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.