Executive Summary

Artificial Intelligence and its Importance for Israel's National Security

Artificial intelligence (AI) is a general name for data-based computer systems that are capable of producing knowledge and new insights through abilities, such as understanding, reasoning, and perception, which until now had been perceived as uniquely human abilities.

AI makes these capabilities possible through a variety of applications that are relatively efficient, reasonably priced, and on a broad scale. The automation of these human abilities creates new opportunities, which affect many areas, including national security. The purpose of this memorandum is to present the complex issue of AI to the public in general and to decision makers in particular. Given the challenges and opportunities that AI embodies, this memorandum makes recommendations for Israel's desired policy in this field.

AI is a technological field that is crucially important to Israel as Israel is currently one of the countries leading in its development. AI also has the potential to help Israel cope with the many challenges it faces. It should be noted that Israel almost completely lacks natural resources, and its economic strength relies heavily on the high-tech industry.

AI's importance has increased as AI is seen as being able to contribute to economic growth, to find cures for illnesses and improve health systems, to improve the efficiency and safety of transportation, to encourage energy efficiency, to improve the understanding of climatic phenomena, and perhaps even to lead to a peace-based stability in the international arena through deterrence. Therefore, it is imperative that Israel's decision makers should be familiar with the field, study its opportunities and challenges, and thus be able to formulate a suitable policy and ensure that it is implemented at a

pace that keeps up with regional and international events, while also taking into account the growing competition in the international arena.

The Different Domains of AI and its Security Applications

AI includes a large number of subdomains, including machine learning, deep learning, computer vision, natural language processing (NLP), as well as a number of interconnected technologies, such as the Internet of Things (various objects characterized by connecting to the internet and being able to transmit and receive information and assist in performing certain actions) and dual-use technologies, which serve both in the civilian and in the security arenas. These and other domains are the foundations for diverse applications in different fields, including commerce, medicine, academia, and transportation, as well as the security sector.

In the security sector, AI technologies are used by military intelligence in systems that are capable of reviewing huge amounts of video data and identifying targets; logistic applications that improve and save resources; autonomous driving that also has potential in the security sector, as it does in the civilian sphere; autonomous weapon systems that enable improved precision and reduce risk for the combatants who use them; planning and support systems for decision making and simulations, which improve and decrease planning and decision-making processes before performing missions, based on copious amounts of data that previously could not be analyzed; command and control systems that cope with big data from various sources by cross-referencing and analyzing them while undertaking missions in real time and improving the results by directing and changing decisions in an ongoing loop; cyber warfare, cyber protection, and electromagnetic spectrum—currently leading in the use of AI—to manage large amounts of data and speeds exceeding human ability for the purposes of attack and protection; forecasting, warning, and preventing or managing disasters, which depend on using enormous databases or different sensors for aggregating information and reaching insights that could not attained by other means.

In addition, AI requires other technologies for its development and use. For example, AI depends on big data for training AI applications; the applications can then perform autonomous operations on files of new data to which they have not been previously exposed. Other examples include technologies that serve as infrastructure for activating AI applications, such

as cloud computing, super-computing and quantum computing, or fifth-generation networks, which are required for quick transfer of data and for improving performance of AI-based systems.

AI also supports various technologies. For example, it supports "swarms," which uses advanced coordination to operate various systems or technologies and applications in the field of human–machine interaction, as well as the brain–machine interface, which are designed to shorten the time between when a person receives the information and makes the decision, and transfers it back to the machine.

These capabilities and applications strengthen the relationship between AI technology and national security in general and Israel's national security in particular, according to its national security concept—and beyond—and the IDF Strategy, issued in 2015. Therefore, proper management of the field of AI has great potential for maintaining and improving Israel's national security, and it has even more importance given the growing field's international competition.

The Arms Race and Technological Competition in AI between World Powers

Since 2014, the leaders of many countries—including major technological and economic powers—have realized the importance of AI for strengthening their countries, alongside industrial and technological developments. China, the United States, and some of the EU countries, for example, have already built national programs in AI and have allocated resources and attention to the field. Most strategies emphasize the importance of AI to economic growth and, moreover, for maintaining national security, including military applications.

One developing area in this arms race is autonomous weapon systems (AWS), capable of locating, identifying, and attacking a target without human involvement, with the United States leading this field, as well as the "swarms" field. Similarly, China leads in many civilian industries relating to AI, partly because of its centralized management and due to government control of civilian companies. In addition, China also has databases full of information about its population, which it has collected over a prolonged period. China was able to collect this information because it disregards both human rights and the rights of the citizen to privacy. Conversely, as a

result, China has trouble recruiting experts and companies, which are fearful of the theft of algorithms and are concerned about the ethical implications of the use of the AI technology they will develop. The European Union, the United Kingdom, and Russia comparatively lag behind China and the United States in the field of AI.

