ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY IN ISRAEL

Liran Antebi

207

Memorandum

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת TEL AVIV
UNIVERSITY תל אביב

Artificial Intelligence and National Security in Israel

Liran Antebi

INSS Institute for National Security Studies

The Institute for National Security Studies (INSS), incorporating the Jaffee Center for Strategic Studies, was founded in 2006.

The purpose of the Institute for National Security Studies is first, to conduct basic research that meets the highest academic standards on matters related to Israel's national security as well as Middle East regional and international security affairs. Second, the Institute aims to contribute to the public debate and governmental deliberation of issues that are – or should be – at the top of Israel's national security agenda.

INSS seeks to address Israeli decision makers and policymakers, the defense establishment, public opinion makers, the academic community in Israel and abroad, and the general public.

INSS publishes research that it deems worthy of public attention, while it maintains a strict policy of non-partisanship. The opinions expressed in this publication are the author's alone, and do not necessarily reflect the views of the Institute, its trustees, boards, research staff, or the organizations and individuals that support its research.

Artificial Intelligence and National Security in Israel

Liran Antebi

Memorandum No. 207

February 2021

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

בינה מלאכותית
וביטחון לאומי בישראל

לירן ענתבי

Institute for National Security Studies (a public benefit company)
40 Haim Levanon Street
POB 39950
Ramat Aviv
Tel Aviv 6997556 Israel

E-mail: info@inss.org.il
http://www.inss.org.il

Copyeditor: Ela Greenberg
Graphic design: Michal Semo Kovetz and Yael Bieber,
TAU Graphic Design Studio

Printing: Digiprint Zahav Ltd., Tel Aviv

February 2021

ISBN: 978-965-92806-9-8

Contents

Artificial Intelligence and National Security in Israel: Main Points

Artificial intelligence (AI) is a comprehensive name for information and computer systems that display intelligent behavior or create new insights and information. This is a groundbreaking technological field that can be implemented in a variety of applications with relative efficiency, at reasonable cost, and on a broad scale. This technological advancement affects many areas, including national security.

For Israel, AI is a field of crucial importance, given that Israel is now one of the leading countries in its development—with its economic strength relying largely on the high-tech industry—and given that this technology has the potential to help cope with many challenges.

AI includes many perceptual-technological areas, including machine learning, deep learning, computerized vision, natural language processing, and a number of ancillary interconnected technologies. In the security realm, AI is used in the following:

- Autonomous driving
- Logistics
- Intelligence
- Cyber and electromagnetic spectrum warfare and security
- Planning and simulation
- Autonomous weapon systems
- Robotics and autonomous systems (land, air, sea)
- Command and control
- Prediction, warning, and prevention of disasters
- Swarms

These capabilities and applications explain why AI technology is closely connected to national security in general and to Israel's national security in particular.

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:

Security and policy challenges

Challenges of use

Organizational challenges

Technical challenges

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

Human resources

Budgeting, finance, and national infrastructure

Research and development

Organization

International, diplomatic, and intelligence aspects

Information sharing

Morality, legislation, standardization, and safety procedures

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.

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.

Preface:
Artificial Intelligence—Why Now?

Artificial Intelligence (AI) is a broad name for simulating intelligent human behavior or creating knowledge and insights that have never existed before by using information and computer systems. This technology is important and groundbreaking; for the first time in history, software can efficiently perform abilities that traditionally have been considered exclusively human—such as understanding, reasoning, perceiving, or communicating—at low cost and on a wide scale, using various applications and having different uses. The mechanization of these human abilities creates new opportunities and influences many areas, including national security.

The realm of AI arguably is a real revolution, after having developed quite slowly for many decades and sometimes even stopping in its tracks. New hardware capabilities, as well as the availability of databases, cloud computing services, and other capabilities, have made this revolution possible, enabling what was once considered only theoretical or even impossible. This technology has enabled products and services, such as autonomous vehicles, computerized medical diagnoses, voice interaction in natural language between computers and people, planning and optimization systems, and recommendations for services and products based on previous actions.

Experts assess that AI will be able to increase the rate of economic growth; find cures for illnesses and improve health systems; enhance the efficiency and safety of transportation; encourage energy efficiency and improve the understanding of climatic phenomena; and perhaps even lead to peace-based stability in the international arena through deterrence. Experts estimate that AI will change our lives beyond recognition, when it takes control of a variety of familiar actions and enables a wide range of new capabilities and applications. Those who assess the feasibility of general AI believe that its capabilities will exceed those of human beings in all areas. Therefore, companies and countries are racing to achieve capabilities in the field of AI, affecting both economic and international fields.

As AI moves into new domains and areas and as its potential grows, the gap will widen between those leading the race and those trailing behind. Furthermore, the field has caused a struggle for talent, knowledge, and the ability to produce value or break through new boundaries. AI, alongside the Internet of Things and big data, will create a new industrial revolution on the largest scale in history. This new revolution is visible in various services and products that have been fundamentally transformed by the use of AI.

Many countries and organizations have begun to recognize that AI is no longer a future or futuristic technology; rather it is now a fundamental need. Leaders of organizations and countries are encouraging the investment, development, and implementation of the use of AI. In some cases, this development has caused competition, and in others, it has lead to a real arms race.

The security arena has felt the influence of AI applications. AI is extensively used in military applications and it affects the ability to produce or maintain military superiority. This is evident in the use of AI technologies in military intelligence, advanced robotics, cyber warfare, and cyber protection, which are now groundbreaking in their use of AI.

Israel is one of the world's leading countries in AI development. This position is manifested by the number of startup companies in Israel and by international companies establishing development centers in Israel. AI affects not only aspects of Israel's economy but also its national security. Israel, which copes with a wide range of security challenges, has relied on advanced technology for several decades to ensure and maintain its national security. In addition, given that Israel does not have many natural resources (except for a certain amount of gas), its economy is based on the high-tech industry, military exports, and other narrow areas. AI offers the ability to cope with these challenges and with future ones while it enables Israel to maintain its economic, international, and security status, and perhaps even to improve it.

Therefore, Israel should formulate a policy in the field of AI to attain these achievements and should not leave such an important and challenging area to be influenced by market forces alone. The speed of decision making on the subject, including the scope of the resources allocated and how the field is supervised and managed is critical, given the rapid development of technology, its influence, and international competition. Thus, the State of Israel cannot afford to delay, since failure in the field may result in grave consequences and high costs.

Many have participated in formulating the materials, knowledge, and recommendations that appear in this study. However, only I, as the author, am responsible for any claim or error that appears here.

On this occasion, I would like to thank the Institute for National Security Studies (INSS) that facilitated this research and allocated the necessary resources, and especially the director, Brig. Gen. (res.) Udi Dekel, for his vast help and support for this research and its publication, out of recognition for the importance of the subject.

My thanks to the members of the professional expert committee who met for the purpose of this study, contributing their knowledge, time, and energy to this research: Mr. Uri Eliabayev, consultant in the field of AI and the founder of Machine & Deep Learning, Israel; Brig. Gen. (res.) Itai Brun, deputy director of INSS; Elisha Stoin, head of the Horizon Scanning Department in the Ministry of Intelligence; Ms. Gil Baram, research director at the Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University; Lt. Col. Chen Weitz, chief data officer, telecommunications branch of the IDF; Mr. Tal, head of the Data Science Group, the Prime Minister's Office; Lt. Col. Eran Dahan, head of the AI sector, Administration for the Development of Weapons and Technological Infrastructure; Dr. Shmuel Even, senior research fellow, INSS; Brig. Gen. (res.) Dr. Sasson Hadad, senior research fellow, head of the Economics and National Security Program, INSS; and Uri Friedman, intern in the Advanced Technologies and National Security Program, who helped in reviewing and consolidating material for this memorandum.

Special thanks to committee members Col. (res.) Boaz Zalmanovich, formerly head of the basic curriculum branch of the IDF Operations Division; and Dror Ben-David, the head of AI in Matrix, Ltd., who, in addition to all else, commented on versions of the memorandum and contributed greatly to improving the final document.

My thanks also go to Dr. Anat Kurz, a senior research fellow and director of research at INSS and Dr. Gallia Lindenstrauss, a senior research fellow at

INSS, who expended great effort in editing and improving this document, Dr. Ela Greenberg for the linguistic editing in English, and Ms. Noam Ran, the head of publications at INSS.

My great thanks and appreciation are given to Ms. Inbar Dolinko, the research assistant in the Advanced Technologies and National Security Program, who worked day and night in managing the work of the professional expert committee, reviewing materials, writing, and editing, and who greatly influenced the nature and content of this document. Her devoted work has contributed greatly to this study and to the work of the program in general.

Last but not least, I wish to thank my family and to Michael, my husband, who supported me during the writing of this memorandum and helped me to find time even during challenging times; and my firstborn son, Rom, who was born at the end of my work on this study. I wish with all of my heart that he grows up in a world where technology is used as little as possible for wars and as much as possible to improve the world in which we live.

Liran Antebi
October 2020

Introduction

At this point, technological changes have taken place at the fastest pace in history, with some having a crucial impact on countries, societies, and individuals. Among these changes, artificial intelligence (AI) is a growing technological field, which has had a revolutionary impact on almost all aspects of life. AI is a concept that generally refers to hardware or software or integration, which can present a behavior that appears intelligent.

This field of technology—initially a branch of computer science—has increasingly assumed a place of honor in the international arena and now is a focal point for competition between companies and countries. The development of AI has occurred along with breakthroughs in other technological and scientific fields, such as cloud computing, big data, advanced robotics, and autonomous cars, and it seems that these developments will alter our world in the near future.

The use of advanced systems, applications, and services has increased, and many countries, companies, and security officials use them according to their needs. Civilian uses of AI include navigation applications, algorithms that offer custom goods or services, applications in banking and financial commerce, and systems in the fields of maintenance and logistics. AI-based systems are also common in the security arena, such as in military intelligence; logistics; command, control, and communications systems; autonomous military systems including weapon systems; and cyber warfare.

AI is no longer a futuristic technology; rather it provides a fundamental need at the present time. Many leaders of organizations or countries have internalized this notion and have adopted policies to encourage development and investment in AI. However, in addition to the advantages of AI, it also includes many challenges in its development, use, and its accompanying effects. Leaders in diverse fields and in the world in which we live should be concerned about these challenges.

This memorandum has two essential goals:

First, it is intended to serve as a general guide for commanders, managers, and decision makers to familiarize them with core issues and terms related to AI and national security. For this purpose, in several chapters, an attempt was made to render complex issues, including technical ones, understandable.

Second, the purpose of this memorandum is to recommend an AI policy in the field of national security, assuming that AI is a fundamental capability that Israel needs and that Israel must maintain and strengthen its capabilities and status vis-à-vis the global race in AI and the regional and other challenges.

Part I of the memorandum presents AI technology and its security applications by discussing the historical background, the technological areas involving AI, and its security applications, as well as the issue of general AI.

Part II addresses issues related to AI and the international arena. It includes an overview of the state of development and the use of AI in leading countries, the possible effects of technology on the international arena, as well as a case study of the use of lethal autonomous weapon systems (LAWS) and the lessons learned about AI and the international arena.

Part III relates to AI in the context of Israel's national security and includes a status review, a review of the concept of Israel's national security, and the connection between AI and national security and the IDF strategy. This section also addresses in detail the many challenges in developing, implementing, and using AI in Israel, as well as security, political, and indirect challenges to Israel's national security.

The memorandum's conclusion gives policy recommendations for strengthening and maintaining Israel's national security, based on AI.

This study relied upon a variety of primary and secondary sources, including policy documents, academic research, interviews with experts and professionals, and conclusions formulated at meetings of the professional expert committee for this study. The committee held discussions on the various subjects that comprise this memorandum. The contents of the discussions contributed to a more thorough understanding of many aspects of AI in regards to the various security organizations, industries, and civilian companies, as well as a profound understanding of the technology and its capabilities. The committee's discussions helped characterize the conceptualization of this memorandum, compose the list of challenges, and plot the policy recommendations.

The policy recommendations indicate a number of key areas in which Israel must act to maintain and improve its national security through AI: the organizational realm; budgeting, financing and national infrastructure; safety, law and ethics; legislation and standardization; knowledge sharing; international, diplomatic, military intelligence, and cooperative aspects; and human resources, including education and training.

Some of these recommendations will require substantial budgets and significant organizational changes, while others will not and can be implemented in a short period of time. Nonetheless, in a field of great importance that is characterized by rapid development and diverse influence, it is necessary to have an overarching body that will coordinate, budget, and guide the activity at the national level, just as Israel does, for example, in the cyber field. This will enable Israel to maintain and improve its status as a global technological leader, while using its relative advantage to positively influence its own national security.

Part I: Artificial Intelligence and its Security Applications

> **By far, the greatest danger of artificial intelligence is that people conclude too early that they understand it.**
>
> Eliezer Yudkowsky, American AI researcher and writer

Chapter One: What is Artificial Intelligence?

The idea of AI first developed in 1945 when Vannevar Bush, one of the early founders, proposed a system to increase human knowledge and understanding. He was followed by Alan Turing, who in 1950 wrote an article on the capabilities of machines to simulate human beings and their ability to perform intelligent actions such as playing chess.[1] The term artificial intelligence (AI) evolved a few years later and is attributed to John McCarthy, a computer scientist and researcher in the field of cognitive sciences, who organized the first academic conference on the subject in 1956, and to Marvin Lee Minsky, who was trained as a mathematician and was involved in research, inventions, and many developments in the field. It was Minsky who coined the popular definition of AI, noting that "AI is the science of making machines do things that would require intelligence if done by men."[2]

At the beginning of the study of AI, the dominant paradigm was the "symbolic" one, which sought to duplicate high-level human thought. Over the years it was replaced by the "connectionist" paradigm, which endeavored to imitate the biological basis of human cognition through artificial neurons. These paradigms, however, failed to meet expectations beyond theoretical or laboratory demonstrations and led to the "winter of AI," when research and investments in AI were minimal for long periods of time.[3]

In the past decade, due to progress in computer science research, the development of hardware and software in computing and communication, as well as cloud computing and big data, AI has significantly progressed, including in subdomains such as machine learning and artificial neural networks (these concepts will be reviewed in detail later). Some studies have claimed that the progress in the areas of neural networks is so profound that it is almost considered synonymous with that of AI.[4]

Most common applications in AI belong to a subdomain called machine learning, which includes statistical algorithms that seek to imitate human cognitive tasks by analyzing large amounts of data and creating rules about them. The algorithm actually "trains" on existing information and creates a kind of statistical model of its own, in order to perform the same task in the future on new data that it has not previously encountered.[5]

AI belongs to the wider field of data science, and indeed, it needs a great deal of data to operate effectively, specifically big data, which is needed to generate significant insights with the help of learning algorithms. However, AI does not depend solely on big data, which is only one of the efficient means of generating value and knowledge from such an amount of data, which requires especially strong algorithms to analyze them.[6]

A considerable part of the work of the founders of AI was the theoretical basis for machine-learning algorithms, which are used in many contemporary systems and enable actions such as image identification and autonomous driving.[7] These systems belong to what is known as narrow AI or weak AI, although sometimes these can be advanced applications. This concept refers to algorithms that are designed to deal with a cluster of specific problems, such as games, image identification, or navigation.[8] This concept differs from general AI, which relates to a system capable of using human-level intelligence for a wide range of tasks.[9] As of this writing, general AI still does not exist, and opinions are divided on whether it will be created, at least within the next two decades. The AI that has been developed belongs mainly to deep learning applications. This technology indeed can be categorized as narrow AI, but it enables a more accurate form of computerized learning as well as a broader commercial use of AI applications.[10]

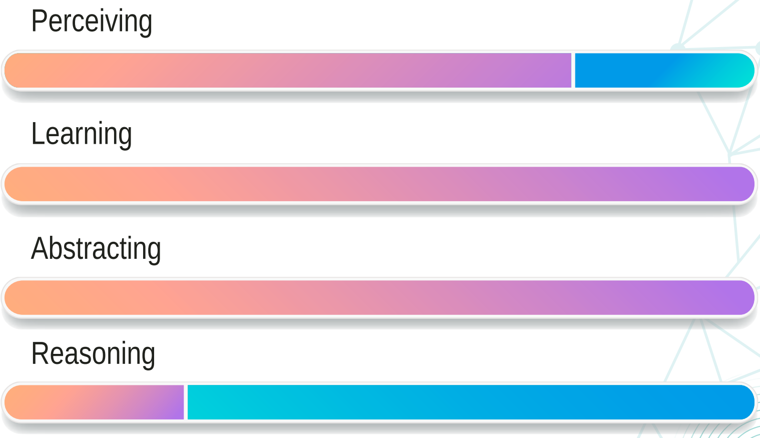
Historical Background: The First Three Waves of AI

The development of AI can be divided into three distinct waves, based on the development of AI's capabilities. The Defense Advanced Research Projects Agency (DARPA) of the US Department of Defense is one of the world's leading bodies in the development of AI for security purposes. DARPA defines AI as a "programmed ability to process information."[11] Alongside this simple definition, DARPA has divided AI into three waves, characterized by the Notional Intelligence Scale in which the following four capabilities are measured, similar to the dimensions of human intelligence:

1. Perceiving: the ability to discern global events
2. Learning: the ability to learn things and adapt to various situations
3. Abstracting: the ability to take knowledge discovered at a certain level and to deduce from it or apply it to another level
4. Reasoning: the ability to explain logically, or to make logical decisions.

The first wave of AI was based on “handcrafted knowledge,” in which experts collected existing knowledge on a particular subject and characterized it within the framework of rules that could apply to a computer, which in turn could learn their implications.[12] This generation of AI includes logistics software for planning operations such as shipments; software for calculating taxes; and software that could play chess games against people. Many computer programs and applications on smartphones or in software such as Microsoft Office are based on this wave of AI. According to DARPA, the products of the first wave have moderate sensory ability and can explain causality in very narrow aspects, but they lack learning abilities, and cannot cope with uncertainty. Nonetheless, DARPA claims that this wave had many achievements, such as in cyber defense, and it continues to be developed and is still relevant today.[13]

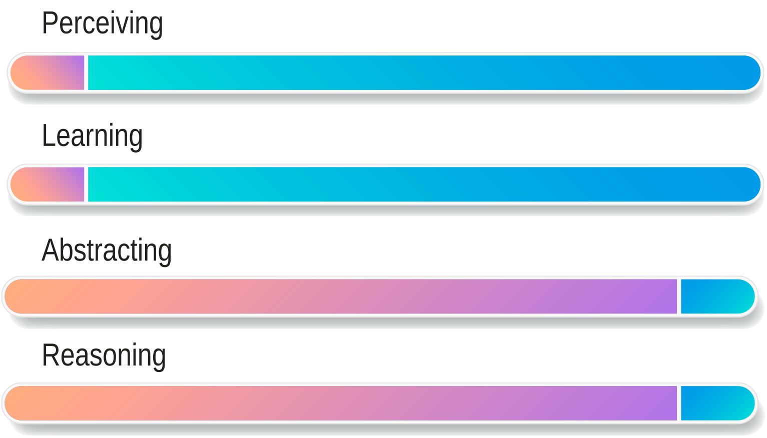
Figure 1. First wave: Handcrafted knowledge



Enables reasoning over narrowly defined problems.
No learning capability and poor handling of uncertainty.

Source: Launchbury, “A DARPA Perspective on Artificial Intelligence.”

Figure 2. Second wave of AI: Statistical learning



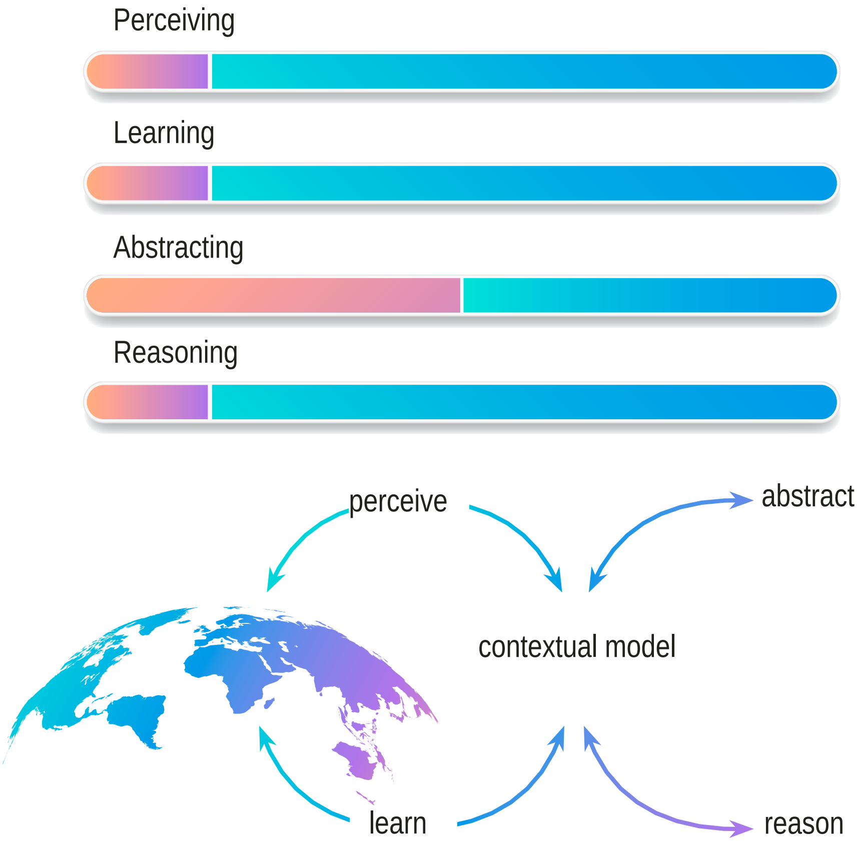
Nuanced classification and prediction capabilities.
No contextual capability and minimal reasoning ability.

Source: Launchbury, "A DARPA Perspective on Artificial Intelligence."

The second wave is referred to as "statistical learning," characterized by categorization. In this wave, experts made use of more advanced capabilities facilitated by machine learning, in which algorithms for statistical learning rely on big data. In this wave, unlike the previous one, the experts taught the computers statistical models for various problems, instead of fixed rules and then trained the algorithms on many examples, until they reached the desired level of accuracy. The products of this wave enabled voice recognition or facial recognition on mobile phones and "bots" that provide customer service through internet chat correspondence.

This generation of AI includes systems for analysis or translation of text; personal assistant software in smart phones; and the ability to play challenging games such as the Chinese strategy game "Go." This wave of AI also includes autonomous driving. This generation of AI, however, does not have the ability to understand the rules or the causality behind the actions it performs, so it is subject to error or manipulation. According to DARPA, the second wave of AI could categorize things according to nuances and predictive ability but lacked contextual abilities and had minimal abilities for logical reasoning.

Figure 3. Third wave: Contextual adaptation



Source: Launchbury, "A DARPA Perspective on Artificial Intelligence."

The third wave, referred to as "contextual adaptation," is an explanatory one, which is currently being developed. The algorithms or systems from this wave will formulate models that explain certain topics. DARPA expects that systems built around contextual models will learn by themselves how different models should be structured. These abilities are significantly different from most of the algorithms that currently operate as a "black box" and create a challenge of explainability as to how they reached conclusions (a topic that will be expanded upon in a later section). Thus, this wave of AI will use information in an abstract manner and take it one step forward, but currently the capabilities of these systems are still limited.[14] It is hoped that the products of this wave will be more "human" and will be able to communicate in natural language, will be able to teach and train themselves (like the Alpha-Go software that has trained itself in thousands of "Go" games against itself), and will be able to collect data from several different sources, and formulate well-explained conclusions.[15] According to DARPA, this wave should greatly improve the AI capabilities in sensory, learning, and reasoning fields, although the products will still only have medium-sized capabilities in the field of abstraction.

Technologies in the context of this wave include "smart assistants," whose capability to assist has advanced beyond the technologies of the second generation, such as Siri and Alexa.[16] Another example is Google Duplex, which can make appointments (such as making a reservation in a barbershop or restaurant) while managing a coherent vocal conversation with a human service representative. Besides the tasks that this software can do autonomously, it also knows how to identify and signal the user regarding tasks that it cannot perform on its own.[17]

While the three waves of AI are easily identified, most research dealing with AI in recent years, particularly in the field of national security, has addressed the fact that there is no one definition for the term AI. Formulating one accepted definition of AI is problematic for two main reasons: First, there are varied and diverse approaches to research in the area.[18] Second, there is a basic difficulty in defining or agreeing upon a definition of "intelligence," because of limitations that have not yet been breached in the study of neuroscience (and also in philosophy); therefore the ability to examine these concepts in relation to machines or to apply them to machines is limited. Despite this difficulty, this study will examine different definitions and suggest a definition for the remaining discussion in this document and the policy recommendations that follow.

AI—An Operational Definition

One of the known definitions of AI, which has already been mentioned, was formulated by Marvin Lee Minsky as "the science of making machines do things that would require intelligence if done by men."[19] The advantage of this definition is that it is broad enough to include different ideas, methods, and means. However, it lacks the use of the term "intelligent" in the human context—a term that has not yet been defined and is characterized unambiguously by the scientific disciplines engaged in the subject. Moreover, when defining the discipline for national security and for making policy recommendations, a more dichotomous definition is necessary, which will help determine what it should include and what is irrelevant.

Darrell West and John Allen have claimed that "artificial intelligence (AI) is a wide-ranging tool that enables people to rethink how we integrate information, analyze data, and use the resulting insights to improve decision making." West and Allen believe that even though there is no uniform accepted definition, it is correct to refer to AI as "machines that respond to stimulation consistent with traditional responses from humans, given the human capacity for contemplation, judgment and intention."[20] According to West and Allen, "AI depends on data that can be analyzed in real time and brought to bear on concrete problems. Having data that are 'accessible for exploration' in the research community is a prerequisite for successful AI development."[21]

According to Shubhendu Shukla and Vijay Jaiswal, AI applications "make decisions which normally require human level of expertise" and help people anticipate problems or deal with issues as they arise.[22] Thus, AI applications act purposefully, intelligently, and adaptively.

After discussing some of the theoretical definitions, it is appropriate to examine how organizations involved in research and development or the regulation and legislation of AI practically define it. Despite DARPA's general definition of AI as a "programmed ability to process information," it needs to be clarified that not every computing system uses AI. AI algorithms are designed to make decisions and do so by using data entered in real time. When they are used on different systems, these are not passive machines capable of mechanical or preset reactions only, as in the era of automation (such as automatic doors or even automatic functions in the washing machine); rather these are machines with sensors, digital data, and even remote inputs, which can integrate the information from various sources, analyze it immediately, and act according to the insights based on the data. This enables a sophistication and speed in accepting the data that was not previously possible.[23]

As far as the US government is concerned, there is no official definition of AI, and various agencies may define it differently, according to their needs. However, a series of laws that regulates the US Department of Defense budget (FY2019 National Defense Authorization Act) provides a definition of AI for the enactment of section 238, which engages in the research and development of the field:

- Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
- An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
- An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
- A set of techniques, including machine learning that is designed to approximate a cognitive task.
- An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.[24]

This definition is quite detailed and is indeed suitable for legislative purposes. It also helps, in comparison to other definitions, to decide which areas of programming and computing do not belong to the discipline of AI. Nevertheless, it is too long and technical. Given the purpose of this document—to make knowledge about AI accessible to decision makers and to recommend policy in the national security sector—this study needs a shorter and simpler definition such as DARPA's. DARPA's definition is more appropriate for the purposes of this research than Minsky's, for example, because it does not relate to the controversial issue of human intelligence, and, in fact, it allows for a variety of currently accepted applications or processing methods and even leaves an opening for future developments, without the burden of technical details that requires expertise to understand. Even if this definition is likely to include "inferior" capabilities of computing and processing, as explained above, some of the methods and perceptions of the first wave are still useful in various fields and applications and therefore valuable.

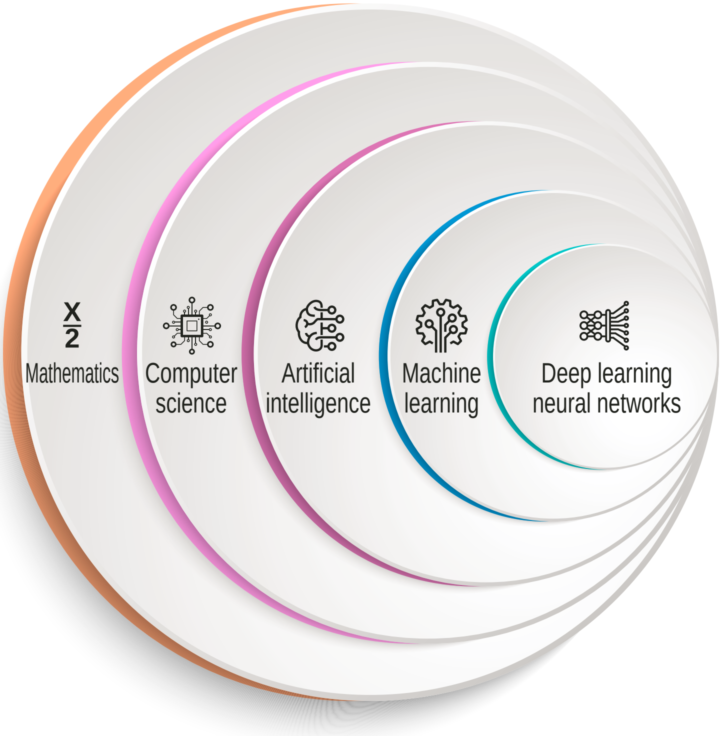
However, in cases where decision makers must narrow the definition in order to examine whether a development meets the definition of AI or not, AI can be referred to as being able to create knowledge and insights that had not existed before, using information and relying upon machines and computers. Focused on the programmed ability to process information, this definition distinguishes between a significant part of AI applications and general computer applications and narrows the general definition in such a way that it still covers a large number of applications and a wide range of disciplines, while emphasizing the creation of new knowledge.

Therefore, the guiding definition of AI used here is **using information and computer systems to present behavior that appears intelligent, or to create knowledge and insights that never existed before**. This definition is broad enough to include various technologies and applications and different kinds of needs to realize these abilities. At the same time, this definition is narrow enough that it does not include all areas of computing, but only those in which properties of AI are expressed. This definition helped to formulate the following chapters.

Chapter Two:
Fields of Artificial Intelligence

AI includes many perceptual-technological areas, including machine learning, deep learning, computerized vision, natural language processing, and a number of ancillary interconnected fields. This chapter focuses on the different subdomains of AI.

Figure 4: AI and its subdomains



Machine Learning

The most common subdomain of AI is machine learning.[25] Machine learning allows algorithms to learn from information and develop solutions independently,[26] by using statistics-based algorithms that “learn” from large databases to recreate human cognitive abilities and thus perform tasks in unfamiliar situations.[27] Machine learning allows algorithms to learn through repetitive training and to create results that improve according to the scope of training and the experience of the algorithm. This is different than software written by a human programmer. One example is an AI program that receives a database of the handwritten alphabet and learns to distinguish between the handwritten letters, even if a person’s handwriting does not appear in the existing repository.

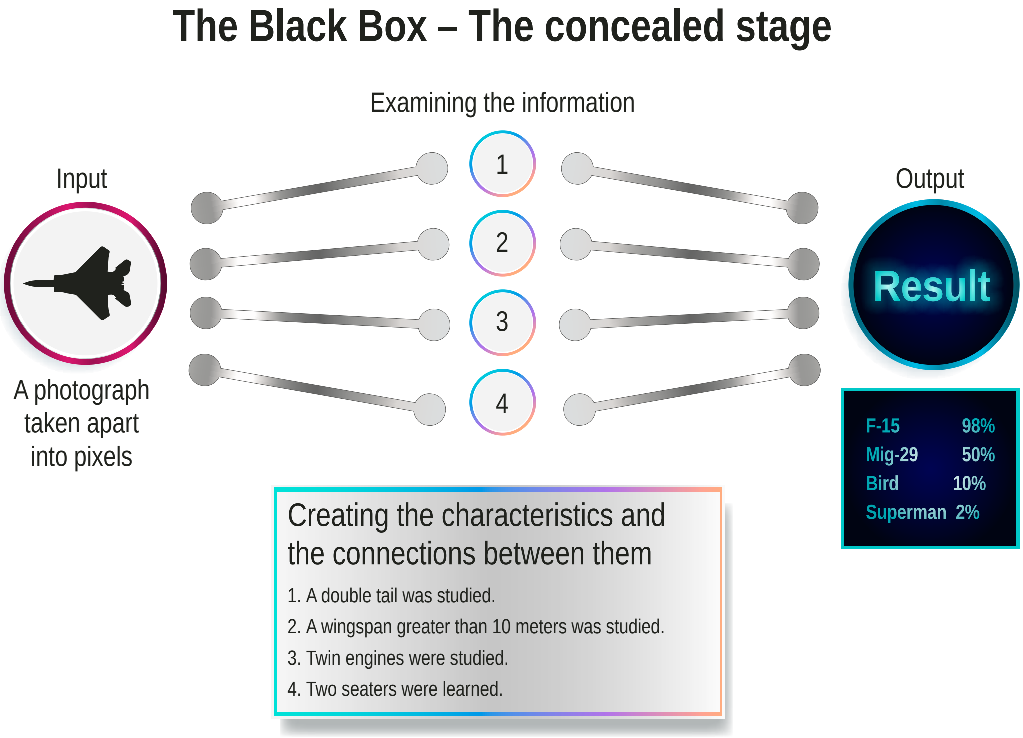
There are several approaches to machine learning, among them supervised learning, in which the programmer bases the learning on an existing initial model, which the machine improves; and unsupervised learning, in which the learning systems develop their own model, which does not depend on an existing model.[28] Another approach is reinforcement learning, in which the software learns from trial and error, rather than from an existing repository of information.

Deep Learning

Deep learning is a subset of machine learning, which uses artificial neural networks. These are algorithms that are inspired by the behavior of the neural network in the human brain.[29] The neural network learns by making small corrections by examining a large amount of data to improve its accuracy.[30] Thus, the output of one neuron is the input of another neuron. Deep learning acquired its name because it is based on many layers of artificial neurons.[31]

Due to their notable successes, neural networks have become the most common approaches to machine learning and are responsible for a variety of achievements in the field of AI, including facial recognition on a level higher than that of the human ability to identify faces; identification of objects in pictures; control of autonomous vehicles and drones; speech transcription at a level that exceeds that of a professional human transcriber; and language translation, including those languages in which the technology was not trained.[32]

Figure 5. Activity of a simple neural network in an application of identifying a photograph


The Black Box – The concealed stage
Examining the information
Input
A photograph taken apart into pixels
1
2
3
4
Output
Result

F-15	98%
Mig-29	50%
Bird	10%
Superman	2%

Creating the characteristics and the connections between them

1. A double tail was studied.
2. A wingspan greater than 10 meters was studied.
3. Twin engines were studied.
4. Two seaters were learned.

These central approaches have capabilities in the following various fields:

Image processing. Image-processing capability uses deep learning and enables software to recognize objects within a picture and to categorize them.[33] The software divides the image into pixels and attaches values to each pixel according to its color. This image analysis passes through the deep system of artificial neuron networks of the software, which is trained upon a large database of images and categorizes the image accordingly. Today, some technologies in this field are already accessible to the public as an off-the-shelf product, such as Google AI Vision software.[34]

Computer vision. Computer vision differs from image-processing technologies in that it enables the software to identify objects in real time and respond to them similar to the ability of human vision but without the need to categorize them. These technologies are used in autonomous cars, for example, because they can identify a person who suddenly runs into the road and warn the driver.[35] Computer vision has also enabled 3-D visualization, bone mass measuring, autonomous navigation, and control of irregular transactions.

Natural language processing. Natural language processing (NLP) is a subdomain of machine learning that enables the software to transcribe, translate, and perform actions according to the broad meanings of a spoken and written language and to produce new words and sentences that are meaningful to a person.[36] Among the natural language processing applications are natural language generation (NLG), which helps process large amounts of information and produce simple, easy-to-understand narratives and insights, and natural language understanding (NLU), which aids in processing texts whose information is missing or unstructured.[37] A wide range of AI applications now use NLP technology, including personal assistant applications such as Siri, Echo, and Google Assistant, language translation applications, government and business applications that analyze large text-based databases, and even security applications in the field of military intelligence.[38]

A related technology, influenced by AI and its development, is the Internet of Things. The Internet of Things (IoT) describes a world in which computers and tiny sensors are embedded into various objects. These objects can produce and store digital information, while they monitor their environment, present information, and perform operations at a certain autonomous—or at least automatic—level. These objects also connect to the internet, allowing them to communicate with the environment, other devices, and people.[39] Because AI technology also relies on the existence of mass data that enables it to make conclusions, the IoT technology has a key part in promoting AI.[40] In addition, integrating this technology into real-time AI applications allows AI system to receive input on real-time reality and to regularly improve its response. This technology, for example, enables the services of smart cities, as was demonstrated in the Chinese city of Hangzhou.[41] Similarly, this technology has many security applications, including the Internet of Battlefield Things (IoBT).

One of the characteristics of AI technology is that it has dual-use capability; that is, the same application can be used for civilian, military, or security purposes.[42] This is not unique to AI and exists in other technologies and scientific fields. The dual-use capability of AI is evident, for example, in software that can autonomously identify inappropriate objects in YouTube videos and alert the user. This software can also identify weapons or suspicious characters in security videos and produce alerts about them.[43]

This dual-use capability creates opportunities as well as challenges. It enables the security industries to collaborate with the business sector and develop technologies with a variety of applications that are useful for both sectors. By means of minimal adjustments, technology developed for the business sector can be used for combat purposes and can provide advanced capabilities for hostile state or sub-state forces.[44] This security challenge is in addition to that of the various off-the-shelf products or technological components, which with simple adjustments can easily become weapons for those who cannot purchase them from the security industries.

The various kinds of AI applications, which have different capabilities and are already embedded in many spheres, are summarized in table 1 below, based on findings of articles and studies from the years 2018–2019.

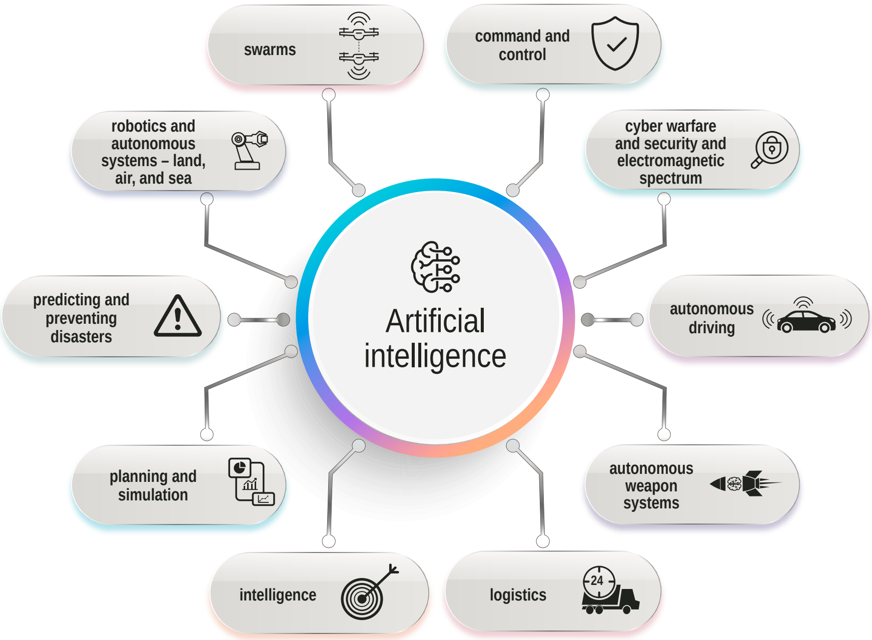
Table 1. Artificial intelligence: Areas of use

	Database analysis	Video processing	Natural Language processing	Autonomous capabilities	Computer vision and image processing	Personalization of services
National Security	✓	✓	✓	✓	✓	
Cyber	✓			✓		
Banks and finance	✓					✓
Transportation	✓	✓	✓	✓	✓	✓
Education	✓	✓	✓			✓
Communication	✓		✓			✓
Labor and manufacturing	✓	✓	✓	✓	✓	
Healthcare	✓	✓	✓	✓	✓	✓

Chapter Three: Widespread Security Applications

AI applications in the security field have become widespread and are quickly accessible. Security establishments in various countries, security companies, and even some civilian companies have contributed to the development of these applications. In the IDF, for example, it is customary to divide the many applications into two main groups: Those that replace "hard workers," such as automatic decoding, automatic translations, and other tasks, most of which are considered endless tasks; Those that help make decisions and, in some cases, autonomous decisions about tasks, such as planning and forecasting.

Figure 6. Artificial intelligence applications in the security domain


Artificial intelligence
swarms
command and control
robotics and autonomous systems – land, air, and sea
cyber warfare and security and electromagnetic spectrum
predicting and preventing disasters
autonomous driving
planning and simulation
autonomous weapon systems
intelligence
logistics
24

Listing all the applications and fields in which AI is used for security issues is difficult because of the large quantity of applications and the rapid rate of change. In addition, some civilian applications could potentially become security applications, and some also influence security (e.g., deep fake applications).

Military Intelligence

A variety of AI capabilities are suitable for military intelligence needs, ranging from image processing to computer vision, processing of language by various methods, and other capabilities. Various military intelligence projects around the world now use algorithms. In an era flooded with data, human power cannot handle all the data collected by the many sensors of the security systems. Thus, using AI in military intelligence is no less imperative, as it helps in automating the military intelligence processes, especially in areas of unstructured information and enables the production of new insights and knowledge that were not possible by previous means.

Among the many military intelligence projects that use AI is the "Project Maven," known for the opposition it has aroused among its employees. Google and the US Department of Defense carried out this computer vision project together, using AI to analyze videos gathered by UAVs.[45] DARPA has a program that develops algorithms to assist in recognizing targets in difficult environments that can be co-located with radar and by comparing the data generated from them.[46] Algorithms are also used in text or audio analysis, which assist in facial recognition applications, among others. In 2018, the Prime Minister's Award for General Security Service was awarded for a machine learning-based project, which helped prevent hundreds of terrorist attacks by analyzing data from a wide variety of sources.[47]

Logistics

The field of logistics has undergone significant changes in both civilian and military uses, as a result of the prediction and planning capabilities made possible by AI. In fact, the US military has been using logistics systems since the 1990s, which helped the army plan and optimize the transfer of forces during the first Gulf War, recouping the investment in thirty-year-old AI research.[48] More recently, the US Air Force has used AI systems to predict aircraft maintenance and create individual aircraft maintenance scheduling.

The US Army's logistics support activity (LOGSA) in the Watson system of IBM has developed a maintenance schedule for the Stryker armored fighting vehicle fleet, based on information collected from its sensors.[49] In fact, in many respects, military logistics is similar to civilian logistics, since both commercial companies and civilian organizations also make extensive use of logistics services and systems maintenance. The design and execution of dual-use logistics tasks rely on a variety of systems, such as robots and certain software, which, for example, help manage Amazon's warehouses.[50]

Autonomous Vehicles

While unmanned cars are relevant to the civilian sector, the security sector has used autonomous vehicles for several decades, with different degrees of autonomous capabilities. These are extremely important on the battlefield, as they can be both a force multiplier and can replace the human factor in danger zones. However, despite their autonomous capabilities, most rely heavily on human involvement and activation. In addition, in terms of the development and applications of autonomous vehicles, the security field trails behind the civilian one where the investments are great. The transition between the two fields is challenging as there is a considerable difference between driving on paved roads according to traffic signals and driving an autonomous vehicle in an open or urban area, where the enemy tries to outwit you.

Autonomous Weapon Systems

In recent decades, many countries have identified the potential of using UAVs for security purposes. Within these systems are a subset of autonomous weapon systems (AWS) that are capable of searching, identifying, and attacking targets independently, without human input.[51] These systems have the potential to fundamentally change the battlefield, because they can be activated with almost no human involvement in executing the tactical mission and are capable of causing lethal damage. For this reason, these systems faced widespread opposition, which even led to hearings in international courts with the intent of limiting them. Today, however, their development has accelerated, and there are fears that the world will face an arms race in this area as well.[52] If AWS are not limited, it is possible that they will become increasingly common and significant on the battlefield in the coming years.[53] At the same time, as the capabilities of AI increase, the use of AWS could expand to a wide range of tasks and uses; along with their other components, AI constitutes the brain of those systems and defines their ability to operate autonomously.

Although this is still an evolving field, several countries have already gained operational experience in using various kinds of autonomous systems. These include air defense systems, such as the American Patriot or the Israeli Iron Dome, which today must have a human operator due to a principled decision made by the countries that operate them.[54] Loitering munitions, such as the Harop, are UAVs that can fly, hover, locate, track, and attack targets without human intervention by means of homing in on radar signals.[55] In addition, several ground systems with a low level of sophistication are capable of firing at a pre-defined area, depending on certain parameters, including movement or heat. These include, for example, the Korean SGR-A1 system.[56]

Planning and Support Systems for Decision Making and Simulations

AI systems that can help plan and support decision making already exist in the civilian field. In medicine, for example, AI systems can make diagnoses based on existing data and information—such as radiological images—and vitals, including heart rate and body temperature. These systems have high capability, sometimes even beyond that of the physicians, and they can assist physicians in making a diagnosis and determining treatment methods according to the specialized field in which they operate.[57]

Similarly, in the security field, AI-based systems will be able to specialize and assist humans in making information-based decisions according to massive amounts of information in a short time. Nonetheless, algorithms are able to assist even in cases when information is scarce, and they can make use of simulations or other means to generate insights or perform operations in a computerized manner. In the future, decision-making systems will perform the actions carried out by planning systems in real time, which will complicate the data processing but increase the pace of the process.

