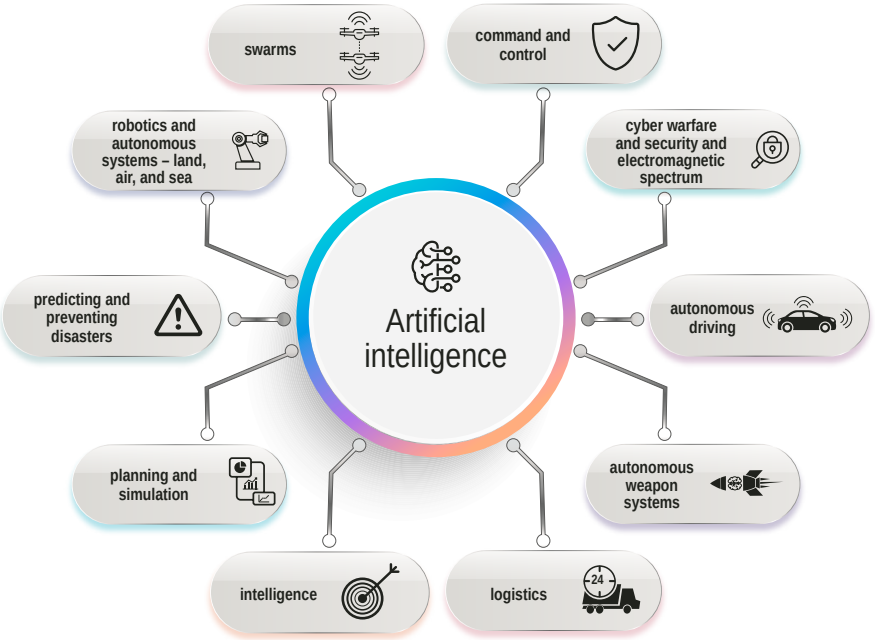
Chapter Three:
Widespread Security Applications

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



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.