The understanding that this technology has crucial importance for economic strength, security resilience, and the empowerment of countries has lead to a real "arms race" between the major powers, namely the United States, China, and Russia. Most of the leading countries in the field have already built national programs around AI and have assigned resources and given executive attention in recognizing its importance. This could affect the international arena and future battlefields. Moreover, there is a concern that new phenomena that have emerged with AI, such as a "hyperwar," could debilitate the stability of the international arena.

Despite the many advantages and technological opportunities,
AI poses various challenges to Israel:

This document presents a number of recommendations for Israel
in the fields of:

This study makes the following key recommendations:

01 Israel should formulate a national strategy for AI and should establish a body that will manage it at the national level.

02 Israel should create a multi-year program for AI, such as the one which exists in the cyber field, to analyze the field broadly and in-depth, to lead a national policy of resource allocation, and to make decisions regarding research and development, human resources, and other matters.

03 Israel should create a national solution for infrastructure issues (hardware, cloud, internet connection), and should allocate an ongoing budget, because the security community, unlike the civilian industry, has needs that do not usually allow for using commercial infrastructures, due to issues of classified information, for example, and other security constraints.

04 Israel should immediately consider integrating AI into security technology in which Israel now has a relative advantage (such as the unmanned aerial vehicles field), in order to produce a power multiplier.

05 The defense sector should train non-technological personnel, including those at senior levels, to be familiar with AI, its limitations, and its capabilities, so that its personnel can be more involved and active in making decisions in the field of AI.

06 The various security organizations should consider the management of personnel at the system-wide level, including defining common roles, standards, and training, transfer of personnel between organizations, in addition to providing incentives and budgets to recruit and retain talented people, in order to not lose them to the civilian industry.

07 Israel should define the areas of research that require financing in a governmental-security budget, given that they are significant to national security and would not be considered otherwise.

08 Israel should invest in comprehensive studies by the national security establishment instead of relying solely on academic studies that tend to be only on a theoretical level and are inadequate or not tested in the areas required by the security establishment.

09 Knowledge sharing in Israel's security establishment is crucial; therefore, Israel should establish mechanisms between the various security organizations to avoid duplicating work, to fill the gaps between the organizations, and to coordinate solutions.

10 Israel should consider a combination of mechanisms to encourage investments in the areas of AI that have a positive effect on national security; in parallel, the government should increase its expenditure on AI in civilian areas to advance the economy in this field.

11 Israel should increase investments in research and development in the human–machine teaming field for the security establishment, with the understanding that despite the highly autonomous nature of the systems, some elements of human control will persist. In this context, it is recommended to prioritize the research and development of AI in areas that support people instead of those that replacing them, until the credibility and safety of the technology is well established, and the administrative and legal aspects have been addressed.

12 The Hebrew language processing field should be developed, including applications such as natural language processing (NLP), speech-to-text, text-to-speech, and more.

13 Israel should develop norms and principles for ensuring safety and responsibility in the use of AI within the security establishment, with the intention that civilian bodies will adopt them as well.

14 Israel should create a code of ethics for the use of AI in the security establishment in general and in the context of human–machine teams in particular.

15 For legal, moral, safety, and redundancy purposes, Israel should decide which systems should retain mechanisms of human supervision and control.

16 Israel should monitor at a national level what occurs in the fields of AI and data sciences at the international level, including all that relates to conventions and standards, to maintain Israel's advantage.

17 Israel should act to strengthen joint research and collaboration with other countries.

18 Israel should cooperate with, and even lead, a coalition of nations in the field of AI, as it does in military intelligence, aerial defense, and other fields.

19 Israel should join and even lead international initiatives—whether security or civilian—to limit rogue elements from attaining achievements in the field of AI.

20 Israel should examine standards and processes in the export of AI systems, including security-related export licenses. Israel should make decisions that will maintain the strength of the industry and its ability to act, while also restricting exports that could harm Israel's security.