AI systems also can build realistic scenarios, simulations, and war games, which will improve training and streamline operational planning based on big data.[58] China, for example, uses this field to strengthen its military, whose experience is relatively limited compared to that of other countries.[59] Given that an AI system can play and win a strategy game like “Go”[60] and an advanced system even taught itself to play the game in a few hours so that it could win the previous system, then such systems—when given the appropriate data—can run a variety of strategic options about a given situation and choose the best one, while taking into account possible actions of the opponent.

Command and Control

Command and control systems eventually will make greater use of AI, including as advisory systems that will be subjected to human control during the operation itself (unlike design systems, decision support and simulations used in pre-operation stages). An example is the US Air Force Command and Control System (MDC2), which is in the development stages. The purpose of this system is to coordinate the planning and execution of air, space, cyber, sea, and land operations. In the short term, AI will integrate data from all these arenas, and after performing learning processes from past events and converting unstructured information to structured information, the system will create a unified operational image for decision makers.[61] This development is significant in the age of information flooding and of dealing with copious amounts and types of data from a variety of sensors and sources. This will also enable systems to plan an operation or assist in navigational planning or defining paths. In the context of communications, AI systems are also being developed to detect when an adversary severs communication connections and to look for alternative means of transmitting information.[62]

Cyber Defense, Warfare, and Electronmagnetic Spectrum

According to DARPA, this is a relevant field for continuing the use of "first generation" algorithms,[63] in parallel with developing the capabilities of the advanced generation of algorithms. Algorithms helps to prevent, detect, and warn against cyberattacks on different computerized systems. The ability to quickly analyze enormous amounts of information from diverse sources helps greatly in this area, while it is also important to be able to handle big data at a speed beyond human ability. These applications are based on the algorithm's ability to detect anomalies—deviations from patterns considered normal—by generalizing scenarios and learning from experience. In this context, the project that DARPA is conducting in the cyber field should be mentioned.[64]

AI is also used for cyberattacks. One example is the IBM-developed malware called DeepLocker, which disguises its purpose until it reaches its destination, recognized by voice or face recognition. This type of malware is considered particularly effective, as it can infect millions of systems without being detected, unlike other cyberattacks that can sometimes be large-scale and “noisy.”[65]

Furthermore, AI already aids in electronic warfare. In the US army, for example, AI systems reduce the cognitive burden needed to quickly and accurately identify signal received by various sensors, by order of priority and by distinguishing between relevant signals and “noise.”[66]

Disaster Prediction, Warnings, and Prevention

AI can help identify, alert, manage and sometimes even prevent disaster situations. AI applications can also assist in predicting earthquakes, floods, volcanic eruptions, and hurricanes. An algorithm developed by Israeli scientist Kira Radinsky can predict and warn of the possibility of violent civil riots, outbreaks of viruses, and even rising prices.[67] Google is developing an AI platform that will help predict floods in India and warn people with its services—such as Google maps or even the Google search engine—who are in the danger zone.[68] At the same time, the Joint AI Center (JAIC) began searching for solutions that would help aggregate information to provide situational awareness, almost in real time, to help those responsible for disaster response to make decisions.[69] These types of systems will be able to operate together with sensors from the field of IoT, which are prevalent in many places or are privately owned, in addition to using various robots or swarms to perform more extensive and improved detection, search, and rescue missions. It is estimated that these and similar applications could save the lives of millions of people.

Chapter Four: Supported and Supporting Technologies

Multiple technologies are influenced by AI or sometimes other technologies are required to enable or support AI applications. Below is a partial list of prominent supported and supporting technologies:

Robotics

The field of robotics has existed since the 1960s. Over the years, and thanks to technological developments, developers have perfected the capabilities of robots, so that fourth generation robots, belonging to the 21st century, are able to analyze new situations, examine their environment, and act accordingly. Some are even able to relate to human emotions. AI is an important component in the development of robotics, since it is the "brain" that controls the physical body of the robot, and with the progress of AI, the functioning and activities of the robots have also improved. Robots now are able to perform a wide range of missions, including autonomous driving, transporting goods, manufacturing products, cleaning, and many other tasks in different fields.

Robots help perform tasks that are characterized by "the 4 Ds": dull, dirty, dangerous, and dear (expensive).[70] In the past two decades, many robots have been used for security purposes in the air, at sea, and on land. As these robotic systems become increasingly autonomous, their potential grows, as does the complexity of legal and ethical issues.

Swarms

Swarms intelligence is a field of AI that imitates animals operating in groups, such as bees and ants. Members of a swarm share a common intelligence that transcends that of the individual member of the group. Developments in the field of processing, networking, and interface design have enabled software and hardware to imitate the swarm's decision-making process. These AI systems receive information from all connected parts, each providing unique information, enabling it to make the best decision for the entire group.[71] DARPA, for example, has been developing swarms for a long time and recently has focused on the cooperation between a swarm and a person.[72] One of DARPA's experiments is the action of a swarm that has the ability to recover, meaning it can successfully execute a task, even if some swarm members are injured or disabled. In such a case, a computer restarts its activity and performs the task based on the new data, and this is the advantage that swarms have over actions based on individual tools.[73]

Human–Machine Interaction

This field includes various subfields of AI that enable easy and effective interaction between machines and people, including natural language analysis, bot chat, analysis of human emotions, and personal assistants, such as Siri and Alexa.[74] The interaction between people and machines occurs by connecting teams of people and robots, by connecting people and AI programs as a means of increasing human abilities; and as an action as one entity that has been cognitively and physically enhanced by machine capabilities. In the security context, militaries seek ways to streamline the human–machine interaction and to create integrated teams that will change planning and fighting and reinforce the defensive strength.[75] In this field, like in others, the ability of a single person to control a large number of tools in the most intuitive and simple manner, or to cooperate with them to enable short response times, is extremely important. In this way, various interfaces are also developed, including the brain–machine interface.

Brain–Machine Interaction

Brain–machine interface is a comprehensive name for devices that communicate with computers through brain activity alone; they translate neurological information into commands in order to control software or hardware. Advanced developments of the interface should enable people to communicate through brainwaves and "read each other's thoughts."[76] Most of the existing interfaces were developed for medical applications, including cochlear implants (hearing devices) and robotic limbs. In 2018, the entrepreneur Elon Musk announced an investment of 27 million dollars in Neuralink—a company that seeks to develop a brain–machine interface that will improve human communications by connecting electrodes to the brain and connecting the brain to computing capabilities.[77] Musk sees the brain–machine interface as a means of improving human abilities and coping with the increasing threat to humanity, which AI presents. This development also has potential for the field of security. DARPA, for example, is working to improve the cognitive abilities of soldiers through the appropriate brain–machine interfaces.[78] This technology greatly relies on AI systems to identify patterns, learn from the environment, and adjust the response to all of these.[79]

Big Data

Development in the field of technology and different types of digital components, including components of IoT, has led to the creation of enormous quantities of "digital signatures," which are expressed as location data (GPS), images, text, and other forms. According to data from 2018, every day, 2.5 quintillion (equivalent to 2.5 billion billions) bytes of information are created, and this rate continues to grow.[80]

Although the concept of big data refers to enormous amounts of data, some relate to big data as a particularly large and complex database, whose management and manipulation involves logistic challenges, since it cannot be done using traditional data processing methods and applications.[81] Others consider big data as a group of statistical techniques capable of identifying patterns in huge arrays of data.[82] Big data is used to train AI, because significant and valuable patterns can be learned from its analysis, and in many cases its size has become a bottleneck in developing certain applications.

Super-Computing

The term supercomputer is not one-dimensional but rather refers to computers that have powerful calculation capabilities and are considered the leading computers when they are built. While the first supercomputer had processing capability of several kiloFLOPS (Floating point operations per second) powerful computers today reach 34 petaFLOPS (10^{15} X 34 FLOPS). Most of the current super-computers use parallel processing—a large number of cores connected together on a fast network. Most super-computers are designed to solve a single problem by way of a specific calculation. Super-computers are also useful for theoretical calculations needed to develop nuclear weapons; as a result, the international arena restricts their production and distribution.[83] It is claimed that the next generation of AI will face the supercomputer problem: The digital world multiplies its volume every two years, and to cope with massive amounts of data while performing various tasks and creating a variety of training methods, tremendous computing power is necessary. Super-computing, which is characterized by an extendable architecture and prevents waste, may meet this need for AI and could enable additional leaps in the field.[84]

Quantum Computerization

Some AI systems require processing and computing capabilities that can support automation processes and cope with huge arrays of data.[85] For this purpose, extremely powerful hardware—sometimes beyond that of the existing computer systems—is needed, rendering certain ideas in the field of AI as merely theoretical calculations. Problems that exceed a particular threshold of complexity and size require more powerful computing power to resolve them, and quantum computing was created to cope with these challenges, which cannot be processed by means of classic computing systems.

Quantum computers use the unique phenomena of quantum mechanics, including quantum superposition and entanglement, and create high-level computing abilities.[86] While "classic" computers perform calculations using binary bits, quantum computers use qubits, which exist in multiple states (superposition); that is, it can be both 0 and 1 at the same time, enabling quantum computers an exponential advantage in their computing capabilities.[87] Quantum technologies can create new paradigms in the way information is collected, stored, and processed, and they can offer improved tools for security, computation, and measurement.[88] The quantum computing revolution has not only improved computing, but it also has the potential to "disrupt" all conventional encryption, thereby causing the collapse of the systems currently in use.[89]

Cloud Computing

Cloud computing allows on-demand access from anywhere to a shared pool of computing resources, including networks, servers, storage, applications, and services.[90] These services allow remote computer connected to the network to access resources. Users of cloud computing do not need to acquire and manage their own resources and systems; instead they rent cloud services, which they can adapt to their needs at a relatively low cost.[91] The types of services include infrastructure as a service (users receive computing resources, such as storage and processing to use), platform (users receive computer resources and tools supported by the provider), and software (instead of purchasing and installing software, the user obtains the provider's software services through a communications network via the provider's website).[92]

Cloud computing can store large amounts of data, which AI systems can access for training or decision making. In addition, the improvement in the capabilities of AI could produce new data to be entered into the cloud, which could help other AI systems learn. In fact, the cloud allows calculation power and capabilities to cope with large arrays of data for AI.[93] The internet infrastructure, however, limits its accessibility, and therefore cloud services cannot be used in every case, because the rate of transfer of information may be partial compared to the needs of the system.

5G—Fifth-Generation Networks

The increasing use of mobile devices and connecting them to the network demand fast data streaming and reliable services that can handle significant traffic on the network. 5G mobile networks should meet this need, considerably expand the bandwidth, and generate a new record high of 20 gigabytes per second for downloading speed, compared to the single gigabyte per second with the 4G networks.[94] 5G networks are expected to allow vendors to extend services provided to consumers (for example, streaming of video or virtual reality applications), to support the growing number of devices connected to networks (e.g., multiple objects in the domain of IoT), to support new industrial uses (such as industrial sensors), to perform advanced data analysis, and to enable the use of advanced technologies such as autonomous vehicles.[95] 5G networks can enable and improve the performance of AI systems by providing the infrastructure for transferring huge amounts of data while AI can reciprocate by understanding the complexity of 5G networks and the information they produce.[96]

Chapter Five: General Artificial Intelligence

While the current era is defined as the era of "narrow AI," capable only of certain actions for which they are defined, researchers and experts also address the possibility of developing "general AI," which will act as a machine that thinks and acts similarly to the human brain.[97] This general definition indicates the complexity of the field, as it combines engineering with the biological, psychological, and cognitive functions of human beings.

Operational definitions relate, for example, to software that can pass the "Turing test" by successfully conducting a continuous conversation with human testers, who have no idea that they are talking to a machine.[98]Another more complex test is the "employment test," testing the machine's ability to perform a wide range of different critical roles in the labor market.[99] Some studies also refer to the computational power or processing required for such AI. However, it is apparent that the whole is greater than the sum of its parts, and that the processing capability is not a sufficient measure to explain such complex technology.

Despite the complexity of its definition, there is a broad consensus that general AI relies upon significant developments in cognitive research, hardware, and software, in addition to global willingness to transfer decision making to machines.[100] In addition, the development of general AI has generated great interest, with the business and public sectors addressing its many aspects.[101]

The feasibility of general AI, however, is still debatable. Researchers cannot agree on the very ability to develop the technology, and they disagree about the time needed to do so, and even if it is possible. Moreover, whether its effects on humanity will be positive or negative is also subject to debate.[102]

General AI faces three central challenges. One is the lack of a definition of AI technology and its problem of measurement.[103] Second, gaps exist in the field of neuroscience and cognition, making it difficult to program a machine to quickly learn something new or make generalizations in a noisy environment, as long as there is no understanding of how a person does it.[104] Third, the hardware challenge also limits the advances in deep learning.[105] In order to advance, it needs more powerful and efficient processing capabilities than those that exist today.

The uncertainty about the future of a general AI notwithstanding, general AI may also have negative implications. Researchers widely agree that the inherent promise of general AI already has created a dangerous race to achieve it, with the United States and China in the lead.[106] The prevailing view is that the first country to develop this type of intelligence will have a significant advantage over its competitors, which raises the likelihood that safety aspects have been neglected during its accelerated development.[107] Moreover, there is concern that a small group of people could abuse general AI, as well as the problem of controlling the product itself, which some fear will be without any limitations,[108] similar to many science fiction films.

It is widely assessed that general AI will influence all areas—including both industry and the labor market—and cause a shift in the global economy, affecting the education system, revolutionizing health care, transportation, and more, while fundamentally changing the behavior of human society.[109] Inevitably, general AI will greatly affect the national security of countries and international relations,[110] because of its implications for both the global balance of power and the nature of war.

Part II: Artificial Intelligence and the International Arena

The rise of powerful AI will be either the best, or the worst thing, ever to happen to humanity. We do not yet know which.

Stephen Hawking, astrophysicist, theoretician, cosmologist, and author

Chapter Six:
The Global Status of Artificial Intelligence

The perception of AI as an innovative and influential means is well expressed by Russian president Vladimir Putin who said, "AI is the future, not only for Russia, but for all of humanity . . . it has tremendous opportunities, but also threats that are difficult to predict. Whoever becomes a leader in this field will be the ruler of the world."[111] Indeed, it is evident that countries have internalized this warning and are creating a cohesive strategy in the field. This chapter will review the field of AI in several leading countries, as a basis for discussing possible international implications and for assessing Israel's relative position in this context.

The United States

The United States is one of the leaders in the civilian and security development of AI. In October 2016, the Obama administration published a report on the future of AI.[112] Since 2017, the United States has been working to formulate a comprehensive strategy for AI with the Trump administration. In December 2017, President Trump signed a national security strategy that set American leadership in new technologies, including AI, as a national goal. The stated objectives were to improve the understanding of the government agencies of the prominent trends in the field; increase collaboration with industry and academia; use existing expertise in civilian research and development and existing resources in the private sector for national security applications; and achieve again the surprise factor by developing new technological areas.[113]

The national defense strategy also highlights the commitment of the US Department of Defense to investing in military applications in the areas of autonomy, AI, and machine learning, along with the use of groundbreaking commercial technologies, to maintain the US competitive military advantage.[114]

It should be noted that the United States is also the world leader in autonomous weapon systems and swarm warfare technologies.

In June 2018, the Joint AI Center (JAIC) was established in the US Department of Defense to coordinate efforts of AI development, implementation, and use. The JAIC also serves as a focal point for advancing AI in the United States. In addition, in February 2019, the Department of Defense released an AI strategy that focused on harnessing technologies in the field to promote national security and prosperity. This strategy seeks to achieve some of the goals determined in 2017, which include improving collaboration with the private sector, academia, and global allies in addition to new goals such as striving for US leadership in terms of the safety and ethics of military use of AI.[115] This emphasis on safety and ethics resulted from the thunderous criticism of leaders, various organizations—including human rights organizations—and employees of technology companies regarding US development policy in general and certain companies and entities—including Google—in particular within the framework of cooperation with the Department of Defense.

On February 11, 2019, the Trump administration announced the American AI Initiative, which aims to implement a broad strategy to promote and protect national AI technology, through collaboration between government, the private sector, academia, the public, and international partnerships.[116]

The Department of Defense's spending in 2016 on developing AI was $600 million, which increased by more than $800 million the following year.[117] According to the Department of Defense, it intends to invest $2 billion to promote AI projects from 2018 to 2023.[118] This is a budget that is relatively large for what may be perceived as a "single technological field." The budget for 2020 reveals a great deal of investment in the field, which reflects the administration's relating to AI as highly important.[119] It has been argued, however, that budgeting is still insufficient for the development, and use of such technology, and the budgetary obstacle may lead to technological inferiority with respect to other nations, notably China, that are seeking to achieve leadership in the field.[120]

Moreover, the administration and the military are having difficulty recruiting the private sector to the national effort. This is especially problematic given that the United States could emerge as the leader in this field due to the actions of commercial companies, from which the Department of Defense purchases products and adapts them appropriately to military needs. This differs from previous periods when the Department of Defense carried out advanced developments, which then moved to the civilian sphere.[121] The problem lies in the different standards of the private sector and the military. Many companies choose to avoid doing business with the Department of Defense because of the complexity of the military procurement process. Commercial companies are also concerned about the intellectual property of software and rights to data.[122] In addition, the Department of Defense has difficulty recruiting and training personnel, as it cannot provide the optimal working conditions and high salaries of the private sector.[123]

The ethical issue of developing AI technologies for the defense sector also poses difficulty in recruiting the private sector. Some companies refuse to cooperate with the Department of Defense, due to concerns that the military and government will use AI for espionage or in weapons.[124] A prominent example is the protest of the Google employees, which led the company to end its contract with the Department of Defense over the prestigious Project Maven.[125] As part of this project, the Department of Defense employed AI developed by Google to interpret videos taken by drones. Google employees were concerned that this would lead to the use of AWS (which are able to commit lethal action without human input). Some even resigned from the project.[126]

The difficulty of collaboration between civilian companies and the Department of Defense has been said to relate to the "distance" between the Silicon Valley and Washington, DC. Most of the leading AI companies are situated in San Francisco, which is geographically far from Washington, DC. This statement relates not only to geographical distance but also to gaps in perceptions and culture between both the government and military corridors and the management and employees of the technology companies. This creates a weakness in the American ecosystem compared to other countries, including Israel and China, where cooperation between government officials and the private business sector is relatively widespread.[127]

China

China is the most prominent competitor besides the United States in the struggle to lead the global field of AI. China has several organized programs comprising its overall strategy in the field. According to the Next Generation

AI Development Plan, China regards AI as a “strategic technology,” which has become the focus of international competition and is crucial to the military and economic futures of any country.[128] As part of this international competition, China aims to lead the field by 2030.[129] Based on an analysis of meeting past goals in areas of defense technology, China likely will allocate significant resources and possibly even take aggressive actions to meet this goal.

The total budgetary investment in the research and development of AI in China, which is not made public, is estimated to be billions of dollars at the minimum. Some estimate that China’s future investments will reach 150 billion dollars, but it is unclear how much will come from the government and how much from industry.[130]

The Chinese ecosystem differs from that of the United States and gives China a significant advantage. Few boundaries exist between the private sector, academia and research, the military, and the government. Consequently, the Chinese government has access to research, development, and implementation of AI outside the public sector, and it can prioritize and guide these processes as it needs. Its ability to harness all the different sectors to achieve national goals enables it to rapidly reduce and overcome its technical disadvantage, and to develop technological independence so that it will not have to rely on Western developments.[131] In addition, the fact that China is not committed to the rights of the individual like Western democracies has enabled China over the years to collect data and information about its citizens.[132] This gives it a considerable advantage, given the importance of data needed for “training” AI systems.

However, this advantage is also China’s weakness. China has difficulty recruiting experts and companies from around the world, because of their concerns about cooperation, particularly in terms of the theft of algorithms and information,[133] as well as of the ethical implications of using AI technology. In addition, China’s hardware and software are technologically poor compared to those of the United States, and it lacks talented human resources for research and development.[134]

As part of its attempt to cope with these challenges, China also operates in the economic realm, investing large sums in American AI companies (a move that generated a counter-reaction from the Trump administration, which blocked Chinese acquisition of a chip production company vital to this technology). [135] China is also working to acquire companies in developing countries, to increase technological control in the field and to constitute an alternative to US technology and services for various clients. [136]

Russia

Although historically, Russia had been considered a superpower in the field of military technology, leading in certain areas (aerial defense systems, for example), since the "revolution in military affairs" (RMA) of the 1990s and the breakdown of the Soviet bloc, Russia has struggled to restore its past glory. Its military industries now lag behind China and the United States, such as in the field of drones, leading Russia to seek collaborations or opportunities for acquiring knowledge, for which it is willing to pay high prices.[137]

Russia's leadership under Putin, nonetheless, has recognized the importance of AI for its economic and defense power. During 2019, Russia decided to formulate a national strategy for AI,[138] with initiatives and programs designed to promote AI development preceding the decision.[139] By 2030, Russia has planned to replace about 30 percent of its military forces with autonomous robots and remote-controlled systems.[140] However, according to the Russians, humans will still make the decisions about the use of lethal weapons.[141]

As part of its efforts to close the gap with other powers and to enable advanced development and extensive use of AI, the Russian government established the Foundation for Advanced Studies.[142] Its central activities include standardization for developing AI in four main areas—image identification, speech recognition, control of autonomous military systems, and support information for the operating loop (the activation loop) of weapon systems.[143] Furthermore, the Russian army began researching a variety of applications of AI, with an emphasis on autonomous and semi-autonomous weapons, and plans to implement AI in land, naval, and aerial vehicles and to develop swarms. Russian military experts have also expressed interest in integrating AI in cruise missiles, unmanned systems, electronic warfare, and cybersecurity and to create a "target library" that will help the systems identify targets and improve their navigational ability.[144] Russia also used AI applications for propaganda and espionage, as well as in its information operations against the United States and its allies.[145]

Despite its aspirations, Russia's weakness in the field of AI is mainly rooted in the quality of its industry and academia, which is poor compared to the world's leading countries; Russia ranked only twentieth in the world in the number of startup companies in the field, while AI research in the Russian academic sector is quite small compared to other countries, and especially to that of the leading powers.[146] In addition, Russia has made budget cuts beginning in 2017, which have continued since.[147] As of 2019, the state investment in AI is believed to be only about $12.5 million.[148]

Unlike China, Russia does not have a strong or high-quality ecosystem, despite having a centralized regime. In 2010, Prime Minister Dmitri Medvedev established a Russian version of Silicon Valley—the Skolkovo Technopark—designed to encourage entrepreneurship and develop new technologies. By 2015, the complex had attracted approximately 30,000 workers. Large US companies like Microsoft, IBM, and Intel also invested in the Technopark. Corruption and over-involvement of the state, however, caused many investors to abandon it and move to other countries in Europe. The approach of the Russian government that free information endangers the state's political and national security—along with the extensive corruption and lack of protection of private property—does not create a fruitful environment for technological entrepreneurship and hinders the development of AI technology.[149] According to estimates presented to the US Congress, these obstacles make it difficult for Russia to reach its objectives and to position itself as a leader in the field.[150]

There are assessments, however, that Russia could successfully lead in narrow areas of AI, especially those related to national security.[151] If Russia is able to resolve organizational issues related to its ecosystem, it could make considerable progress in implementing AI, despite its lack of adequate financing and investment.[152] For example, a company connected to the army has a project in the field of AI, which includes about 30 private companies, the Russian Academy of Sciences, and various universities, and is likely the largest public-private project in Russia.[153] However, these optimistic assessments are dubious, because Russian researchers have difficulty collaborating with colleagues from the West because of security concerns and censorship by the Russian security forces. In addition, companies have little incentive to invest in Russia, out of concern that the state could take control of developments in the field of AI, while Russia would face losing its talent, as it did in the case of the Skolkovo Technopark.[154]

Europe: France, Germany, and Britain

The European Commission promotes a European-wide concept of developing AI, which is seen as improving the lives of Europe's citizens in security and economic terms. Cooperation between the EU states should firmly put them at the forefront of the technological revolution, ensuring both competitiveness in the field and conditions for development and use of AI according to "European values."[155]

In April 2018, 25 European countries met and signed a declaration of cooperation on AI, alongside the national initiatives of several EU member states.[156] In addition, the European Union presented a strategic AI plan, which focused less on the development or security aspects and more on the civilian or "soft" aspects of the field, including the promoting of technological and industrial capabilities; coping with the socioeconomic changes that AI could cause; and creating a framework for appropriate ethical and legal use of the technology.[157]

The European Union faces several challenges in promoting this policy, including a budgetary one that relates to the high investments required of the countries involved and from their private sectors.[158] As of 2019, three EU states—France, Germany, and Britain—have formed more than 50 percent of the AI market in Europe, with Britain leading by a considerable gap. At the beginning of 2020, it is unclear how Britain's leaving the European Union will affect this issue. Even before Britain's exit, however, only three European states led in the field of AI.[159]

France formulated its policy in the field of AI in the Villani Report of 2018, which called for a focus on four sectors: health, transportation, environment, and security and defense. The report also gave rise to a national strategy for AI, which sought to position France as one of the five leading countries in the field and the leader of AI in Europe. France's strategy emphasizes the importance of the ethical and moral aspects of AI.[160] Between 2014 and 2019, France invested more than 1.85 billion dollars to promote research in AI.[161] According to President Macron, up to the end of his term in office in 2022, the government will invest 1.5 billion euros in promoting research and development, encouraging initiatives, and collecting data.[162]

France's strong points are in AI development related to the health system and autonomous vehicles. France is aware that it needs greater capacity and is working to attract foreign researchers.[163] In regards to security, the Villani

Report acknowledges that using AI to preserve France's status—both in relation to its allies and adversaries—is unavoidable; however, according to statements by senior government officials and the French industry, France intends to involve humans in the use of autonomous weapons.[164]

Germany adopted a national strategy for AI in November 2018 and allocated about three billion euros for research and development in the field. The German strategy has three main goals: (1) positioning Germany and Europe as a leader in the development and use of technology, while ensuring the future competitiveness of Germany compared to its competitors; (2) ensuring the responsible use and development of AI to serve the interests of society; and (3) implementing AI in the context of extensive social dialogue and political activities.[165] Germany has worked to promote cooperation with other countries in the field, including France and even China, which invests heavily in German companies and has improved the technological relations between the two countries. Germany's advantage is in the automotive industry and the field of industrial robotics.[166]

Britain, which left the European Union at the beginning of 2020, manages several government initiatives that are researching and planning for the use of AI. Although Britain recognizes that it will not be able to compete with powers such as the United States or China in terms of financing or providing skilled human resources, it seeks to employ the ethical use of AI as the focus of Britain's competitive advantage over the other countries.[167] The British national policy focuses on the fields of entrepreneurship and economics. In the AI Sector Deal of April 2018, the British government pledged to support AI and invest a billion euros in the industry.

According to the AI Sector Deal, the government must cooperate with the academic and research community, industry, and end users to ensure access to the necessary skills in the field. Usually cooperation between these parties begins with the study of basic, non-controversial security applications, which can serve as a basis for extensive military use in the future (e.g., the hackathon, which is organized by British Science and Technology Laboratory and the US Air Force Research Laboratory, for developing autonomous aerial systems for fire relief). But it seems that Britain, as elsewhere in the world, suffers from a skills gap, and thus it must invest in education to develop and attract a talented workforce.[168]

The British Defense Ministry report of December 2018 includes a commitment to expand the use of AI to cope with both military threats and changing warfare. One of the military programs in the field is the Autonomy Program, which explores the new technologies that could have the greatest military impact and operates in the field of developing algorithms, AI, machine learning, and the next generation of autonomous military systems. One of the most covert developments in the field is the "BAE Systems Taranis" drone, also known as the "Raptor," which is operated and manually controlled remotely by a pilot but has an autonomous flight mode.[169]

Table 2. Comparative summary of AI in other countries

	United States	China	Russia	European Countries
Is there a national plan and what type?	There is a national plan, and other policy papers address it as well. The plan is comprehensive in approach, addressing both civilian and security aspects.	China has some policy documents that together constitute a comprehensive strategic plan, addressing both security and civilian aspects.	Although there is no national program at the time of this writing, the Russian government began to formulate one during 2019.	Some countries have a national plan for the field, while others have only a few initiatives. The statement of cooperation of 25 EU countries reflects the EU policy, which emphasizes the civilian and economic aspects of AI.
Budget	The budget is estimated in the billions of dollars, but according to some assessments, it is insufficient and can lead to a technological deficit.	According to some of the assessments, China has budgeted about 150 billion dollars. Even if the budget is lower, China's financial investment is still the greatest.	Russia has cut its budget since 2017; the budget for the field is estimated to be 12.5 million dollars.	The budget depends on the investments of the EU countries and its private sectors, which could challenge the development and research of AI, since the countries have different levels of investment in AI.
Ecosystem	The challenges are in mobilizing the civilian market to cooperate with the army and the government, given the ethical, economic, and technical difficulties.	Given the nature of the regime in China, there are almost no boundaries between the private market, academia, the army, and the government; thus the state's ability to harness the entire ecosystem for this purpose is practically limitless.	The quality of industry and academia in the field is poor, when compared to other countries. Intense political involvement, widespread corruption, and the negative attitude toward free information make creating a productive and effective ecosystem difficult.	There is a gap between the national level and the European level. Although the importance of creating a quality ecosystem at both levels is recognized, it is not clear whether it has been successful.

Chapter Seven: Potential Effects on the International Arena

The possible effects of AI technologies on the international arena are enormous. Besides the general race to achieve AI and the arms race in this field, this chapter considers several other potential effects that AI could have on the international arena, as well as the impact of the arms race.[170]

Safety and Risks

Today there are no international standards for the safety of AI, except at the state level. As a result, AI systems that have various defects could enter the market, such as a system whose underlying database contains built-in biases against certain populations, or whose database is wrong in the first place so that it could produce erroneous results, or whose code was not trained on a sufficiently large database, and therefore may be erroneous.

The uncontrolled development of AI also poses a risk to safety, as it could become dangerous should systems that develop code on their own spin out of control and undermine proper functioning of vital civilian and military infrastructures.[171] One of the main risks results from the race to lead the field of AI, manifested by the investment of countries and the activity of private companies.[172] This phenomenon is apt to influence the international arena—all or in part. Yet, despite these challenges, the international forums have focused only on a few threats, such as the UN attempt to restrict or ban AWS in the framework of the Convention on Certain Conventional Weapons (CCW).[173]

Other Areas of Armament and the Risk of a "Hyperwar"

A major concern is the possible negative impact that AI could have on other areas of armament, such as nuclear armament,[174] as well as the risk of a "hyperwar." This term relates to war that is carried out with AI, which enables automated decision making, rendering human decision making barely possible during a confrontation in the conventional observe, orient, decide, and act (OODA) loop.[175] As a result, the amount of time associated with the decision-making loop cycle will be reduced to almost immediate reactions. These developments have many changing implications.[176] If the risks of nuclear or other arms races are also included, then the potential for damage to the international arena could be enormous.

The Balance of Power and the Creation of a New World Order

One of the most influential factors affecting a country's strength is the scope and ability of its population to contribute to the economic, defense, and security sectors.[177] A country with a relatively large and productive population that can be mobilized by the army is stronger than countries that have a smaller population or an aging population and negative growth. However, in the current era, AI and other advanced technologies could strengthen the countries with smaller or aging populations. AI could contribute to creating a new world order, in which countries with small populations could become powerful and relatively influential, by virtue of their increased ability to wage war.[178] It is even beyond what we know today; as technologies become increasingly autonomous, the human involvement will decrease and cause familiar historical phenomena to become increasingly extreme.

A New Bipolar Era: China–United States

The new world order also directly relates to the growing competition between China and the United States.[179] These two countries, whose competition is mainly economic, are also competing in the field of AI, with the understanding that leadership in this field could affect almost any field. Although since the end of the Cold War, the world has enjoyed relative international stability due to the unipolar American hegemony, the competition in AI may become another tier in the struggle between the United States and China for global leadership. This struggle concerningly could return the world to a bipolar era—a division of the international arena into two blocs, led by these two countries.[180]

Widening the Gap between Developed and Developing Countries

Changes in the field of AI may widen the gap between developed countries and developing ones and could limit the ability of the latter to operate in the international arena and perhaps even to maintain their sovereignty.[181] This gap could lead to large waves of emigration to advanced countries, or for certain countries—or groups within them—to use violent measures such as terrorism in response to threats because of their inability to cope with the gap that already exists today between those who have access to advanced technologies and those who do not.[182]

Improving the Quality of Life and the Stability of the International Arena through Deterrence

In addition to the pessimistic forecasts concerning the effect of AI on the international arena, it is forecasted that AI will positively increase the global economic growth rate; find cures for illnesses and improve health systems; improve the efficiency and safety of transportation; encourage energy efficiency and improve the understanding of climatic phenomena; and perhaps even to lead to peace-based stability in the international arena by means of deterrence.[183]

Chapter Eight:
What Can Be Learned from the Autonomous Weapon Systems?

In the security field in general and in that of the battlefield in particular, autonomous weapon systems (AWS) are extensively discussed in terms of autonomy and AI. The public discussion has focused on the limitations of these systems for several years, and since 2014 the official UN discussions have also focused on them. This test case focused on AWS seeks to expand the understanding of some of the challenges presented by the development of AI.

AWS can be defined as systems that are capable of performing a lethal operation without direct human input, as a result of interaction between the environment and the computer system.[184] Nonetheless, some bodies use wider or more operative definitions.[185] Various AWS are operational today on the battlefield and are used in different applications, ranging from active defense systems to systems for conquering and attacking targets on land, air, and sea.[186]

A key reservation about these systems relates to the ethical and legal implications of implementing lethal action without a person being involved in the process. Those opposed to these systems claim that their use violates ethical norms, since they are lacking human compassion and sensitivity. In warfare, international humanitarian law prohibits targeting civilians who are neither involved in the hostilities nor vital to the armed struggle, in addition to prohibiting any disproportionate harming of military targets; thus, the legal claim against the AWS is that they do not have any decisive ability to distinguish between civilians and combatants, which even people lack.[187]

In addition to the principle of distinction, international law dictates the principle of proportionate response, meaning that harming the target should be done according to the estimate of the target's contribution and importance to the success of the adversary's efforts.[188] This estimate varies and is affected by the characteristics of the battle and its progress—often in many arenas at the same time—which AWS (today) find difficult to weigh during their operation,[189] especially given that single-valued criterion specified in the law that can be encoded into the system for implementing principles.

The difficulty in implementing these principles within the autonomous systems is just one example that the law poses to new autonomous systems. Another dilemma is the issue of legal liability, which is unenforceable when a person is not involved in making the decision. It is not clear who should be prosecuted if these systems cause undesirable consequences that contradict international law.[190] Similar to the field of AWS, AI systems may also challenge the conventional law and moral codes and may compel humanity to provide practical answers to complex questions. Undoubtedly, ethical and legal dilemmas will emerge wherever autonomous devices can make decisions about human life or can endanger human lives, such as when they are on the road or used in medicine.

AWS also poses a regulatory dilemma, which includes the problem of defining the technology and the challenge of limiting its development. The United Nations has been discussing these systems since 2014, and even more so since 2016 when it established a group of governmental experts on lethal autonomous weapon systems (GGE on LAWS) to discuss the possible limitations on the development or use of these systems and their integration into the battlefield.[191] As of 2020, however, the member states of the GGE on LAWS have not yet managed to agree even on the definition of AWS so that they can present recommendations for coping with the challenges the technology poses.[192] Even if the GGE on LAWS can agree on a definition, restricting the development of these technologies requires the cooperation of all countries, including Russia and the United States, which do not restrict development.[193] Instead of imposing restrictions, they want to encourage economic growth in AI and an open market, in addition to maintaining their military superiority—even if they choose not to use autonomous weapon systems.[194] Therefore, these countries support the regulation of a particular field only after developing the technology, rather than limiting its development in advance.[195] Limiting the development and use of these systems might also become difficult to implement, due to the fast speed of development and the slow pace of regulation.

Some have argued that formulating a response to the ethical dilemmas of AI and advanced technologies will benefit humanity.[196] The case of AWS, however, shows that the political and international arena will most likely not reach a consensus on the regulatory framework, due to the opposing interests of the various players. Moreover, the ability of the systems to change and develop as a result of their ability to learn will undoubtedly affect the challenges that AI poses, such as being difficult to define or limit with exiting legal and regulatory means.

The technological development of AI presents decision makers with ethical, legal, and regulatory challenges at both the national and international levels. Given the complexity of the issue, it is advisable for countries to act and formulate a position on the subject so that they can ensure their interests.

Part III: Artificial Intelligence and National Security in Israel: Opportunities and Challenges

Scientific research is needed not just for security needs, all of our economic and cultural activities cannot be described without fully using the conquests of science and technology. The development of Israel, the advancement of agriculture, industry, the navy, education, curing the nation, demand all to cultivate science to the best of our ability. The same is true of our security needs.

David Ben-Gurion, the first prime minister of Israel

Chapter Nine: Artificial Intelligence in Israel

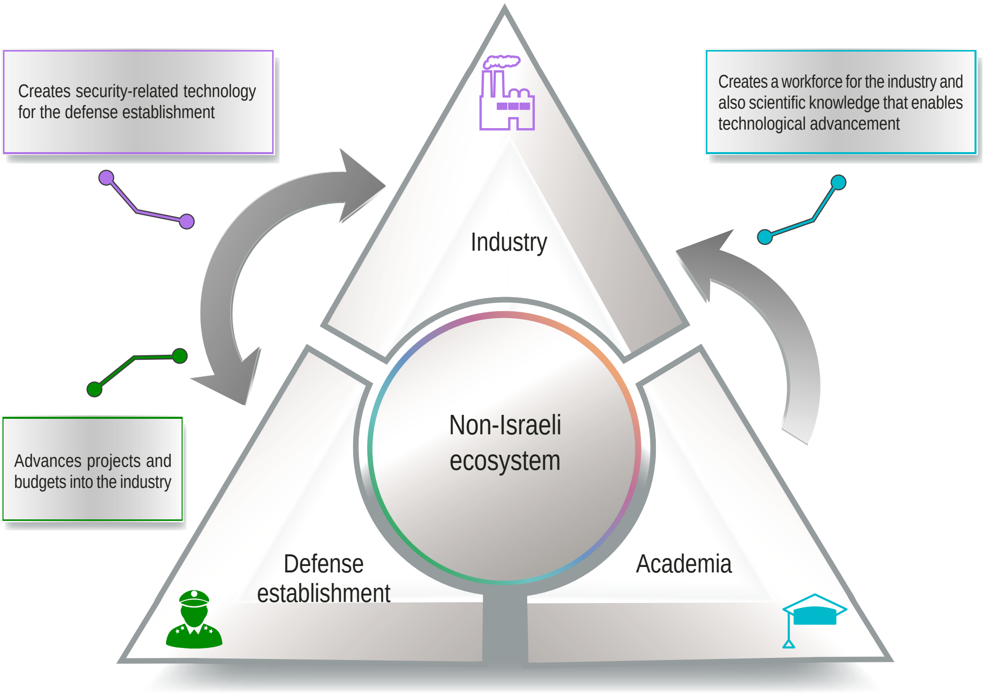
Israel is an international technological leader in both civilian and security fields. In recent years, Israel has gained a significant foothold in AI, thanks to the growth of startups in Israel and to the international companies that have established development centers in Israel. A large part of the security solutions have embedded AI into their systems, which strengthens their capabilities. Israel has several characteristics that affect these aspects, and this chapter will describe the fields in which Israel leads, including the unique ecosystem and the interactions between the various elements.

Israel's Technological Strength

Known for its powerful technological strength, Israel has been referred to as the "startup nation," because of its large number of startup companies in comparison to the size of its population. Technologies and capabilities in the field of communications that the security establishment developed in collaboration with the academic sector enabled Israel to take advantage of the developing internet in the 1990s. Many Israeli companies at that time, among them Checkpoint, Amdocs, and Nice, firmly established Israel's stature as a leading power in the fields of communication, security, data storage, and semiconductors. Furthermore, Israel's entrepreneurial culture has led to the growth of innovative companies, which greatly have contributed to the country's successful technological ecosystem.[197]

Israel understood from its inception that it must compensate for its lack of natural resources and limited human resources compared to its adversaries by investing in human resources and technology, an understanding that was embedded in the national security strategy of the first prime minister, David Ben-Gurion. Over the years, Israel's success in these areas has grown.

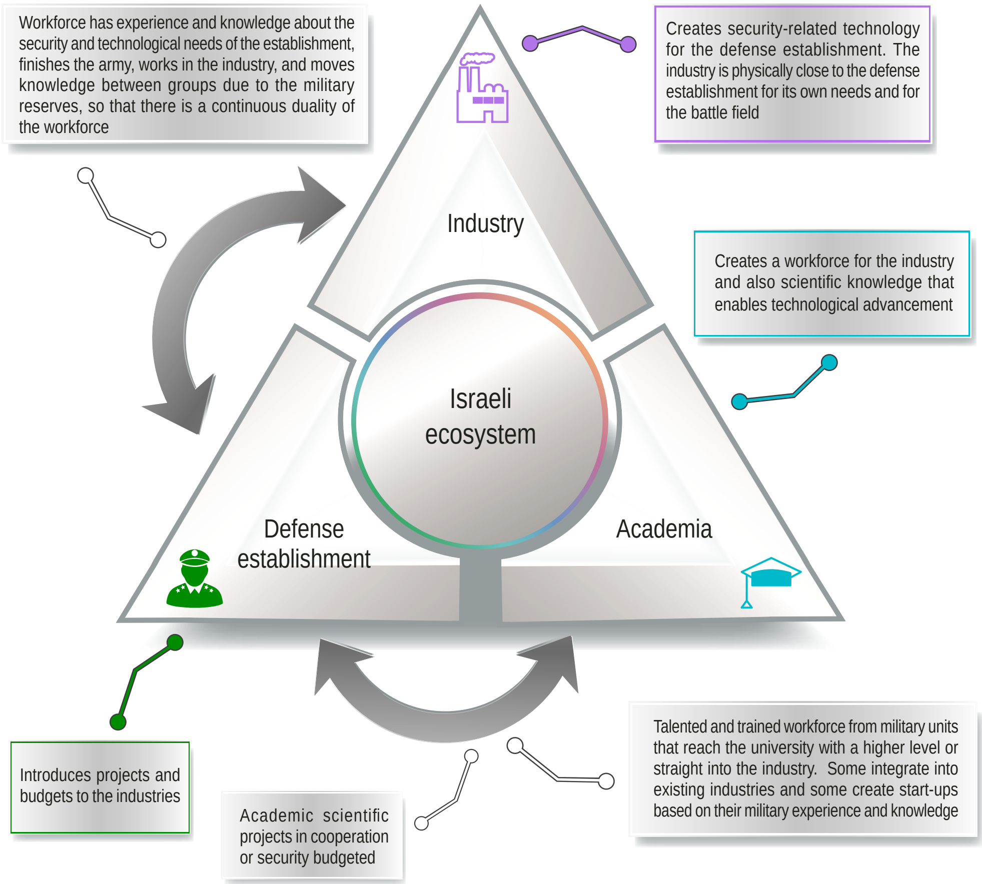
Figure 7. The non-Israeli ecosystem


Creates security-related technology for the defense establishment
Creates a workforce for the industry and also scientific knowledge that enables technological advancement
Industry
Non-Israeli ecosystem
Advances projects and budgets into the industry
Defense establishment
Academia

Security exports, for example, increased and transformed Israel into one of the world's largest weapons exporters, while the security industries have turned Israel into a technological and economic power whose capabilities many countries rely upon and are interested in acquiring or utilizing.

The competitive advantage of Israel's security industry in the international market has resulted from its close relationship with the IDF, as the industry relies upon security units to advance the research, development, and implementation processes, which promote sales.[198] The "double-feeding element" (the transfer of human resources between the IDF and the security industries)—partly the result of the mandatory military service model and the unique Israeli military reserve service—also influences the transfer of knowledge and strengthens those responsible for Israel's technological strength. As a result, the Israeli ecosystem differs from that of many other countries, as the two figures below show.

Figure 8. The Israeli ecosystem



Workforce has experience and knowledge about the security and technological needs of the establishment, finishes the army, works in the industry, and moves knowledge between groups due to the military reserves, so that there is a continuous duality of the workforce

Creates security-related technology for the defense establishment. The industry is physically close to the defense establishment for its own needs and for the battle field

Creates a workforce for the industry and also scientific knowledge that enables technological advancement

Introduces projects and budgets to the industries

Academic scientific projects in cooperation or security budgeted

Talented and trained workforce from military units that reach the university with a higher level or straight into the industry. Some integrate into existing industries and some create start-ups based on their military experience and knowledge

The Israeli Ecosystem and AI

The Israeli ecosystem is comprised of security bodies, the academia, and industry and operates cooperatively, sharing ideas and human capital. For example, the Israeli academia enables research that contributes to the development of AI and forms the basis of different AI systems.[199] The leading industries and the giant technological companies have also established research centers, working alongside thousands of innovative startups. The industrial sector has also witnessed a significant increase in the field of AI. Between 2014 and 2018, the percentage of companies engaged in the field increased by 120 percent, from 512 companies to 1,150, some developing the core technology of AI, and others developing supported technologies, such as autonomous vehicles and cybersecurity.[200] Gartner, a research company, has ranked Israel as leading in having the "cool and hot" vendor companies in 2017, over China and the United Kingdom.[201] The existence of these companies is made possible partially by Israel's unique ecosystem. Moreover, the year 2018 was a turning point for the funding of Israeli companies that engage in AI, raising about $2.25 billion[202]—a testament to the rapid growth of this market.

