data flow enable the formation of diverse, data-based, joint taskforces that will be much more lethal and effective in the face of challenges posed by a disappearing enemy.[20]

Conclusions

The emergence of AI-based capabilities is one of the significant military innovations of our era, which has a dramatic potential to affect national security. In the Israeli case, this applies both in terms of the enormous opportunity it holds and in terms of the threats Israel would face, if it fails to adapt and transform. However, even among keen advocates of the revolutionary approach, there are concerns that the opportunity for the desired transformation within the IDF might be missed out due to some tech-phobia and parochial interests.[21] In order to tap the great potential of the current wave of military innovation, revolutionary or evolutionary, these issues must be addressed, and the developed capabilities must be coupled with the development and implementation of the IDF's new doctrine. Furthermore, maintaining and intensifying the relations between the security sector and the rest of the ecosystem is vital both for Israel's national security and for establishing Israel's leading position in the global race, which in turn affects national security.[22]

At the same time, the full operational potential of the AI age is yet to be discovered. Works such as this contribute to the ongoing strategic learning process by using specific case studies to illustrate potential interpretations of the transformative nature of the technology in the military context. A longer historical perspective is required to decide whether we are at the gate of a new RMA or simply continuing the IT-RMA. In the meantime, the fact remains that massive budgets are being invested in the AI field worldwide, and defence communities are engaged in a strategic learning competition in an attempt

[20] Kochavi, A. (2020). Introduction by the Chief of Staff. *The Dado Center Journal.* 28-30:pp.8-10. (Hebrew).
[21] Ortal. *We're Confused, Too*. p.96.
[22] Dagan, O. and Cohen-Inger, N. (2020). Working Group on Artificial Intelligence and National Security Report. In Ben-Israel et al. *The National Initiative.* pp. 248-255. (Hebrew).

to adapt themselves and their militaries to gain advantages. In this context, potential areas for future research could be: the effect of AI capabilities on the offense-defene balance; the threshold of warfare and military fractions; and on human-machine dialectics – where would militaries draw the line between humans and machines? These subjects also touch upon some fundamental ethical issues, and that is another aspect that demands further exploration with regard to AI in general and military AI in particular. Further research on these matters will derive theoretical and operational value for militaries worldwide, and a special added-value for militaries in democratic like-minded countries, which are likely to identify opportunities for collaborations based on shared values, threats, and perception of the emerging technology.

About the Author

Leehe Friedman is a Visiting Research Fellow with the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS) and an Adjunct Professor at the Lauder School of Government, Diplomacy and Strategy at Reichman University (IDC Herzliya). She was previously the Academic Director of the Honors Track for Strategy and Decision Making at the Lauder School, and the Coordinator of the 'Israeli National Initiative for Secured Intelligent Systems (AI)'. With the Initiative's co-Leaders, Prof. Gen. (ret.) Isaac Ben-Israel and Prof. Eviatar Matania, she is co-author of the special report for the Prime Minister offering a National AI Strategy for Israel. Leehe holds an MA in Security Studies and a BA in Government, Diplomacy and Strategy, both with the highest distinction. Her work focuses on the fields of strategic planning, national security, international relations, and the effect of emerging technologies, mainly nuclear, cyber and AI, on these areas. Her experience includes projects with the Strategic Planning Department and the Research Department of the Israeli Defense Forces, Israel National Cyber Directorate, The Institute for National Security Studies, Deloitte and more.

About the Institute of Defence and Strategic Studies (IDSS)

The **S. Rajaratnam School of International Studies (RSIS)** is a global think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education, and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

IDSS comprises nine research programmes, namely: China, Indonesia, Malaysia, Maritime Security, Military Studies, Military Transformations, Regional Security Architecture, South Asia, and the United States. For greater synergy, with effect from April 2020, China and the United States are grouped as the Major Powers, Indonesia and Malaysia are clustered as Malaysia-Indonesia, and Emerging Security consists of Military Transformations along with the Humanitarian Assistance and Disaster Relief at the Centre for Non-Traditional Security Studies (NTS Centre). The Military Studies Programme focuses on professional military education for the Singapore Armed Forces.

For more details, please visit www.rsis.edu.sg and www.rsis.edu.sg/research/idss. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

RSiS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University, Singapore

Nanyang Technological University, Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg