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.