The security bodies and the military also have undergone impressive development, especially for the purposes of military intelligence—so that they can cope with a wide range of sources of information—and for operational activities. In addition to processing data and reaching conclusions, various autonomous systems, such as gliders, robots, sensors, and vehicles are being developed and are even being used at the forefront of knowledge and ability in the world.[203]

In Israel, connections between academia, the civil–commercial industry, and the security bodies occur quickly at the organizational, social, and professional level, due to Israel's advantage of being a small country. Beyond the physical closeness, which promotes innovation and creativity, academia and industry in Israel share a "partnership of fate," which helps mobilize them to work together on behalf of Israel's security.[204]

The short physical distance between the substantial concentration of technological companies and Israel's government or security centers also helps strengthen cooperation. This is quite different from the situation in the United States, for example, where the geographical distance and the time difference between Washington DC and Silicon Valley—the technology development center—are considerable.

The direct link between senior and high-ranking personnel in many places (including in certain military units) and an open and entrepreneurial character of Israeli culture (in comparison to countries where it is more hierarchical and bureaucratic) help move ideas and gain achievements. In the field of AI, Israel does not seem to have any special advantages, but in areas such as big data or hardware, the strength of Israel's ecosystem gives it a relative advantage. At the same time, however, Israel's size and its limited resources also create challenges, so it is important to combine the different relative advantages to create force multipliers.

Israel's Other Technological Advantages and Integrating Forces with AI

Other fields have a relative technological advantage and provide Israel with strength and influence in the international arena. One is the development, production, and export of unmanned aerial vehicles (UAVs), in addition to Israel's extensive operational experience in the field. Already in the 1960s and 1970s, Israel used drones for photographic purposes, and in the 1980s it began to use them for deception and information gathering. In the 2000s, the main use of UAVs was for military intelligence-gathering in asymmetric conflicts, with the Second Lebanon War (2006) being a turning point. This was the first war in history in which more unmanned flight hours were carried out than flight hours of fighter jets, and in which the UAVs loitered continuously over the fighting area throughout the entire fighting.[205] This turning point demonstrates the capabilities and experience that Israel has had in the field as early as 2006.

Since then, Israel has continued to invest in this field, and in recent years, it has made large deals with countries such as India and Germany. From 2005 to 2013, Israel was the world's leading exporter in the UAVs market, with the Israeli market share of exports reaching about $4.62 billion.[206]

Israel is also one of the leading countries in developing, producing, and using other unmanned systems, some which enjoy a level of autonomy. These include unmanned patrol vehicles, ground robotic systems, and loitering munitions, such as the Harop and the Harpy, which the international arena considers AWS.[207] According to foreign news reports, China, Germany, India, South Korea, Turkey, Uzbekistan, and Azerbaijan all have purchased these systems.[208]

Israel also gains strength from the nations that seek to collaborate with it, given Israel's significant technological knowledge and experience over the years. For example, Israel and Japan have announced joint research in military drones and unmanned surveillance systems. Israeli–American cooperation to protect against unmanned aerial systems should also be noted.[209] In addition to the strengthening of contacts, Israel also has used its advantage in the field such as when Israel agreed to sell drones to Russia in exchange for Russia's avoiding the sale of S–300 anti-aircraft weapons to Iran.[210]

Israel also is a global leader in cybersecurity and cyber warfare. As part of the "dual feeding" process, leading military technology units such as the Unit 8200 of the IDF intelligence recruit talented high school graduates for military service, where they receive significant training and experience, and upon their release from the army, they integrate into startup companies or establish their own companies, many in cybersecurity. As a result of the military service that grants professional experience, the graduates of this unit are able to cope with complex issues faster and more efficiently than university graduates or young entrepreneurs who were not part of these military units and who lack practical experience. In addition, Israel's National Cyber Authority oversees the national computer emergency response team (CERT) and coordinates with the private sector.[211] This serves as a global model for coordinated handling and managing of issues and resources. In recent years, the Israeli security industries have also devoted a great deal of resources and effort to the cyber sector to maintain Israel's competitive advantage and to avoid being dependent on other countries.[212] A survey of companies in the fields of AI, data science, and intelligent robotics found that cybersecurity is considered the main technology in which Israel has the capacity to lead.[213]

Israel has another relative advantage in the autonomous automotive industry. Israel's strength is in development and implementation of complementary technologies for autonomous systems, including sensors and navigation systems, and Israel has recently permitted more testing of autonomous vehicles within its borders using a real environment. A number of ventures in this field operate in Israel and these include technological testing of autonomous vehicles, carried out by the giant companies, alongside small startups, as well as several trials of transportation services with autonomous vehicles.[214] Companies such as GM and Mercedes develop autonomous technologies for cars in Israel, while Volkswagen has partnered with the Israeli company Mobileye in developing an autonomous taxi service. According to a report of the company KPMG, which provides financial services and organizational consultation, Israel ranks first out of 25 in the fields of technology and entrepreneurship, primarily due to the military experience of its entrepreneurs.[215]

Developments in the field of AI and Israel's ability to improve its achievements in these areas and preserve its competitive advantage directly influence the technological areas mentioned here. Moreover, having a combination of abilities in the various fields could serve as a significant power multiplier for Israel. Given Israel's size and the limitations of its human resources, it is imperative that Israel emphasize a combination of fields to increase its competitive advantage. Therefore, mobilizing Israel's ecosystem, which has high-quality capabilities in the field of AI by using existing technological advantages, should ensure that Israel has long-term defensive and technological power.

Chapter Ten:
Artificial Intelligence, National Security in Israel, and the IDF Strategy

In dealing with the issue of AI and national security, it is essential to understand not only the technology and its capabilities but also the concept of national security itself. This concept has been subject to controversy, which is mainly political, cultural, or environmental. This chapter describes the general concept and relates specifically to Israel's security concept.

What is National Security?

National security is the ability of a nation to protect its citizens and its internal values from threats, including hostile states and terrorist organizations.[216] In other words, national security is "ensuring national existence and protecting vital interests."[217] A more expansive definition of national security is the "preservation of norms, rules of institutions and values of a society."[218]

Although the historical and theoretical reference to national security emphasizes military aspects, a broader approach is now widespread. Besides the external security–military threat, the United Nations, for example, includes seven layers in its definition of national security: (1) economic: creating employment and implementing measures to prevent poverty; (2) food: taking measures to prevent famine and a lack of food; (3) health: ensuring means to prevent diseases, contaminated food, malnutrition, and lack of access to basic medical care; (4) environmental: taking measures against environmental damage, depletion of resources, natural disasters, and pollution; (5) personal security: employing measures to prevent physical violence, crime, terrorism, domestic violence, and child slavery; (6) community: applying measures against ethnic, religious, and other identity-based tensions; and (7) political: taking measures against political repression and human rights violations.[219]

It is possible to narrow the gap between theoretical definitions and reality by examining and analyzing a country's national security concept, which is usually expressed in its national goals in regards to its capability and the challenges that might hinder them, in addition to the methods and resources used for achieving these goals.

Israel's Security Concept

Unlike many countries in the world, Israel has not enshrined its security strategy in an official document approved by the Knesset (Israel's parliament) or the government. Today, the foundations of Israel's security are considered to be deterrence, early warning, and decisive defeat, with the fundamental principle of defense having been added over the years. The central goal of the security concept is to ensure the existence of the State of Israel, create effective deterrence, neutralize threats, and thwart confrontation. The role of thwarting confrontation has grown over the years, partially due to the increasing threat of terrorism and indirect fire at Israel's civilian front by hostile organizations along Israel's border.[220]

For the past two decades, the following five main dimensions have been included in the term "the national security of Israel": (1) internal and external security; (2) international affairs and Israel's international status; (3) the national economy and resources; (4) governability (expressed by the ability to make decisions and execute them); and (5) the strength of civil society.[221]

Given the geopolitical changes in the Middle East and changes in the inner Israel arena that have taken place since the establishment of Israel, a government committee, led by Dan Meridor, was formed to address Israel's national security and presented its conclusions in 2006. The document produced by the Meridor Committee—much of which is still classified—is considered to be the closest Israel has to an official security concept, given that that it was adopted by then minister of defense, Shaul Mofaz, and that parts of it actually have been implemented, although this concept was never approved by a cabinet or the entire government.[222]

The Meridor report lists the national goals upon which Israel's security concept is based as follows:

1. Ensuring the survival of the State of Israel and protecting its territorial integrity and the security of its citizens and inhabitants;

2. Protecting the values and national character of the State of Israel, as a Jewish and democratic state and as the home of the Jewish people;
3. Ensuring the State of Israel's ability to maintain its socioeconomic strength, like any other advanced country;
4. Reinforcing the State of Israel's international and regional standing and seeking peace with its neighbors.[223]

Similarly, the Meridor report also addresses various challenges facing Israel, such as non-conventional weapons, terrorism, and confrontation with regular armies, and emphasizes the policy of response.[224] Furthermore, the report also relates to other key issues that form Israel's security agenda, including the Palestinian issue, the international–political arena, security resources, the "people's army," the quality advantage, and decision-making processes, in addition to the comments that the report raised regarding national military intelligence and the process of implementing and updating the security concept.[225]

In examining the Meridor Committee's report a decade after its publication, Dan Meridor and Ron Eldadi claim that the report's original conclusion—that a conventional military threat is unlikely, especially given Israel's military strength and superiority and the Arab world's increasing weakness—is still valid.[226] At the same time, the Meridor report also refers to factors that have shifted greatly over the past decade, such as cyber, which has become a key factor of the highest degree in the security concept of deterrence, defense, and attack. Another factor is the increase in "soft" components, such as cognition, media, law, and others, in addition to the need to strengthen cooperation with key players in the international and regional arenas.[227]

In short, despite the absence of a government-approved official document, the general outlines of Israel's security concept are manifested in earlier documents, actual policy, and the Meridor Committee's report. This is in spite of the fact that the concept has shifted at times with changing regional or international policies. At the very least, the core foundations of the security concept are evident, some of which have not changed since the establishment of the state, and some that are newer but have been increasingly validated by their adoption, investment, and implementation in the past two decades.

How Can AI Affect National Security in Israel?

Rapid advances in technological development have re-enforced the belief that AI will extensively affect a country's national security. This is apparent from the assumptions of researchers and senior figures in the field as well as national programs and budgetary investments of leading countries, including the United States, China, and Russia. As a state with advanced capabilities in AI and broad security needs, Israel could benefit greatly from using AI and its applications to achieve and preserve its national security objectives.

For the past two decades, AI has significantly affected the following dimensions of Israel's national security: (1) foreign and domestic security—by using AI applications in military intelligence, weapon systems, and other military systems; (2) foreign relations and Israel's international reputation—by preserving the status of Israel as a technological leader and exporter of technology and knowledge; (3) the economy and the national resources—by developing and investing in AI as a leading field in Israel's economy, which greatly relies on technology (rather than on natural resources); (4) governability—by overseeing the making and implementation of decisions and support for decision making and simulations; and (5) the strength of civil society—by improving the quality of life of Israel's citizens.

An analysis of the four basic pillars of Israel's security concept—deterrence, early warning, decisive defeat, and defense—reveals that AI potentially could have a positive impact on achieving and maintaining each pillar, by integrating AI into the different military systems or by creating new ones.

AI can greatly assist in achieving many of the goals presented in the IDF Strategy (2018) by the Chief-of-Staff Gadi Eizenkot. The strategy comprises four basic efforts that are relevant to all military action: attacking, defensive, assisting, and enabling.[228] Technological superiority is crucial to advance these efforts, with AI being central to this superiority.

For example, AI has been used in aerial defense systems, which have a considerable impact on the defensive effort. Also, extensive use of AI in military intelligence and telecommunications helps improve capabilities relevant to the warning systems. AI can also assist the IDF in operational learning and planning (also mentioned in the IDF strategy),[229] whether by using planning and simulation systems or by using technologies. They can reach conclusions that were impossible to reach in the past with human efforts, due to the difficulties in handling and analyzing vast amounts of data.

In addition, Israel has a comparative advantage in technological fields, including unmanned systems and cyber, which are distinct security fields. Combining these fields with AI as a power multiplier can help Israel to preserve and expand its national security, whether done through military means or economic and international influence.

Chapter Eleven: Challenges in Using AI

Along with the rapid technological advances in AI, a number of various challenges have appeared in different arenas. A discussion of the challenges is important to examining the ways of dealing with these challenges, within the policy framework.

Table 3. Various challenges in using AI

Technical Challenges	Organizational Challenges	Challenges of Use	Security and Political Challenges
Challenges in development	Designated budgets	Safety and reliability	Ethics in warfare
Adapting civilian technology for military use	Human resources	The difficulty of adaptation	Law and justice
Standardization	The challenge of being a small state	Adapting the pace	Dependence
Hardware and energy	The approach of senior officials toward AI	Unexpected results	AI among Israel's adversaries
Implementation challenges	Politics and opposition to organizational changes	A person in or out of the operating loop	The arms race
Configuration	The connection to the civilian industry	Biases	Arms control
Data	Mistrust and gaps between the civilian and military spheres	Ethics	Cyber warfare
The "black box"—explainability		Fake news—the operational challenge	Nuclear weapons
			Hyperwar
			False information
			Job market and employment
			Extreme inequality in distributing resources in society

Technical Challenges

Challenges in development. In the past, the relationship between the IDF, industry, and academia was conducted in such a way that the army led the technological development, while commercial companies and the academia adopted the technologies developed. In recent years, this has been reversed: Commercial companies carry out most of the development, while the army adopts the technology and adapts it to its needs.[230] This creates difficulty in developing high-quality security technology, since the army does not have the needed professional knowledge. While the civilian AI companies rely on senior academics or on a leading academic body, the security establishment is challenged in all that relates to developing knowledge or products that are AI-based. Furthermore, the security establishment does not engage in independent research and development, which produces the infrastructure for future specialized abilities that are essential to achieving a comparative advantage. The security establishment, however, is currently closing the gap with civilian industry.

Adapting civilian technology for military use. Adapting civilian technology for military use poses a challenge in that it causes the algorithm to provide a solution that is inappropriate, as a result of being trained for other needs.[231] The difficulty in adapting the technology is partly due to the code-to-product challenge; that is, the transition from lines of code based on theoretical research to a product that can be used in practice. Furthermore, the academic and industrial involvement in AI focuses more on investing in the research rather than on producing AI. In many cases, even when the research is quite advanced, it is not applicable to security agencies, either due to technical reasons, such as processing power, or because they relate to the civilian world, which do not always correspond to security needs.

Standardization. Standardization in the fields of performance and safety in the civilian market differs from the security arena. In addition, research studies indicate that AI systems increasingly fail in complex environments outside the laboratory, contributing to the difficulty of the civilian and military sectors to work together.[232] This means problems and delays in integrating civilian applications into the security sector.

Hardware and energy. AI systems require tremendous computing and processing capabilities, both which need cooling and electrical power. Few bodies can meet the energy consumption required, both in terms of supply capability and cost. Google, for example, deals with this difficulty by using AI systems that help reduce the energy consumption by approximately 30 percent.[233] Facebook has tried to address the issue by establishing a data center near the Arctic Circle, in northern Sweden, to make use of the region's natural climate for the cooling needs of the data centers.[234] The increase in efficiency in this area, however, is still marginal compared to developments in other areas related to AI, and most bodies—with the exception of these technological giants—and countries find it difficult to cope with this challenge.

In addition, the need for sufficiently powerful hardware, which will enable the processing capability, is another challenge. Israel currently does not have enough servers and it lacks a national infrastructure in the field of AI. This is unlike other areas of computerization and science, where Israel has invested significantly in national infrastructures, enabling it to achieve international leadership in the field.

Implementation challenges. "Legacy systems" is the accepted term for expensive military systems that have a long lifetime and are not replaced frequently, such as airplanes and tanks. The implementation of AI in these systems is a challenge, given the frequent and dynamic changes in the field of AI.

Configuration. The rapid rate of change poses a challenge for the bureaucratic security establishment in terms of the configuration of AI. With the development of new systems and products, the security establishment considers several options and chooses the preferred one for the system's configuration. Afterwards, it distributes this configuration to the users with instructions for use. As AI is constantly changing, defining the configuration is difficult. AI is likely to challenge the security establishment in determining whether the product in question is good enough for distribution to the users in the various security agencies.

Data. Data is the cornerstone of developing high-quality AI, considered the "oil of the new era," as data enables training the algorithms and preparing them for autonomous action. A lack of data challenges the security establishment's ability to use AI. For example, in the security sector, where sensors have been used for several years, the data is, for the most part, erased at times, due to the lack of space and high costs of storage. In addition, the information collected over the years may not always be suitable for processing within the framework of AI, and it is necessary to “clean it” and rearrange it to accommodate its use with an AI application.

Secrecy and compartmentalization are another challenge for security agencies. As the security agencies are not connected to external networks and cloud technology, they are unable to use the data centers of other entities, whether civilian or security, sometimes even within the same organization. Therefore, these bodies are compelled to operate within the framework of their hardware capabilities and internal databases. The security establishment avoids sharing not only data but also algorithms or results obtained for various bodies, due to fear of exposing data through reverse engineering.

Moreover, in the intelligence and operational world, the occasional lack of data does not enable the training of vital algorithms needed to solve problems. For example, one image or a few images of strategic importance are not enough to train the algorithm properly to act on that subject or phenomenon.

Furthermore, the security agencies collect most of the information in routine times and do not address statistical changes in emergencies or combat. Databases do not represent a future operational reality, and as a result, data training is done based on routine or emergency scenarios from the past. This challenge is comparable to preparing for the war that already has occurred, while the operational arena is unpredictable and constantly changing.

Another challenge facing security organizations in the field of information is the difficulty in relying upon off-the-shelf AI products. The security and military intelligence agencies have unique problems, which require dedicated collection and analysis of data that does not exist in the civilian sphere.

“The black box”—explainability. One of the main characteristics of AI system is that it is a “black box,” meaning it is unable to explain the processes that cause the system to make a particular decision.[235] In the national security sector, transparency is significant, as a problem usually has more than one solution, and examining all the considerations when choosing a solution is crucial.[236] Therefore, the absolute reliance on AI systems in decision making, without understanding how the decision was made, is of concern. A central question in this context is whether the machine and the person share the same understanding of the goal and the limitations of its implementation.[237]

Directly related is the lack of trust in systems. Trust issues make it difficult to implement AI systems in areas where the implications are likely to be very costly.[238] Even if an algorithm can be explained, this will not be a perfect solution, particularly since research explainability tends to differ from operational explainability. The transparency threshold required for each user and domain is different, and full transparency will not necessarily contribute equally in all areas.[239] Similarly, explainable solutions in every application is not possible, because in applications that must operate in very short time constants—sometimes beyond the limit of human ability—it is impossible to place a person in the system's operating loop to analyze the explanatory data.

It is important to remember that the goal of explainability is to improve the performance of the application, although it is not perfect. However, even today, when people make the decisions, there are errors, whose implications can be serious. If the machine is statistically less likely to err, and thus performance is improved, it is better to rely on the machine—despite the challenge of explainability—except in areas when a principled decision is made to avoid relying on the decision of the machine, such as for moral or legal reasons.

Organizational Challenges

Designated budgets. To develop and implement AI systems, significant investment in computer power and support systems, as well data security, infrastructure, and people is necessary.[240] Nowadays, giant commercial companies have immense budgets—sometimes even greater than those of certain countries—and military and political bodies find it difficult to compete and obtain the budget needed for development and implementation. This is one reason that the security bodies prefer to deal with technological issues such as cyber rather than AI. Security bodies have also estimated that they can rely upon future civilian developments. Moreover, some relevant security and political organizations have not even properly budgeted the field of AI, and some have not budgeted it at all, due to its novelty and the difficulty of changing and adapting the AI system.

Human resources. It is difficult to recruit and retain skilled personnel who can develop, adapt, and implement AI systems into the military and state bodies, because of the stiff competition from the private sector, which offers better employment conditions.[241] In addition, because of the restrictions of the security organizations—confidentiality and compartmentalization—personnel does not move freely between the different security organizations, and creating a career path that will retain qualified people in the service of the state is difficult. This is a significant challenge, given the narrow size of this field, Israel's limited human resources, and the fierce competition for talent from the civilian companies.

The challenge of being a small state. Being a relatively small country often positively influences Israel's ecosystem in the field of AI, mainly because of the close proximity between decision-making centers and the technological development centers, as well as the direct connection or relative closeness between decision makers and developers or companies. Israel's unique model of mandatory military service and the reserves service that influence movement of human resources from the army to the civilian industries both benefit Israel's technological fields. Israel faces investment and budgeting difficulties, however, due to its small gross domestic product (GDP) compared to competing countries. Therefore, it is essential to distribute efforts and skilled personnel to a variety of security and market needs. Moreover, the entry of the giant technological companies into Israel—despite developing centers to develop AI and benefiting Israel's economy—has created a bottleneck in the field, creating a challenge for human resources.

The approach of senior officials toward AI. Decision makers tend not to be familiar with the capabilities of AI and do not appreciate the significance of integrating AI into the security fields. Commanders and senior officials are also reluctant to operate according to analyses produced by an AI system. These are primarily veteran personnel who are part of the decision-making community and are required to approve procurement programs or to make important decisions in other areas. Even relatively low-level personnel in the field, who, for the most part, do not have a statistical and mathematical background, find it difficult to rely on AI systems and to manage operations or other activities that are based on them, even though they are more likely to relate to technology than the generation of senior officials.

Politics and opposition to organizational changes. Technological change often transforms the nature and definition of people's roles, discouraging any affinity for AI among personnel in security organizations, which are large and bureaucratic. In addition, implementing AI does not bring any immediate benefit, and therefore personnel tend to resist its implementation and use.[242] Political reasons—fear of changes in position or job—partly fuels this resistance, similar to the historical objection to mechanization or computerization.

The connection to the civilian industry. The organizational nature of the security establishment poses a challenge to the relationship with the civilian industry, which is crucial to the development of AI. For example, the procurement and contracting processes are complex and prolonged when working with the army, in contrast to the civilian market, where transactions are done quickly.[243] The security establishment is not used to working with civilian commercial companies, especially startup companies. These startup companies have promising technology, but they lack the administrative infrastructure that will enable them to work with the bureaucratic security establishment. Furthermore, many startups never mature into enduring companies, and security agencies are reluctant to sign contracts with them as they lack confidence in their continuity over time.

