

Report Part Title: Fields of Artificial Intelligence

Report Title: Artificial Intelligence and National Security in Israel

Report Author(s): Liran Antebi

Published by: Institute for National Security Studies (2021)

Stable URL: <https://www.jstor.org/stable/resrep30590.8>

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at <https://about.jstor.org/terms>



JSTOR

Institute for National Security Studies is collaborating with JSTOR to digitize, preserve and extend access to this content.

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.

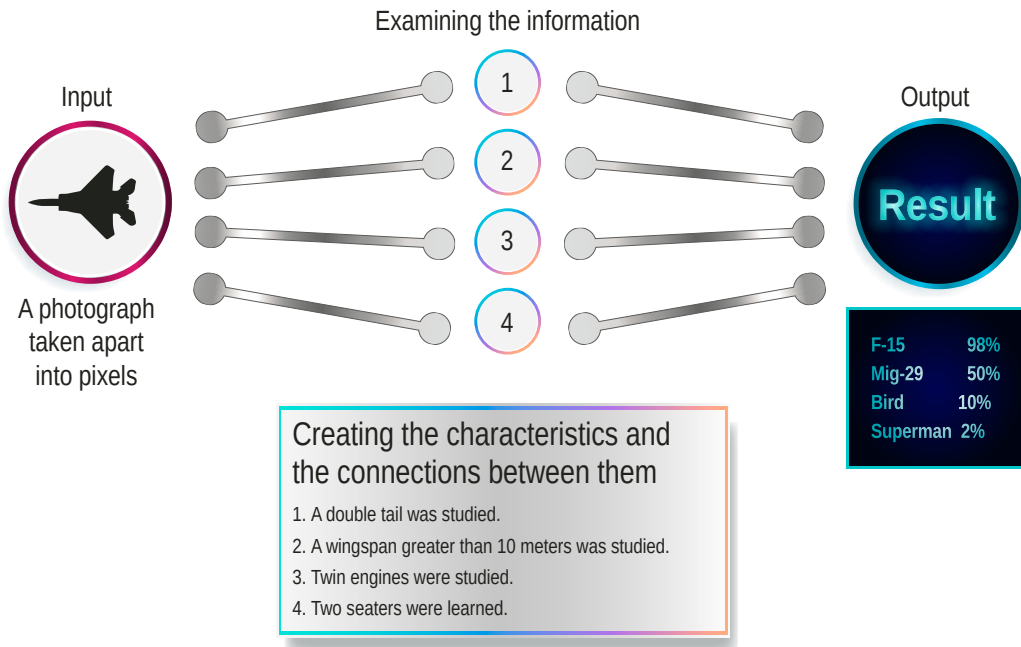
Deep Learning

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



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 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