In addition, AI can influence the international arena in other ways, and this needs to be considered when formulating policy in the field. These include risks related to the safety of AI: adverse effects on other fields of armament including nuclear weapons; risk of "hyperwar"; influence on the balance of power and the likelihood or risk of a new world order; an increased gap between developing and developed countries, or, alternatively, an improved quality of life and stability in the international arena through deterrence.

Historical test cases of arms races shed light on these subjects, including the relatively new case of autonomous weapon systems (AWS), which shows that the speed at which international law limits innovative technologies is quite slow. The technological development in the field will eventually present decision makers in various countries with moral, legal, and regulatory challenges, and the likelihood of solving them in a timely manner through international tribunals and cooperation between countries is slim.

Challenges in the Field of AI and Recommendations for Handling Them

Given the international competition in developing AI and despite its many benefits and opportunities, this technology poses diverse challenges for Israel, which demand the attention of decision makers in the field:

- **Technical**, including developmental issues; difficulty in adapting civilian technology to military use; standardization challenges in hardware and energy; lack of raw data; the difficulty in explaining the results of an AI system, because it is a "black box."
- **Organizational**, comprising the need for designated budgets; investment and management of human resources; Israel's being a small country with limited resources.
- **Usage**, including difficulties in adapting the pace of the environment or the people who use these systems to their high capabilities; the difficulty of AI systems to adapt to new environments in which they have not been trained; safety and reliability concerns; ethical challenges; biases based

on the information provided; and the use of AI for producing "fake news" that seems credible.

- **Security and political,** which include the international arms race; difficulty in agreeing to and applying weapons control procedures in this field; the dependency on AI that will be created, in addition to their being subject to cyberattacks or other manipulations. "Soft" challenges, which nevertheless significantly influence national security—sometimes indirectly—also belong to this category. These include ethical and legal issues; effects on job and employment markets; the potential for extreme inequality in distributing a country's resources, which could undermine a country's stability.

These factors have contributed to the recommendations given here. The purpose of the recommendations is to maintain and increase Israel's capabilities in the field of AI, to use these capabilities among the various security bodies, and to prepare for handling the challenges posed by this technology, such as the use of AI by Israel's adversaries or, alternatively, in the context of an international arms race. The main recommendations are:

Organizational: It is necessary to formulate a national strategy for AI and to establish a body that will manage it at the national level, recognizing its importance and the urgency of having national management for this field. This is in addition to forming a multi-year program in the field of AI; creating and strengthening structural models in the security establishment, which will enable responsiveness and flexibility; forming common bodies, methods of action, and joint work spaces for professionals from various security organizations who are involved in this field, and other bodies that influence Israel's national security.

Research and development: It is necessary to test the immediate integration of AI in security-related technology, areas in which Israel has a relative advantage (such as unmanned aerial vehicles) to generate a power multiplier based on existing knowledge and investments. Israel should invest in comprehensive research by the defense establishment and avoid exclusively relying on the academic sector in this area. The State of Israel should prioritize research and development of AI in those areas that provide an ongoing advantage. The state should also promote the development of security applications based on existing civilian AI technologies, the

development of the defensive capabilities of AI for protection and attack, and more.

Budgeting and creating a national infrastructure: Israel should create a comprehensive solution for the conspicuous lack of a national infrastructure in the field of AI. The state should allocate an ongoing designated budget for everything related to the field and should define research areas that will be financed by the government.

Human resources: Human resources management should be examined at a system-wide level and not at the internal-organizational level where it is currently being managed. Israel should examine integrating the security establishment into existing training programs and creating new training programs. The state should train non-technological personnel to be familiar with the field, its capabilities, and its limitations.

Ethics, legislation, standards, and safety procedures: Israel should firmly establish the capacity to create AI safety standards and controls; develop norms and principles for safety and responsibility in using AI in the security establishment; define an ethical code in regards to AI and especially for the human–machine teams in the security establishment; define classification and standards of the AI systems for the purposes of jointness, safety, and the capacity to conduct joint discussion between various bodies and organizations, in addition to organized processes vis-à-vis industry; and to define standards related to research in the human–machine field.

Knowledge sharing: The main recommendation is to increase the sharing of knowledge in Israel's security establishment by creating fixed mechanisms to prevent duplication and create coordinated solutions, which are necessary due to limited budgets and personnel in the field. Ongoing knowledge-sharing processes with other agencies should also be established.

The international, diplomatic, and intelligence aspects: It is imperative to follow the international developments in the field of AI in order to adapt Israel's policy and retain its existing advantage in the field; to strengthen joint research and cooperation between Israel and other countries; and to consider whether, how, and which AI applications Israel should limit through international conventions.

In conclusion, Israel should formulate a policy in the field of AI so that it can attain significant achievements in the field and not allow such an important and challenging area to be influenced by market forces only.

Given the rapid pace of development and international competition, the speed of decision making, the amount of resources allocated to executing the decisions, and the control and management of the many tasks in the field are all important. Managing these issues together would have a crucial impact on Israel's future strength, including its economy and its ability to maintain and improve its national security.