Mistrust and gaps between the civilian and military spheres. Some companies are reluctant to cooperate with security officials for ethical reasons, or out of fear that their employees will object (this problem is less serious in Israel than in the United States, for example). Companies that develop innovative products also tend to be fearful about signing contracts with security agencies, due to intellectual property considerations.[244] Another concern relates to the definition of AI as being a security-based product and the export regulations that are applied to it, which make it difficult to export. The security establishment is also apprehensive that work done in partnership with commercial companies could result in leaking knowledge, algorithms, and information, as a result of exposing or commercializing a product jointly created.

Challenges of Use

Safety and reliability. AI systems and a substantial part of the technologies upon which they are based are new and innovative, and in some cases, it is difficult to explain how they operate. Thus, it is not easy to adapt them to safety standards and to ensure their reliability prior to use. At the same time, it is difficult to exercise or implement the use of these systems so that their speed and novelty is realized, but not at the expense of safety and proof of reliability. This difficulty is expected to increase as systems change, develop, and require repeated inspections. The need to balance between the nature of these systems and the need to act swiftly vis-à-vis the current standards of the security sector is likely to pose a challenge, from the decision-making level to that of the commanders in the field.

The difficulty of adaptation. AI systems have difficulty adapting to new environments (domain adaptability),[245] which is crucial to the dynamic security arena, especially the battlefield. This challenge is also apparent in the need to train the systems for the proper environment, where data in the field is sometimes lacking. The limited ability of the users themselves to get the desired results from the AI systems also affects this difficulty.

Adapting the pace. The ability of AI to act and react quickly can be an advantage, but there is concern that changing the pace in the battlefield will cause instability, especially if it surpasses the operator's ability to understand events and control them at the operative level.[246] Another problem may occur if the pace of operating the systems exceeds the ability of the security establishment to absorb events, analyze them, and choose the strategically effective response. (This challenge may also affect international aspects such as *hyperwar*.)

Unexpected results. AI systems sometimes produce unpredictable and non-conventional results, as already mentioned. This may be advantageous in the battlefield, especially in terms of analyzing military intelligence or being able to surprise the other side. However, it is also liable to cause serious risks and errors, which are caused by the system's assumptions that differ from those of a person at their own discretion.[247] In addition, technical debt—a gap between the pace of technical development and the sufficient understanding of the behavior, risks, and control methods needed to manage this technical development—is a concern.[248] In the context of AI and national security, this relates to the militaries that use AI-based systems too quickly, without fully understanding them. Even if the risk of using a single AI-based system seems minimal, its interaction with a rival system that has been trained on a different database may have serious consequences, especially if an arms race in the field takes place.[249] Furthermore, the explainability challenge makes it difficult to devise ways of coping with various security events, and of preparing scenarios and responses accordingly.

A person in or out of the operating loop. Another challenge is the price of leaving a person in the operational loop vis-à-vis the ethical and legal problems that could occur if that person is removed. Maintaining a person in the operational and supervisory loop for ethical, safety, and legal reasons relates to the discussion of armed autonomous systems and other systems. Nonetheless, maintaining a person in the system's decision-making loop may slow down its operation. Some countries will face a challenge if they decide to keep a person in the operational loop of AI, while others or non-governmental parties will use AI without a person in the operational loop.[250]

Biases. It has been said that "an AI system is only as good as the data it accepts." When the data used to train the machine is not sufficiently diverse, biases may arise.[251] However, it can be argued that even when "the data is perfect," it actually reflects social bias, such as gender and ethnic differences.[252] Regarding the operational aspect, information that is skewed—accidentally or maliciously—may affect the systems' operation, including military intelligence systems, decision-making support systems, and AWS. Therefore, special attention should be given to systems that could affect critical decisions. In addition, in the security context, it is necessary to distinguish between bias that is caused by a lack of diverse data, which it is possible and even desirable to resolve, and biases that will be performed maliciously, by exploiting the systems' vulnerabilities of the adversary to create intentional deception.[253]

Ethics. Dealing with the moral aspects of AI raises questions about the systems' decision-making process and the ethical considerations taken into account. As already discussed, the systems may express bias and discrimination toward specific groups in society. However, most problems are discernable when it comes to potential issues affecting human life. Therefore, a certain amount of human involvement is necessary, especially when using systems that operate lethal force.

Fake news—the operational challenge. AI can create fake news that appears credible and whose origins are difficult to identify. False information could distort military intelligence or block the actions of military forces and could lead military officials to doubt the information they receive. Deceptive operations of the other side could make it difficult for the security establishment to instruct civilians in emergencies, or to share reliable and credible information to civilians and military forces. The security establishment might not be able to prevent transmitting false information that could harm soldiers and civilians alike.

Security and Policy Challenges

Ethics in warfare. It is difficult and perhaps even impossible to predict and program every decision that AI or an autonomous tool will be required to make in all areas of life. This is not merely a programming challenge but also an ethical one, especially in relation to situations and issues that lack consensus. Even in cases of consensus, AI decisions will be culturally dependent. Although the central challenge in this context is the use of LAWS, even in civilian areas, the use of autonomous systems has ethical implications, which must be considered.

The autonomy of AI and the accompanying ethical considerations have diverged into two opposing camps. One camp argues that AI-based systems such as robotic systems can be programmed to operate better than humans in many fields, because these tools can make decisions quickly and accurately and are not affected by fatigue, fear, or other physiological and emotional traits that characterize people. Some believe that ethical theories can be calculated according to considerations of pleasure and suffering.[254] In this way, these systems will actually be able to activate, in their own way, ethical considerations when deciding to perform an action.

The other camp does not believe that the AI-based systems can make moral decisions and believes that even in the future, these systems will not be able to make moral decisions. In the absence of both human emotions and the ability to evaluate and understand emotions, it is argued that AI-based systems cannot possibly make proper moral decisions, unlike humans, who relate to their actions morally. No matter how all-encompassing the programming of the AI systems is, it cannot encompass all elements of moral considerations; even if it could calculate pleasure and suffering, it would be hard to include considerations of justice or of sacrificing an individual for the sake of the community.

Regardless, it is impossible to ignore the fact that AI and autonomous systems based on it are quickly being developed and fulfill a variety of tasks in diverse areas. For the first time in history, these systems compel humans to make calculated and unambiguous decisions in fields that were until now based only on the decision making of individuals in different places in the world, based on their own education, values, and culture. Therefore, humanity may be required to formulate a unified set of values based on the joint thinking of the philosophers of various cultures, and jurists from different countries, to enable the world to develop and progress. Although this is an opportunity for international cooperation, given the difficulty of the international arena in reaching decisions about lethal AWS, it seems this will remain a challenge. Israel will also face this difficulty when it seeks to expand the use of AI in various fields, especially national security.

Law and justice. The responsibility for the consequences of using autonomous AI—accountability—poses a major legal challenge. While traditionally, the owner of a machine, or the one who operates it, is responsible for the consequences of its use, it is difficult to establish responsibility when actions are a result of autonomous learning and action, especially in the case of causing unintentional damage to property, improper discrimination, or human injury.[255]

Damage caused by the malfunction of an autonomous system can occur, for example, on the road, in a workplace, or as a result of incorrect diagnosis in the field of medicine. In these cases, it is not clear if the responsibility falls upon the manufacturer, the programmer, or the person who purchased or activated the machine. The problem is exacerbated on the battlefield where an error by AWS, for example, is liable to cause considerable destruction and harm to civilians—even if unintentional and if no human can be held responsible for it.[256] The difficulty in establishing legal liability makes it difficult for society to act legally against countries that deviate from international law, since they can operate autonomous systems and can cause considerable damage without facing any consequences for their actions. This situation is liable to encourage reckless actions and undermine the stability of the international system and national security.

Dependence. As AI is increasingly trusted, the nation's dependence on it could endanger national security if hardware malfunctions (e.g., power outages or difficulty in cooling down essential server farms), software failures, or intentional attacks occur. Moreover, the entire security system could fail if most security tools depend on it. Thus, it is imperative to maintain matching capabilities, such as weapons, vehicles, and communication systems that are not connected to AI. This need for redundancy creates a budgetary challenge, in addition to creating asymmetry between Israel and its adversaries who are more willing to depend on AI than Israel is.

AI among Israel's adversaries. The spread of AI may allow small countries and non-state organizations to negatively affect the battlefield, if they succeed in exploiting AI on a broad scale.[257] This challenge is particularly relevant to countries and organizations whose conduct is different than that of liberal democratic states. For example, Iran invests heavily in AI and is able to make quick moves in the field of technology, because it is an authoritarian state that controls industry, academia, and the army. Iran heavily invests in academic studies in AI and in 2018 was ranked the highest country in the Middle East—and ninth in the world—in the number of publications in the field of AI, out of 152 countries. On this scale, Israel is only ranked 46th.[258] At the end of 2019, Iran's president, Hassan Rouhani, called for cooperation with other Muslim countries to improve AI technology. Rouhani is quoted as saying that "digital economy is the future of the world economy, and growth in the field will be achieved by cooperation."[259] Israel should be concerned that other Muslim countries, some not amenable to Israel, will answer this call.

In this context, it should be noted that these are mostly non-democratic, non-liberal states, which could decide to use AI systems differently—regarding ethics and international law—from the way Israel chooses to use AI technology by means of self-limitation.

The arms race. The arms race in the development of AI is prominent between the United States and China, while Israel and Iran are the leading players in the Middle East. The race may undermine the world order and change the existing balance of power, if China catches up to the United States. Israel may have to choose with which side to collaborate—decision that will have security and economic implications.

Arms control. Technological developments that are based on AI, such as AWS, have stimulated discussions in international tribunals about their liability in undermining global stability and in harming human rights. This issue extends beyond morality alone. Countries with a relative advantage in the field—such as the United States and Israel—are not interested in restricting themselves, for both security and economic considerations. Moreover, in the past, the weapons control sector focused primarily on controlling systems and their distribution, and now the emphasis is increasingly on controlling components. Some believe that this change will help restrict countries from selling or acquiring certain technological abilities of AI applications, including the underlying software. This could reduce the interest in developing such technologies, because of the lower commercial incentive, or it could incentivize certain countries to develop them for their own needs and "against all odds."

Cyber warfare. AI systems expand the vulnerability that opponents can exploit. First, AI systems increase the number of "hackable things," including systems that could cause a fatal outcome. This concern increases if all the systems in the organization share the same vulnerability.[260] Second, "stealing" AI systems may be relatively easy, because they are almost exclusively based on software that can be used immediately after the theft (unlike stealing the plans of an airplane). Moreover, these systems have dual use, some of which can be obtained commercially and adapted for security purposes.[261] Third, AI systems can be used to detect new vulnerabilities and vectors to attack.[262] Adversaries will be able to enter errors aimed at the system's categorization, to damage its ability to identify, which is crucial in making decisions.[263] There is also a concern that AI systems could provide individual actors and non-governmental organizations with cyber capabilities that they did not have before. Even if they are unable to develop their own complex software for a cyberattack, they could adapt code developed by others.[264]

Nuclear weapons. The use of AI-based systems in the areas of decision making, military intelligence, or command and control could affect the operation of armaments, including nuclear weapons, regardless of whether these weapons are connected to AI systems directly or indirectly. Specifically, AI systems could increase the use of nuclear weapons, even if they are not directly connected to nuclear weapons launchers. This is due to a change in the balance of power, which has so far ensured relative stability, based on mutual deterrence.

Hyperwar. AI systems, the rapid pace of decision making that they allow, and the responsiveness of weapon systems could result in a hyperwar. That is, the rate of events could be so rapid that the operator or strategist would not be able to understand the events and control them, meaning that human decision making would almost never affect the process. Immediate reactions in a conflict have destructive potential, although in some of the cases and with certain systems they are liable to help produce deterrence.

False information. AI provides mechanisms for generating propaganda that is precisely adapted to specific audiences and for expanding its distribution. This is particularly problematic in terms of fake news, where false content is distributed in a very targeted manner, thus having a widespread impact.

Within democracies where communication and internet are open, AI can serve as a tool for foreign bodies that seek to influence the democratic processes using very effective distribution tools.

At the same time, however, AI systems can also be used to identify and filter false content. For the most part, however, the ability to create and disseminate false information through AI exceeds the ability of AI tools to identify such information,[265] since many examples are needed to train the algorithm to identify false information.

Bots are one example of this use. Bots are software programs that artificially simulate content that can manipulate the public agenda and dictate the content's widespread exposure, which is considered an indicator of its credibility. The use of bots was common in the US presidential election in 2016, when more than half of the network traffic belonged to bots, which distributed false information about the candidates.[266]

"Deep fakes" are another example. These are fake videos that take advantage of existing video and sound data arrays to produce bogus content that seems extremely credible. In fact, videos of this type challenge the understanding of the concept of "truth" and erode the belief in content and the credibility of empirical facts measured by the senses.[267] Israel, which is a democracy with an open media, faces both security and political challenges in this context.

Job market and employment. Given the technological revolutions, significant changes in employment are evident. Many scholars believe that humanity is on the verge of a new industrial revolution,[268] due to the development of AI and the IoT.[269] The developments of the fourth revolution are expected to produce new jobs, as occurred in the previous revolutions, improve efficiency in industry and services, and increase supply and lower prices. Lowering the prices should lead to a growth in private consumption, which will continue to encourage the expansion of the global economy.[270]

At the same time, however, these changes could cause many professions to disappear from the labor market. While the earlier revolutions led to the demise of professions that required manual labor, the current revolution could render professions in fields of knowledge and information redundant by replacing them with AI. The labor market could also become more flexible and rely on employees' skills and their adaptability to the changing reality, rather than on their professional knowledge.[271] This creates a challenge for developed countries, which will be required to change their approach to education and employment and create systems that will enable lifelong learning and development. Similarly, the state's support systems and the laws of employment will have to change to the new reality, to support the different population sectors and their needs.

Looking several decades into the future raises questions about when AI software will perform better than people do in various professions, such as writing books and performing surgeries.[272] This could cause a serious occupational crisis to most of humanity and would compel a new social order that does not revolve around employment. Alternatively, completely new professions and forms of work could emerge, that would not have the traditional characteristics of the work market today, including a physical presence.

An autonomous labor market poses indirect challenges to national security. First, autonomized industries would become a target for attacks from competing countries. Since the economies will increasingly rely on computerized systems, countries must focus on developing safeguards that will ensure the reliability of industries and of national security. Second, if the countries fail to find employment for many who lose their jobs due to the autonomizing of jobs, they will have to ensure their welfare by other means. Some countries, such as Finland, have discussed a basic living allowance to ensure the socioeconomic security of its citizens, some of whom will not be employed due to the effects of progress and automation.[273] Other countries will need to have this discussion, as certain areas of employment will be reduced by autonomous systems. Another important discussion of this field refers to the collection of "income tax from robots," which could begin to replace employees in various fields.[274] Such changes will be required to financially and socially stabilize society.

Extreme inequality in distributing resources in society. Globalization and technological advancement have widened socioeconomic gaps both at the national and global levels.[275] Because modern society is based on the distribution of profits according to relative contribution, the erosion of many professions could leave many people without the ability to contribute to the economy. While the economy will continue to grow, it is possible that fewer people will be able to benefit from the distribution of its profits.[276] Access to technology itself may also be characterized by inequality. The first state to have advanced AI will gain a “first advantage” over others in various fields, including economics and security. Similarly, individuals who have access to advanced AI technologies will also be advantageous. Inequality could also expand to access to health care, personal security, quality of life, and self-advancement.[277] In this context, it is foreseen that businesses with insufficient resources will not be able to compete with the AI capabilities of large companies, thus creating monopolies. Countries currently have considered limiting the major technological companies,[278] having recognized the inherent risks of those monopolies. This is a complex problem, which will continue to become apparent and will require a response as the technology develops.

Conclusion and Recommendations

> **The need to develop strategic concepts relevant to this new and inevitable technology has become overwhelming**

Henry A. Kissinger, an American policy maker, diplomat, and geopolitical consultant who served as US Secretary of State and National Security Advisor;

Eric Schmidt, an American businessman and former CEO of Google;

Daniel Huttenlocher, dean of the Schwarzman College of Computing at MIT.

Chapter Twelve: Conclusion and Recommendations

AI is a technology that has revolutionary potential in all areas. Being able to make a machine responsible for actions that were once carried out by a person and to surpass them—even in areas where automation was never imagine—has remarkable effects. Indeed, it is still difficult to fully assess the scope of the revolution and its characteristics, but it is impossible now to ignore the need to prepare for it and for its far-reaching implications, both for those who successfully adopt it and lead in the field, and for those who trail behind.

Israel currently has a relative advantage in the field of AI. This advantage relies on its being a "startup nation," and on past and present investments in science and technology, infrastructure, and education, which have enabled the growth of an ecosystem that integrates industry, academia, and security entities, advancing the field through collaboration, knowledge, and human resources at a level higher than in most other countries. As a result, AI could constitute a key factor in maintaining and strengthening Israel's national security. To exploit this potential, Israel should pursue policies directed at orderly management and investment in the field of AI. Without orderly management and sufficient investment, Israel is liable to descend into an inferior position compared to both friendly and even hostile countries. Moreover, the field has its challenges, for which Israel must prepare itself to reduce risks and to maintain and develop advantages. We should acknowledge the importance of not only operational issues but also of "soft" issues, such as ethical or legal questions, which require thought and deliberation so that the technology will have a positive effect as much as possible.

The conclusion makes a number of recommendations in key areas in which Israel should act to maintain and improve its national security through

AI: Organization; research and development; budgeting; safety; morality; law; standardization; knowledge sharing; international, diplomatic, military intelligence and cooperative aspects; human resources, education and training. The burning issues are those of national infrastructures and human resources.

These recommendations are based on research conducted on AI policy—the focus of the expert committee that advised this research—in addition to the work of the committee, its discussions, and its conclusions. Some recommendations, which relate to more than one field, are mentioned only once. Some issues require large budgets, while others require organizational attention and adjustments of the existing situation. Some can be implemented on low budgets, although the potential for impact is high. The recommended policies refer primarily to the relatively narrow "hard" aspects of national security, although AI also has existing and potential influences in other broader areas.

A delay in formulating and managing policies in the field could damage Israel's national security, especially as an aggressive arms race is taking place in the majority of advanced countries, which see AI as a power multiplier. In this context, by taking early action in the field, based on clear, research- and knowledge-based policies, Israel has a greater chance of maintaining its positive lead and perhaps even to expand it for its own benefit.

Organization

- Israel should formulate a national strategy for AI and create a body that will manage it at the national level.
- Israel should create a multi-year program for AI, like the one that exists in the cyber field, to analyze the field broadly and comprehensively, to lead national policy of resource allocation, and to make decisions regarding research and development, human resources, and other matters.
- Israel should create structural models in the security establishment in general, and in the IDF in particular, which will enable Israel to maintain the pace with the changing rate of technology and allow for more responsiveness and flexibility than exists today.
- Israel should build common work arrangements of the security community, the IDF, industry, and academia to make use of their advantages and make knowledge accessible within the organization of these communities.

- Israel should remove obstacles to promoting innovation and entrepreneurship in the government so that advanced technologies can be integrated and implemented in government activities in the security fields.

Research and Development

- Israel immediately should consider integrating AI into security technology in which Israel has a relative advantage (such as the UAV field), in order to produce a power multiplier.
- Israel should invest in comprehensive studies by the national security establishment and not rely solely on academic studies that often are only on a theoretical level and are insufficient or not tested in the areas required by the security establishment. Israel should standardize and develop the scope of the research and development required, as it does in other technological areas.
- Israel should prioritize research and development of AI in areas that can provide an enduring advantage and reduce key risks, rather than focusing on "niche applications."
- Israel should promote security developments based on existing AI technology (utilizing dual capability), to take advantage of the progress in the civilian sector and to encourage it.
- Israel should develop a national strategy focused on data that will improve access to data and its use by the various security agencies, while also ensuring its protection.
- The Hebrew language processing field should be developed, including applications such as NLP, speech-to-text, text-to-speech, and more. This is because the security establishment works in Hebrew, as do all of Israel's citizens. The use of Hebrew will help strengthen local industry in the context of AI.
- Investments in research and development in the human–machine field for the security establishment should be increased, 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 help people instead of those that replacing them, until the credibility and safety of

the technology is well established, in addition to the administrative and legal aspects.

- Defense and military intelligence communities should invest in the development of counter-AI capabilities, for defense and attack purposes.
- Israel should develop AI applications to improve the use of current and historical military intelligence material.
- The field of AI in the Israeli security establishment is based on sensor systems, unlike systems that rely on databases and the collection of data. Israel should consider dealing with problems whose basis of data is not sensory, especially for military intelligence needs.

Budgeting, Financing, and National Infrastructure

- Israel should create a national solution for infrastructure issues (hardware, cloud, internet connection) and should allocate an ongoing budget for the use of the security community, which unlike the civilian industry, is not allowed to use the commercial infrastructures, partly because of its use of classified information.
- Israel should formulate a goal-oriented budgeting model, with the help of the security community, which could make use of outputs.
- Israel should determine the areas in which it intends to invest at the national level and which areas do not conform to its size and capabilities, and about which it should cooperate with civilian entities, both Israeli and international (such decisions would probably be within the role of AI authority, whose establishment is being discussed).
- Israel should define the areas of research that will require financing from the government budget and are significant to Israel's national security and would not be considered otherwise.
- Israel should consider a combination of mechanisms to encourage investments in the areas of AI that have a positive effect on national security.
- The government should increase expenditure on AI in civilian areas that will accelerate the economy.

Human Resources—Education and Training

- In the various security organizations, it is recommended that personnel be managed at a system-wide level, including the definition of common roles, standards, training, transfer of personnel between organizations, as well as incentives and budgets to recruit and retain talented people, so that they are not lost to the civilian industry.
- The security establishment (and the security industry) should be incorporated into existing training programs in the field, in particular the academic ones, to train personnel so that they are not trained only on a theoretical level, and to set up special training, competitions, or other frameworks that will connect talented people in the field with the needs of the security establishment.
- The defense sector should provide non-technological training to personnel, including those at senior levels, to familiarize them with AI, its limitations, and its capabilities, so that they can be more involved and active in making decisions about AI.
- Israel should invest in science, technology, mathematics, and engineering, as well as in problem-solving skills in a connected environment and should focus on preparing students for a future in which AI is an influential factor in both military and civilian life.

Ethics, Legislation, Standardization, and Safety Procedures

- Israel should establish organizations that are designed to create standards for AI and supervise safety in its use.
- 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 also adopt them.
- 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.
- For legal, ethical, safety, and expendability purposes, Israel should determine which systems will retain mechanisms of human supervision and control.
- Israel should define the classification and standards of AI systems for purposes of integration, safety, and mutual discussion to enable easier

and more organized processes than those currently present, vis-à-vis industry, as well as for development and procurement processes, and implementation in general.

- Standards and processes in the export of AI systems, including security-related export licenses, need to be examined. 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.
- Israel should define a standard in the context of human–machine research: It needs to ask where the role of the person in the human–machine team should be and how the chosen policy in the contracting and procurement methods of each security organization and the government office should be implemented.

Knowledge Sharing

- 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.
- Israel should create a uniform standard for certain positions, such as "head of data science" in each of the relevant organizations and offices and a permanent forum that will facilitate knowledge sharing between the organizations at the various working levels.
- The various organizations should form knowledge-sharing mechanisms in the lower professional echelons, based on civilian models (as much as possible in relation to information security), which are currently being used by the civilian industry.

International, Diplomatic, Intelligence, and Cooperative Aspects

- Israel should monitor at a national level what occurs in the international system in terms of AI and data sciences—including conventions and standards—to maintain Israel's advantage.
- Israel should establish a comprehensive plan for measuring, assessing, and monitoring the capabilities of different players (civilian or national) in the field of AI, to prevent strategic surprises.

- Israel should act to strengthen joint research and other collaboration with other countries.
- Israel should cooperate with, and even lead, a coalition of nations in the field of AI, as it does in the fields of military intelligence, aerial defense, and others.
- Israel should integrate itself into, and even lead, international initiatives—to limit rogue elements from attaining achievements in the field of AI, whether security or civilian.
- Israel should examine which AI applications, if any, it should strive to limit (or whose limitation it should strive to prevent) through agreements and conventions.

Notes

[1] Chris Smith et. al., "The History of Artificial Intelligence" (Seattle: University of Washington, 2006), 4, https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf.

[2] Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica:RAND Corporation, 2018), 9.

[3] Geist and Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?*

[4] Geist and Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?*

[5] US Library of Congress, Congressional Research Service, *Artificial Intelligence and National Security*, by Kelley M. Sayler, R45178 ver. 5 (2019), 2, https://crsreports.congress.gov/product/pdf/R/R45178/5.

[6] Geist and Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?*, 6.

[7] Geist and Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?*

[8] Congressional Research Service, *Artificial Intelligence and National Security*.

[9] Congressional Research Service, *Artificial Intelligence and National Security*.

[10] William A. Carter et al., "A National Machine Intelligence Strategy for the United States," *Center for Strategic and International Studies* (March 2018), 14.

[11] John Launchbury, "A DARPA Perspective on Artificial Intelligence," TechnicaCuriosa, 2017, https://machinelearning.technicacuriosa.com/2017/03/19/a-darpa-perspective-on-artificial-intelligence.

[12] Launchbury, "A DARPA Perspective on Artificial Intelligence."

[13] Launchbury, "A DARPA Perspective on Artificial Intelligence."

[14] Launchbury, "A DARPA Perspective on Artificial Intelligence."

[15] Roey Tzezana, "Artificial Intelligence Tech Will Arrive in Three Waves," Futurism, March 28, 2017, https://futurism.com/artificial-intelligence-tech-will-arrive-in-three-waves.

[16] Scott Jones, "Third Wave AI: The Coming Revolution in Artificial Intelligence," Medium August 28, 2018, https://medium.com/@scott_jones/third-wave-ai-the-coming-revolution-in-artificial-intelligence-1ffd4784b79e.

[17] Oshrit Gal-El, "Listen: Google Duplex, Google's Smart Software that Knows How to Make Reservations by Telephone," *Globes,* May 9, 2018, [Hebrew], https://www.globes.co.il/news/article.aspx?did=100123526.

18 Congressional Research Service, *Artificial Intelligence and National Security*, 1.

19 Geist and Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?*, 9

20 Darrell M. West and John R. Allen, "How Artificial Intelligence Is Transforming the World," Brookings, April 24, 2018, https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/.

21 West and Allen, "How Artificial Intelligence Is Transforming the World."

22 Shubhendu S. Shukla and Vijay Jaiswal, "Applicability of Artificial Intelligence in Different Fields of Life," *International Journal of Scientific Engineering and Research* 1, no. 1 (September 2013): 28.

23 West and Allen, "How Artificial Intelligence Is Transforming the World."

24 Congressional Research Service, *Artificial Intelligence and National Security*, 1–2.

25 Congressional Research Service, *Artificial Intelligence and National Security*, 2

26 Paul Scharre and Michael Horowitz, *What Every Policymaker Needs to Know* (Washington, DC: Center For a New American Security, 2018), 4.

27 Congressional Research Service, *Artificial Intelligence and National Security*, 2.

28 Getz et. al., *Artificial Intelligence, Data Science, and Smart Robotics: First Report* (Haifa, 2018), 56.

29 Scharre and Horowitz, *What Every Policymaker Needs to Know*, 5

30 Bernard Marr, "What Is Deep Learning AI? A Simple Guide with 8 Practical Examples," *Forbes*, October 1, 2018, https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/#5cc02c558d4b.

31 Scharre and Horowitz, *What Every Policymaker Needs to Know*, 6.

32 Getz et. al., *Artificial Intelligence*, 56–57.

33 Dataman, "What Is Image Recognition?," Towards Data Science, November 8, 2018, https://towardsdatascience.com/module-6-image-recognition-for-insurance-claim-handling-part-i-a338d16c9de0.

34 Google Cloud, "Vision AI," https://cloud.google.com/vision.

35 Google Cloud, "Vision AI," https://cloud.google.com/vision.

36 Getz et. al., *Artificial Intelligence*, 63.

37 William D. Eggers, Matt Gracie, and Neha Malik, "Using AI to Unleash the Power of Unstructured Government Data: Applications and Examples of Natural Language Processing (NLP) Across Government," Deloitte Insights (2019), 3.

38 Eggers, Gracie, and Malik, "Using AI to Unleash the Power of Unstructured Government Data."

39 Getz et. al., *Artificial Intelligence*, 63.

40 Getz et. al., *Artificial Intelligence*, 63.

41 Kacper Kubara, "Artificial Intelligence Meets the Internet of Things," Towards Data Science, July 10, 2019, https://towardsdatascience.com/artificial-intelligence-meets-the-internet-of-things-a38a46210860.

42 Congressional Research Service, *Artificial Intelligence and National Security*, 2.

43 Congressional Research Service, *Artificial Intelligence and National Security*, 2.

44 Congressional Research Service, *Artificial Intelligence and National Security*, 2.

45 Samuel Gibbs, "Google's AI Is Being Used by US Military Drone Programme," *Guardian*, May 7, 2018, https://www.theguardian.com/technology/2018/mar/07/google-ai-us-department-of-defense-military-drone-project-maven-tensorflow.

46 Adam Bryant, "Target Recognition and Adaption in Contested Environments (TRACE)," DARPA, http://www.darpa.mil/program/trace.

47 Yoav Ziton and Itamar Eichner, "500 Thwarted Attacks in a Year: Netanyahu and the Head of the GSS Awarded a Prize for Groundbreaking Operations," *Ynet*, December 5, 2018 [Hebrew], https://www.ynet.co.il/articles/0,7340,L-5420118,00.html.

48 Nurit Cohen-Inger and Gal Kaminka, "And Now for the Forecast: The IDF on the Road to an Intelligent Army–A Road Map for the Adoption of Artificial Intelligence Technologies in the IDF," *Bein Haktavim*, no. 18 (2018), 9 [Hebrew].

49 Congressional Research Service, *Artificial Intelligence and National Security*, 9.

50 Nat Levy "Amazon's Newest Pillars? AI and Logistics Key to Tech Giant's Future, Study Says," GEEKWire, April 24, 2017, https://www.geekwire.com/2017/amazons-newest-pillars-ai-logistics-key-tech-giants-future-study-says/.

51 "Autonomous Weapon Systems—Q and A," International Committee of the Red Cross November 12, 2014, https://www.icrc.org/en/document/autonomous-weapon-systems-challenge-human-control-over-use-force.

52 Billy Perrigo, "A Global Arms Race for Killer Robots Is Transforming the Battlefield," *Time*, April 9, 2018, https://time.com/5230567/killer-robots/.

53 Paul Scharre, *Robotics on the Battlefield Part I: Range, Persistence and Daring* (Washington, DC: Center For a New American Security, May 2014), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_RoboticsOnTheBattlefield_Scharre.pdf?mtime=20160906081925.

54 Human Rights Watch, *Losing Humanity: The Case against Killer Robots* (New York: Human Rights Watch, 2012), 11, https://www.hrw.org/sites/default/files/reports/Losing%20Humanity%20Executive%20Summary.pdf.

55 Dan Gettinger and Arthur H. Michel, "Loitering Munitions in Focus," The Center for the Study of the Drone at Bard College (2017), https://dronecenter.bard.edu/files/2017/02/CSD-Loitering-Munitions.pdf.

56 Ingvild Bode and Hendrik Huelss, "Autonomous Weapons Systems and Changing Norms in International Relations," *Review of International Studies* 44, no. 3 (July 2018): 393–413, https://doi.org/10.1017/S0260210517000614.

57 Cohen-Inger and Kaminka, "And Now for the Forecast."

58 Tom Upchurch, "How China Could Beat the West in the Deadly Race for AI Weapons," *Wired,* August 8, 2018, https://www.wired.co.uk/article/artificial-intelligence-weapons-warfare-project-maven-google-china.

59 Elsa Kania, "Learning Without Fighting: New Developments in PLA Artificial Intelligence War-Gaming," *China Brief* 19, no. 7 (April 9, 2019), https://jamestown.org/

program/learning-without-fighting-new-developments-in-pla-artificial-intelligence-war-gaming.

60 Neta Gurvitz, “Alpha-Go Beat the World Champion of the Game Go—What Happens When the Computer Has Intuition?” *Haaretz,* March 30, 2016 [Hebrew], https://www.haaretz.co.il/magazine/.premium-1.2898680.

61 Congressional Research Service, *Artificial Intelligence and National Security*, 12.

62 Congressional Research Service, *Artificial Intelligence and National Security*, 12.

63 Launchbury, “A DARPA Perspective.”

64 Congressional Research Service, *Artificial Intelligence and National Security*, 10–11.

65 Marc Ph. Stoecklin, “DeepLocker: How AI Can Power a Stealthy New Breed of Malware,” Security Intelligence, August 8, 2018, https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/.

66 Nancy Jones-Bonbrest, “U.S. Army, Artificial Intelligence Improves Soldiers’ Electronic Warfare User Interface,” US Army, March 18, 2019, https://www.army.mil/article/218705/artificial_intelligence_improves_soldiers_electronic_warfare_user_interface.

67 Elihay Vidal, “Dr. Kira Radinsky Knows What Will Happen in the Future, and already Has Earned Millions from It,” *The Marker,* July 22, 2016, [Hebrew], https://www.themarker.com/markerweek/1.3014535.

68 Naveen Joshi, “How AI Can And Will Predict Disasters,” *Forbes*, March 15, 2019, https://www.forbes.com/sites/cognitiveworld/2019/03/15/how-ai-can-and-will-predict-disasters/#647259f85be2.

69 Anoushka Deshmukh, “How DOD Is Using AI to Speed Disaster Relief,” Defense Systems, July 10, 2019, https://defensesystems.com/articles/2019/07/10/ai-disaster-relief.aspx.

70 Getz et. al., *Artificial Intelligence,* 57–58.

71 Lynn Metcalf, David A. Askay, and Louis B. Rosenberg, “Keeping Humans in the Loop: Artificial Swarm Intelligence to Improve Business Decision Making,” *California Management Review* 61, no. 4 (2019): 84–109, https://doi.org/10.1177/0008125619862256.

72 Defense Advanced Research Projects Agency, “DARPA Seeks Proposals for Third OFFSET Swarm Sprint, Awards Contracts for Second,” October 12, 2018, https://www.darpa.mil/news-events/2018-10-12.

73 Jay Peters, “Watch DARPA Test Out a Swarm of Drones,” The Verge, August 9, 2019, https://www.theverge.com/2019/8/9/20799148/darpa-drones-robots-swarm-military-test.

74 Getz et. al, *Artificial Intelligence,* 63.

75 Mick Ryan, “Human–machine Teaming For Future Ground Forces,” CSBA, April 25, 2018, https://csbaonline.org/research/publications/human–machine-teaming-for-future-ground-forces.

76 Jeff Coleman, "Brain Computer Interface with Artificial Intelligence and Reinforcement Learning," Medium, May 4, 2018, https://medium.com/@askwhy/brain-computer-interface-with-artificial-intelligence-and-reinforcement-learning-9c94b0454209.

77 Alexandre Gonfalonieri, "A Beginner's Guide to Brain-Computer Interface and Convolutional Neural Networks," Medium, November 25, 2018, https://towardsdatascience.com/a-beginners-guide-to-brain-computer-interface-and-convolutional-neural-networks-9f35bd4af948.

78 Sarah Marsh, "Neurotechnology, Elon Musk and the Goal of Human Enhancement," *Guardian*, January 1, 2018, https://www.theguardian.com/technology/2018/jan/01/elon-musk-neurotechnology-human-enhancement-brain-computer-interfaces.

79 Coleman, "Brain Computer Interface."

80 Bernard Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#7356097a60ba.

81 Gil Press, "12 Big Data Definitions: What's Yours?," *Forbes*, September 3, 2014, https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#56a9281013ae.

82 Joshua Bleiberg and Darrell M. West, "Using Standards to Make Big Data Analytics That Work," Brookings, March 7, 2014, https://www.brookings.edu/blog/techtank/2014/03/07/using-standards-to-make-big-data-analytics-that-work/.

83 Carmel Shur, "What is a Super-Computer?," Davidson Institute, February 5, 2017, [Hebrew], https://davidson.weizmann.ac.il/online/askexpert/מהו-מחשב-על.

84 "The Next Wave of AI Won't Happen Without Supercomputing," *Cray* (blog), June 11, 2019.

85 Elsa B. Kania and John Costello, *Quantum Hegemony?: China's Ambitions and Challenge to U.S. Innovation Leadership* (Washington DC: Center for New American Security, 2018), 5, https://www.cnas.org/publications/reports/quantum-hegemony.

86 IBM, "What Is Quantum Computing?," 2020, https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/.

87 IBM, What Is Quantum Computing?"

88 Kania and Costello, "Quantum Hegemony?," 3–4.

89 Uri Berkowitz and Tal Shahaf, "The World is on the Verge of a Quantum Revolution, and Israel Must Enter the Race," *Globes*, July 20, 2018 [Hebrew], https://www.globes.co.il/news/article.aspx?did=1001246863.

90 Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145, (Washington DC: National Institute of Standards and Technology, 2011), 2, https://csrc.nist.gov/publications/detail/sp/800-145/final.

91 Amazon, "What Is Cloud Computing?," 2020, https://aws.amazon.com/what-is-cloud-computing/.

92 Mell and Grance, *The NIST Definition*, 2–3.

93 Yahya Mohamed Mao, "Combining Cloud Computing and Artificial Intelligence (AI)," Medium, April 23, 2018, https://medium.com/nworld-publications/combining-cloud-computing-and-artificial-intelligence-ai-9db02226c7e3.

94 Amy Nordrum, Kirsten Clark, and IEEE Spectrum Staff, "Everything You Need To Know About 5G," IEEE Spectrum, January 27, 2017, https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g.

95 US Library of Congress, Congressional Research Service, *Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress*, by Jill C. Gallagher and Michael E. Devine, R45485 (2019), https://fas.org/sgp/crs/misc/R45485.pdf.

96 Sarah Yost, "Brave New World: Everything Gets Smarter When 5G and AI Combine," Electronic Design, February 11, 2019, https://www.electronicdesign.com/industrial-automation/brave-new-world-everything-gets-smarter-when-5g-and-ai-combine.

97 Pei Wang, Kai Luiu, and Quinn Dougherty,"Conceptions of Artificial Intelligence and Singularity," *Information* 9, no. 4 (April 2018): 2, https://doi.org/10.3390/info9040079.

98 Luke Muehlhauser, "What Is AGI?," Machine Intelligence Research Institute, August 11, 2013, https://intelligence.org/2013/08/11/what-is-agi/.

99 Muehlhauser, "What Is AGI?"

100 M. L. Cummings et al., *Artificial Intelligence and International Affairs Disruption Anticipated* (London: Chatham House, 2018), iv, https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf.

101 Seth D. Baum, Ben Goertzel, and Ted G. Goertzel, "How Long until Human-Level AI? Results from an Expert Assessment," *Technological Forecasting and Social Change* 78, no. 1 (January 2011): 185–195, https://doi.org/10.1016/j.techfore.2010.09.006.

102 Baum, Goertzel, and Goertzel, "How Long until Human-Level AI?"

103 John E. Laird et al., "Claims and Challenges in Evaluating Human-Level Intelligent Systems," *Advances in Intelligent Systems Research*, Proceedings of the 2nd Conference on Artificial General Intelligence, no. 9 (June 2009), https://dx.doi.org/10.2991/agi.2009.17.

104 Vedran Dunjko and Hans J Briegel, "Machine Learning and Artificial Intelligence in the Quantum Domain: A Review of Recent Progress," *Reports on Progress in Physics* 81, no. 7 (July 2018), https://doi.org/10.1088/1361-6633/aab406.

105 William J. Dally et al., "Hardware-Enabled Artificial Intelligence," in *IEEE Symposium on VLSI Circuits* (Honolulu: IEEE, 2018), 3–6, https://doi.org/10.1109/VLSIC.2018.8502368.

106 Wim Naudé and Nicola Dimitri, *The Race for an Artificial General Intelligence: Implications for Public Policy*, IZA Discussion Paper no. 11737 (Bonn: IZA: Institute of Labor Economics, 2018), 2, https://www.iza.org/publications/dp/11737/

the-race-for-an-artificial-general-intelligence-implications-for-public-policy; Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (2018): 37–57, https://doi.org/10.15781/T2639KP49.

107 Stuart Armstrong, Nick Bostrom, and Carl Shulman, "Racing to the Precipice: A Model of Artificial Intelligence Development," *AI & Society* 31, no. 201–206 (May 2016): 1, https://doi.org/10.1007/s00146-015-0590-y.

108 Nick Bostrom, "Strategic Implications of Openness in AI Development," *Global Policy* 8, no. 2 (2017): 1–14, https://doi.org/10.1111/1758-5899.12403.

109 Martin Ford, *Rise of the Robots: Technology and the Threat of a Jobless Future* (New York: Basic Books, 2015).

110 James Johnson, "Artificial Intelligence and Future Warfare: Implications for International Security," *Defense and Security Analysis* 35, no. 2 (2019): 147–69, https://doi.org/10.1080/14751798.2019.1600800.

111 "'Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day," RT World News, September 1, 2017, https://www.rt.com/news/401731-ai-rule-world-putin/.

112 Ed Felten and Terah Lyons, "The Administration's Report on the Future of Artificial Intelligence," White House, October 12, 2016, https://obamawhitehouse.archives.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence.

113 White House, *The National Security Strategy of the United States of America* (December 2017), 20–21, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

114 Department of Defense, *Summary of 2018 National Defense Strategy of United States of America: Sharpening the American Military's Competitive Edge* (2018), 5, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

115 Department of Defense, *Summary of 2018 National Defense Strategy.*

116 "Artificial Intelligence for the American People," White House, accessed May 22, 2019, https://www.whitehouse.gov/ai/executive-order-ai/.

117 Congressional Research Service, *Artificial Intelligence and National Security*, 2.

118 "AI Policy—United States," Future of Life Institute, 2020, https://futureoflife.org/ai-policy-united-states/?cn-reloaded=1.

119 US Government Publishing Office, *A Budget for a Better America: Fiscal Year 2020* (Washington, DC: Government Publishing Office, 2019), 267–273.

120 Congressional Research Service, *Artificial Intelligence and National Security*, 5.

121 Guy Katz, "'The 'Innovation Race': A Paradigm Change in the Security Research and Development System," *Bein Haktavim* 18 (2018): 15–30 [Hebrew].

122 Congressional Research Service, *Artificial Intelligence and National Security*, 8.

123 Congressional Research Service, *Artificial Intelligence and National Security*, 17.

124 Congressional Research Service, *Artificial Intelligence and National Security*, 18.

125 Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times*, April 4, 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.

126 Liran Antebi, "We Are Not Far from the Day When Robots Have a Finger on the Trigger," *Haaretz*, August 24, 2017 [Hebrew], https://www.haaretz.co.il/misc/article-print-page/.premium-1.4385839.

127 The term ecosystem is borrowed from the field of biology and refers to a system that works in interaction, cooperation, and in mutual fertilization. In the technological context, it tends to focus on the bodies and organizations that comprise the technological landscape in the country: the academic sector, the private-civilian industry, the military, and the defense and government industry. It is customary to acknowledge the importance of productive cooperation between the parts of the ecosystem as essential for high quality and rapid technological development.

128 Graham Webster et al., "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," New America (blog), August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

129 Lindsey R. Sheppard et al., *Artificial Intelligence and National Security: The Importance of the AI Ecosystem* (Washington DC: Center for Strategic and International Studies, November 2018), 49, https://www.csis.org/analysis/artificial-intelligence-and-national-security-importance-ai-ecosystem.

130 Sheppard et al., *Artificial Intelligence and National Security*.

131 Congressional Research Service, *Artificial Intelligence and National Security*, 20; Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* (Washington DC: Center for a New American Security, February 2019), 15. https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

132 Amy K. Lehr, "Responding to the Xinjiang Surveillance State—and Its Likely Progeny," Center for Strategic and International Studies, November 13, 2018, https://www.csis.org/analysis/responding-xinjiang-surveillance-state-and-its-likely-progeny.

133 Matthew P. Goodman, "Predatory Economics and the China Challenge," *Global Economics Monthly* 6, no. 11 (November 2017), https://www.csis.org/analysis/predatory-economics-and-china-challenge.

134 Allen, *Understanding China's AI Strategy*; Sheppard et al., *Artificial Intelligence and National Security*, 49.

135 Congressional Research Service, *Artificial Intelligence and National Security*, 7.

136 Sheppard et al., *Artificial Intelligence and National Security*, 51.

137 Anshel Pfeffer, "Israel Will Sell Drones to Russia So that It Will Cancel a Deal With Iran," *Haaretz,* June 25, 2009 [Hebrew], https://www.haaretz.co.il/news/politics/1.1267820.

138 Samuel Bendett, "Putin Orders Up a National AI Strategy," Defense One, January 31, 2019, https://www.defenseone.com/technology/2019/01/putin-orders-national-ai-strategy/154555/.

139 "AI Policy—Russia," Future of Life Institute, February 2020, https://futureoflife.org/ai-policy-russia/.

140 Part of the assessments note that the target year is 2025.

141 Sheppard et al., *Artificial Intelligence and National Security*, 47–48.

142 Sheppard et al., *Artificial Intelligence and National Security*, 48.

143 Samuel Bendett, "In AI, Russia Is Hustling to Catch Up," Defense One, April 4, 2018, https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/.

144 Congressional Research Service, *Artificial Intelligence and National Security*, 24.

145 Sheppard et al., *Artificial Intelligence and National Security*, 48.

146 Sheppard et al., *Artificial Intelligence and National Security*, 23.

147 Sheppard et al., *Artificial Intelligence and National Security*, 48.

148 Bendett, "In AI, Russia Is Hustling to Catch Up."

149 US Library of Congress, Congressional Research Service, *Artificial Intelligence and National Security*, by Daniel S. Hoadley and Nathan J. Lucas, R45178 ver. 3 (2018), https://crsreports.congress.gov/product/pdf/R/R45178/3.

150 Aaron Bateman, "Russia's Quest to Lead the World in AI Is Doomed," Defense One, June 12, 2019, https://www.defenseone.com/ideas/2019/06/russias-quest-lead-world-ai-doomed/157663/.

151 Sheppard et al., *Artificial Intelligence and National Security*, 48.

152 Sheppard et al., *Artificial Intelligence and National Security*, 48.

153 Bendett, "In AI, Russia Is Hustling to Catch Up."

154 Bateman, "Russia's Quest."

155 European Commission, "Artificial Intelligence," July 20, 2020, https://ec.europa.eu/digital-single-market/en/artificial-intelligence#A-European-approach-to-Artificial-Intelligence.

156 European Commission, "EU Member States Sign up to Cooperate on Artificial Intelligence," April 10, 2018, https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence.

157 European Commission, *Artificial Intelligence for Europe* (April 25, 2018), 2–3, https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF.

158 European Commission, *Coordinated Plan on Artificial Intelligence* (December 7, 2018), 3, https://ec.europa.eu/knowledge4policy/publication/coordinated-plan-artificial-intelligence-com2018-795-final_en.

159 Fabian J. G. Westerheide, *The European AI Landscape* (2018), https://ec.europa.eu/digital-single-market/en/news/european-artificial-intelligence-landscape.

160 Frank Slijper, Alice Beck, and Daan Kayser, *State of AI*, *The Big Picture* (Ultrecht: Pax, 2019), 23–25, https://www.paxforpeace.nl/publications/all-publications/the-state-of-ai.

161 Sheppard et al., *Artificial Intelligence and National Security*.

162 Slijper, Beck, and Kayser, *State of AI.*

163 Sheppard et al., *Artificial Intelligence and National Security*.

164 Slijper, Beck, and Kayser, *State of AI*, 23–25.

165 "AI Policy—Germany," Future of Life Institute, 2019, https://futureoflife.org/ai-policy-germany/.

166 Sheppard et al., *Artificial Intelligence and National Security*, 52.

167 "AI Policy—United Kingdom," Future of Life Institute, 2019, https://futureoflife.org/ai-policy-united-kingdom/.

168 Slijper, Beck, and Kayser, *State of AI*, 19–21.

169 Slijper, Beck, and Kayser, *State of AI*, 19–21.

170 Cummings et al., *Artificial Intelligence and International Affairs*, iv.

171 Nate Soares, "Safety Engineering, Target Selection, and Alignment Theory," Future of Life Institute, January 2, 2016, https://futureoflife.org/2016/01/02/safety-engineering-target-selection-and-alignment-theory/.

172 Bostrom, "Strategic Implications of Openness in AI Development."

173 "Meeting 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, December 11, 2017, 1–6, CCW/MSPP/2017/8, https://undocs.org/pdf?symbol=en/CCW/MSP/2017/8.

174 Geist and Lohn, *How Might Affect the Risk of Nuclear War?*, 1–22.

175 West and Allen, "How Artificial Intelligence Is Transforming the World," 6–7.

176 John Allen and Amir Hussain, "On HyperWar," Fortuna's Corner, January 2, 2018, https://fortunascorner.com/2017/07/10/on-hyper-war-by-gen-ret-john-allenusmc-amir-hussain/.

177 Hans J. Morgenthau, *Politics among Nations:The Struggle for Power and Peace* vol. 1, 4th ed. (Tel Aviv, Yachdav, 1968), 155 [Hebrew].

178 Liran Antebi, "The Proliferation of Autonomous Weapon Systems: Effects on International Relations," in *National Security in a 'Fluid' Reality,* ed. Carmit Padan and Vera Michlin-Shapir, Memorandum no. 195 (Tel Aviv: INSS, 2010), https://www.inss.org.il/publication/national-security-in-a-liquid-world/.

179 Ryan Hass and Zach Balin, "US-China Relations in the Age of Artificial Intelligence," Brookings, January 10, 2019, https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/.

180 Randall Schweller, "Opposite but Compatible Nationalisms: A Neoclassical Realist Approach to the Future of US-China Relations," *Chinese Journal of International Politics* 11, no. 1 (Spring 2018): 23–48, https://doi.org/10.1093/cjip/poy003.

181 Andrew Berg, Edward F Buffie, and Luis-Felipe Zanna, "Robots, Growth, and Inequality," *Finance and Development* 53, no. 3 (September 2016): 10–13.

182 Ekkart Zimmermann, "Globalization and Terrorism," *European Journal of Political Economy* 27, no. S1 (December 2011): S152–S161, https://doi.org/10.1016/j.ejpoleco.2011.09.003.

183 see Zachary S. Davis, *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise* (Livermore, CA: Center for Global Security Research*,* 2019), 14–15, https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf; Joshua P. Meltzer, "The Impact of Artificial Intelligence on International Trade," Brookings, December 13, 2018, https://www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/; David G. Victor, "How Artificial Intelligence Will Affect the Future of Energy and Climate," Brookings, January 10, 2019, https://www.brookings.edu/research/how-artificial-intelligence-will-affect-the-future-of-energy-and-climate/.

184 Andrew Williams, "Defining Autonomy in Systems: Challenges and Solutions," in *Autonomous Systems: Issues for Defense Policymakers*, ed. Andrew P. Williams and Paul D. Scharre (Norfolk: Capability Engineering and Innovation Division, Headquarters Supreme Allied Commander Transformation, 2014), 33.

185 Liran Antebi, "The International Process to Limit Autonomous Weapon Systems: Significance for Israel," *Strategic Assessment* 21, no. 3 (November 2018): 84.

186 Antebi, "The International Process to Limit Autonomous Weapon Systems."

187 Markus Wagner, "The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems," *Vanderbilt Journal of Transnational Law* 47, no. 5 (December 2014): 1389–1392.

188 Wagner, "Dehumanization of International Humanitarian Law," 1393–1399.

189 Wagner, "Dehumanization of International Humanitarian Law," 1393–1399.

190 Wagner, "Dehumanization of International Humanitarian Law,"1399–1405.

191 Antebi, "The International Process," 85–86.

192 Antebi, "The International Process," 85–86.

193 Antebi, "The International Process," 90–91.

194 Cameron Russell, "A Case for Not Regulating the Development of Artificial Intelligence," Towards Data Science, April 2, 2019, https://towardsdatascience.com/a-case-for-not-regulating-the-development-of-artificial-intelligence-f3d23db2e8c.

195 Antebi, "The International Process," 90–91.

196 "Preparing for the Ethical Dilemmas of the AI Era," Proceedings (Washington DC: Brookings, September 14, 2018), 7, https://www.brookings.edu/wp-content/uploads/2018/09/gs_20180914_ethics_ai_transcript.pdf.

197 Neta Linzen and Uri Gabai, "2018–19 Innovation in Israel—A Snapshot" (Innovation Authority, Ministry of the Economy and Industry, 2018), 53 [Hebrew].

198 Nissim Chanya, "Changes in the Israel Security Development and Production System, and How Much It Has Adapted to the Present Era," *Bein Haktavim* 6 (2016): 39–88 [Hebrew].

199 Cohen-Inger and Kaminka, "And Now the Forecast."

200 Amir Mizroch, "In Israel, A Stand Out Year For Artificial Intelligence Technologies," *Forbes*, March 11, 2019, https://www.forbes.com/sites/startupnationcentral/2019/03/11/in-israel-a-stand-out-year-for-artificial-intelligence-technologies/#3ddd6d5230a8.

201 Cohen-Inger and Kaminka, "And Now for the Forecast."

202 Datanation, "A Record Year: Artificial Intelligence Startups Raised 2.25 Billion Dollars in 2018," *The Marker,* March 21, 2019 [Hebrew].

203 Getz et. al., *Artificial Intelligence*, 195–196.

204 Cohen-Inger and Kaminka, "And Now for the Forecast."

205 Liran Antebi, "Unmanned Aerial Vehicles in Asymetric Warfare: Maintaining the Advantage of the State Actor," in *The Quiet Decade: In the Aftermath of the Second Lebanon War, 2006–2016*, Memorandum no. 167, ed. Udi Dekel, Gabi Siboni, and Omer Einav (Tel Aviv: INSS, 2017), 83–94.

206 Liran Antebi, "Global Changes in the Proliferation of Armed UAVs: Risks, Challenges, and Opportunities Facing Israel," *Cyber, Intelligence and Security* 2, no. 3 (December 2018): 65–81.

207 Sheppard et al., "Artificial Intelligence," 50–51.

208 Antebi, "Unarmed Aircraft," 81.

209 Sheppard et al., "Artificial Intelligence," 50–51.

210 Pepper, "Israel Will Sell Drones."

211 Robert Knake, "What the US Should Learn from Israel's Silicon Valley," Defense One, December 19, 2016, https://www.defenseone.com/ideas/2016/12/what-us-should-learn-israels-silicon-valley/134013/.

212 Getz et. al., *Artificial Intelligence*, 20–21.

213 Orr Hirshauge, "The Security Industries Discovered the Fifth Combat Arena," *The Marker,* January 14, 2014 [Hebrew], https://www.themarker.com/technation/1.2216479.

214 Antebi, "Unmanned Aircraft," 81.

215 Lilach Baumer, "Despite Tech Prowess, Israel Ranks Low on Autonomous Vehicle Readiness," *Calcalist*, February 18, 2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3756559,00.html.

216 Gershon Cohen, *What's National about National Security?* (Tel Aviv: Ministry of Defense Publishing House 2014), 20.

217 Yisrael Tal, "On National Security," *Ma'arachot* no. 286 (February 1983), 3.

218 Samuel M. Malinda, "Sovereignty and Global Security," *Security Dialogue* 29, no. 3 (1998): 281–292.

219 Human Security Unit, United Nations Office for the Coordination of Humanitarian Affairs, *Human Security in Theory and Practice* (United Nations, 2009), https://www.undp.org/content/dam/turkey/docs/news-from-new-horizons/issue-41/UNDP-TR-HSHandbook_2009.pdf·

220 Udi Dekel and Omer Einav, *An Updated Israeli National Security Concept*, Special Memorandum (Tel Aviv: INSS, 2017), 7–8 [Hebrew].

221 Dekel and Einav, *An Updated Israeli National Security Concept*, 7.

222 Dan Meridor and Ron Eldadi, *Israel's Security Concept—the Report of the Committee to Formulate a Security Concept (Meridor Committee) and its Examination after a Decade*, Memorandum no. 182 (Tel Aviv: INSS, August 2018), 7 [Hebrew].

223 Meridor and Eldadi, *Israel's Security Concept*, 15.

224 Meridor and Eldadi, *Israel's Security Concept*, 23–28.

225 Meridor and Eldadi, *Israel's Security Concept*, 32–38.

226 Meridor and Eldadi, *Israel's Security Concept*, 40.

227 Meridor and Eldadi, *Israel's Security Concept*, 47.

228 State of Israel, Chief of Staff's Office, "The IDF Strategy," (April, 2018), 26–27.

229 State of Israel, Chief of Staff's Office"The IDF Strategy," 27.

230 Guy Feiglin, *The Innovation Race: Commercial and Military Technology in Means of Warfare—The Appropriate Point of Balance* (Haifa: Chaikin Chair for Geostrategy, University of Haifa, 2018).

231 Congressional Research Service, *Artificial Intelligence and National Security*.

232 Congressional Research Service, *Artificial Intelligence and National Security*.

233 Chris Middleton, "Google Using DeepMind AI to Reduce Energy Consumption by 30%," Internet of Business, 2018, https://tinyurl.com/y8jqgs78.

234 James Vincent, "Mark Zuckerberg Shares Pictures from Facebook's Cold, Cold Data Center," The Verge, September 29, 2016, https://www.theverge.com/2016/9/29/13103982/facebook-arctic-data-center-sweden-photos.

235 Congressional Research Service, *Artificial Intelligence and National Security*.

236 Sheppard et al., "Artificial Intelligence."

237 Congressional Research Service, *Artificial Intelligence and National Security*.

238 Congressional Research Service, *Artificial Intelligence and National Security*.

239 Congressional Research Service, *Artificial Intelligence and National Security*.

240 Congressional Research Service, *Artificial Intelligence and National Security*.

241 Congressional Research Service, *Artificial Intelligence and National Security*.

242 Congressional Research Service, *Artificial Intelligence and National Security*.

243 Congressional Research Service, *Artificial Intelligence and National Security*.

244 Congressional Research Service, *Artificial Intelligence and National Security*.

245 Congressional Research Service, *Artificial Intelligence and National Security*.

246 Congressional Research Service, *Artificial Intelligence and National Security*.

247 Congressional Research Service, *Artificial Intelligence and National Security*.

248 Mitre Corporation, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD* (January 2017), 32, https://fas.org/irp/agency/dod/jason/ai-dod.pdf.

249 Congressional Research Service, *Artificial Intelligence and National Security*.

250 Liran Antebi, "The International Process to Limit Autonomous Weapon Systems: Significance for Israel," *Strategic Assessment* 21, no. 3 (2018): 75–86.

251 Congressional Research Service, *Artificial Intelligence and National Security*; West and Allen, "How Artificial Intelligence Is Transforming the World."

252 Bernard Marr, "Artificial Intelligence Has a Problem with Bias, Here's How to Tackle it," *Forbes*, January 29, 2019, https://www.forbes.com/sites/bernardmarr/2019/01/29/3-steps-to-tackle-the-problem-of-bias-in-artificial-intelligence/#3f51bdb27a12.

253 Mesut Ozdag, "Adversarial Attacks and Defenses against Deep Neural Networks: A Survey," *Procedia Computer Science* 140 (2018): 152–161, https://doi.org/10.1016/j.procs.2018.10.315; Jacob Steinhardt, Pang Wei Koh, and Percy Liang, "Certified Defenses for Data Poisoning Attacks," *NIPS '17: Proceedings of the 31st International Conference on Neural Information Processing Systems* (December 2017): 3520–3532; Patrick Hall, "Proposals for Model Vulnerability and Security," O'Reilly Media, March 20, 2019, https://www.oreilly.com/ideas/proposals-for-model-vulnerability-and-security.

254 Mark Coeckelbergh, "Moral Appearances: Emotions, Robots, and Human Morality,"*Ethics and Information Technology* 12, no. 3 (2010): 235–241.

255 Andreas Matthias, "The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata," *Ethics and Information Technology* 6 (2004): 175.

256 Rebecca Crootof, "War Torts: Accountability for Autonomous Weapons," *University of Pennsylvania Law Review* 164, no. 6 (2016): 1347–1348.

257 Congressional Research Service, *Artificial Intelligence and National Security*.

258 Rayn Daws, "Report: UK leads AI developments in Europe, Iran in Middle-East," *AINEWS*, November 11, 2019, https://artificialintelligence-news.com/2019/11/11/report-uk-ai-developments-europe-iran-middle-east.

259 "Iran Ready to Coop. with Islamic States in AI Technology, says Rouhani," *MEHR News Agency*, December 18, 2019, https://en.mehrnews.com/news/153485/Iran-ready-to-coop-with-Islamic-states-in-AI-technology-says.

260 Congressional Research Service, *Artificial Intelligence and National Security*.

261 Congressional Research Service, *Artificial Intelligence and National Security*.

262 Michael C. Horowitz, et al., A*rtificial Intelligence and International Security* (Washington DC: Center for a New American Security, July 2018), 3–4, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018_Final.pdf?mtime=20180709122303.

263 Allen, "Understanding China's AI Strategy."

264 Horowitz, et al., *Artificial Intelligence and International Security*, 3–4.

265 Horowitz et al., *Artificial Intelligence and International Security*, 5–6.

266 Horowitz et al., *Artificial Intelligence and International Security*, 5–6.

267 John Villasenor, "Artificial Intelligence, Deep Fakes, and the Uncertain Future of Truth," Brookings, February 14, 2019, https://www.brookings.edu/blog/techtank/2019/02/14/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/.

268 This revolution will be the fourth industrial revolution, after the first began in the mid-18th century, with the introduction of automation into industrial processes; the second in the 19th century with the move to mass production processes; and the third in the second half of the 20th century, with the entry of computers.

269 Jaap Bloem et al., *The Fourth Industrial Revolution: Things to Tighten the Link Between IT and OT*, VINT Research Report 3 of 4 (Sogeti, 2014), 11–14, https://itblogsogeti.com/2014/12/17/the-fourth-industrial-revolution-vint-research-report-iii-download-sogeti/; World Economic Forum, *The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution* (January 2016), 5, http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.

270 John Hawksworth, "AI and Robots Could Create as Many Jobs as They Displace," World Economic Forum, September 18, 2018, https://www.weforum.org/agenda/2018/09/ai-and-robots-could-create-as-many-jobs-as-they-displace/.

271 Smadar Somekh and Khaled Kadry, *The Future of the Work World: A Review of Major Trends* (Jerusalem: Myers JDC Brookdale, August 2017), 120 [Hebrew].

272 Katja Grace et al., "Viewpoint: When Will AI Exceed Human Performance?" Evidence from AI Experts," *Journal of Artificial Intelligence Research* 62 (July 2018): 729, https://doi.org/10.1613/jair.1.11222.

273 Assaf Oni, "The Finnish Researcher who Swept the World with the Idea of Basic Income: 'They Also Thought that it Would Not Be Possible to Abolish Slavery,'" *Globes*, February 15, 2019 [Hebrew], https://www.globes.co.il/news/article.aspx?did=1001273333.

274 Nirit Cohen, "Should Robots Have to Pay Income Tax?" *Globes,* September 15, 2017 [Hebrew], https://www.globes.co.il/news/article.aspx?did=1001205097.

275 World Inequality Lab, *World Inequality Report 2018* (2017), 199–201.

276 Julia Bossman, "Top 9 Ethical Issues in Artificial Intelligence," World Economic Forum, October 21, 2016, https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/.

277 Yuval Noah Harari, *21 Lessons for the 21st Century* (London: Vintage, 2019).

278 Ian Shirr and Richard Neiva, "Department of Justice Kicks off Antitrust Review of Tech Giants," CNET, July 23, 2019, https://www.cnet.com/news/department-of-justice-kicks-off-antitrust-review-of-tech-giants/; Emily Stewart, "Poll: Two-Thirds of Americans Want to Break Up Companies like Amazon and Google," Vox, September 18, 2019, https://www.vox.com/policy-and-politics/2019/9/18/20870938/break-up-big-tech-google-facebook-amazon-poll.

INSS Memoranda, May 2019–Present

No. 207, January 2021, Liran Antebi, *Artificial Intelligence and National Security in Israel*.

No. 206, November 2020, Orna Mizrahi, Udi Dekel, and Yuval Bazak, The Next War in the North: *Scenarios Strategic Alternatives and Recommendations for the State of Israel.* [Hebrew].

No. 205, September 2020, Liran Antebi, *Artificial Intelligence and National Security in Israel* [Hebrew].

No. 204, September 2020, Kobi Michael and Michal Hatuel-Radoshitzky, *Seventy Years to UNRWA—Time for Structural and Functional Reforms.*

No. 203, September 2020, Ofir Winter, ed., *Existential Threat Scenarios to the State of Israel*.

No. 202, July 2020, Sasson Hadad, Tomer Fadlon, and Shmuel Even, eds., *Israel's Defense Industry and US Security Aid*.

No. 201, May 2020, Sasson Hadad, Tomer Fadlon, and Shmuel Even, eds., *Israel's Defense Industry and US Security Aid* [Hebrew].

No. 200, May 2020, Zipi Israeli, *The National Security Index: Trends in Israeli Public Opinion* [Hebrew].

No. 199, May 2020, Kobi Michael and Michal Hatuel-Radoshitzky, *Seventy Years to UNRWA—Time for Structural and Functional Reforms* [Hebrew].

No. 198, December 2019, Ofir Winter, ed., *Nothing is Forever: Existential Threats to the State of Israel* [Hebrew].

No. 197, October 2019, Yossi Kuperwasser and David Siman-Tov, eds., *The Cognitive Campaign: Strategic and Intelligence Perspectives*.

No. 196, September 2019, Gadi Eisenkot and Gabi Siboni, *Guidelines for Israel's National Security Strategy.*

No. 195, September 2019, Carmit Padan and Vera Michlin-Shapir, eds., *National Security in a "Liquid" World*.

No. 194, August 2019, Assaf Orion and Galia Lavi, eds., *Israel-China Relations: Opportunities and Challenges*.

No. 193, July 2019, Yoel Guzansky with Miriam Goldman and Elise Steinberg, *Between Resilience and Revolution: Regime Stability in the Gulf Monarchies.*

No. 192, July 2019, Gabi Siboni, *Guidelines for a National Protection Strategy* [Hebrew].

No. 191, May 2019, Yossi Kuperwasser and David Siman Tov, eds., *The Cognitive Campaign: Strategic and Intelligence Perspectives* [Hebrew].

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 have been perceived as uniquely human abilities. Experts estimate that AI will change our lives beyond recognition, when it takes control of a variety of familiar actions and enables a wide range of new capabilities and applications. This technology has already affected many areas, including national security. Many countries and organizations have begun to recognize that artificial intelligence is no longer a future or futuristic technology; rather it is now a fundamental need. Given the potential influence of AI and Israel's being a leader in this field, in 2019, the Institute for National Security Studies convened a team of experts to formulate a recommended policy for Israel in this field.

This memorandum serves as a guide to the core issues and terms related to AI. The memorandum presents the technology and its security applications; reviews the state of development and the use of technology in leading countries, and its current and future influences on the international arena, including the "arms race." The memorandum surveys and analyzes the situation in Israel, in addition to the many challenges of AI's development, implementation, and use in the field of security and policy. Finally, this memorandum makes policy recommendations regarding AI in the fields of research and development, budgeting and infrastructures, human resources, legislation, regulation, morality, and more.

This memorandum emphasizes that Israel should now 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. The issues presented here could have a crucial impact on Israel's future strength, including its economy and its ability to maintain and improve its national security.

Dr. Liran Antebi is a research fellow and manages the Advanced Technologies and National Security program at the Institute for National Security Studies. Her main research interests are technological forecasting and policy; the effects of technology on security; the impact of advanced technologies on the policy of countries, companies, and organizations; the intensity and future of war; military technology, such as drones, robots, and artificial intelligence, and the implications of its use. She served as a member of the International Panel for the Regulation of Autonomous Weapons systems. Dr. Antebi lectures at Ben-Gurion University, in the academic program of the Israeli Air Force flight school, and at the Interdisciplinary Center Herzliya (IDC) in the Honors Program of the School of Government. She also privately researches and advises various bodies in Israel and abroad, including security agencies, military units, commercial companies, and the UN.

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב