Studies in Conflict & Terrorism

ISSN: 1057-610X (Print) 1521-0731 (Online) Journal homepage: https://www.tandfonline.com/loi/uter20

Artificial or Human: A New Era of Counterterrorism Intelligence?

Boaz Ganor

To cite this article: Boaz Ganor (2019): Artificial or Human: A New Era of Counterterrorism Intelligence?, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2019.1568815

To link to this article: https://doi.org/10.1080/1057610X.2019.1568815

Published online: 27 Feb 2019.

STUDIES IN CONFLICT & TERRORISM
https://doi.org/10.1080/1057610X.2019.1568815

Routledge
Taylor & Francis Group

Artificial or Human: A New Era of Counterterrorism Intelligence?

Boaz Ganor

Lauder School of Government, Diplomacy & Strategy and International Institute for Counter-Terrorism (ICT), IDC Herzliya, Israel

ABSTRACT

A new revolution has begun in counterterrorism—the Artificial Intelligence (AI) revolution. The AI revolution has had a significant impact on many areas of security and intelligence. The use of AI and big data in general, and in the field of intelligence and counterterrorism in particular, has led to intense debates between supporters of the continuation and expansion of the use of this technology and those who oppose it. The traditional delicate balance between effectiveness in the fight against terrorism and the liberal democratic values of society becomes even more crucial when counterterrorism engages in AI and big data technology.

ARTICLE HISTORY
Received 9 November 2018
Accepted 21 December 2018

Humankind is in the midst of a technological revolution, no less significant than the Industrial Revolution of the eighteenth and nineteenth centuries—the Artificial Intelligence (AI) revolution. Henry Kissinger, who examined the challenges of the modern world in light of the AI revolution, noted that this revolution and its implications will have no less impact than the historical effects of technological revolutions of the past.[1] Artificial intelligence, based on the advanced processing of big data via machine learning, is changing thought patterns and strategies in many different areas. The development of AI in combination with other technological advancements, in the field of robotics, for example, will probably lead to the elimination of various professions, such as professional drivers (in light of the development of the autonomous vehicle), accountants, pilots, and combat soldiers.

The technological revolution of AI has had a significant and immediate impact (which is certain to increase in the future) on many areas of security and intelligence, especially regarding the use of intelligence for the purpose of thwarting terrorism. The use of big data in counterterrorism began after the 11 September 2001 attacks, and has gained momentum in recent years as the result of a combination of several processes: the rate of technological development and progress, the vast experience that has been accumulated in the use of big data for civilian purposes, and the achievements that the use of big data has made in "preventive policing" and the prevention of future crime (especially with regards to credit card fraud).[2]

CONTACT Boaz Ganor ganor@idc.ac.il Lauder School of Government, Diplomacy & Strategy and International Institute for Counter-Terrorism (ICT), IDC Herzliya, Israel.

The fusion of AI, machine learning, and big data in counterterrorism operations has been implemented in many intelligence and operational spheres, such as: determining the structure of terrorist networks and organizations, identifying disputes and splits, recognizing incitement to terrorism online, locating high value targets, and so on. This article focuses on the use of AI, machine learning, and big data for the purposes of thwarting terrorist attacks in general and "lone wolf" attacks in particular. The article uses an Israeli case study in order to analyze the challenges and dilemmas that derive from the use of AI and big data in the prevention of terrorist attacks. The reason is that Israel have been challenged with more "lone wolf" attacks in recent years than any other country and as such have developed unique AI and big data capabilities as described in the article. The Israeli case study can therefore serve as an analytical model to examine its drawbacks and benefits, which could later be applied to other countries.

The Use of AI in Counterterrorism: Pros and Cons

The use of AI and big data in general, and in the fields of intelligence and counterterrorism in particular, has led to intense debates between supporters of the continuation and expansion of the use of this technology and those who oppose it.

Supporters of the use of AI and big data in counterterrorism in general and in prevention of "lone wolf" attacks in particular argue that its effectiveness in this field has been long proven and that many security, police, and intelligence agencies around the world have employed it and achieved much success. These supporters emphasize that today almost everyone has a digital footprint that can be tracked and processed, and therefore a lot of data can be gleaned, including on terrorists, through their use of cell phones, computer systems, applications, social networks, e-mail correspondence, digital cameras, automotive computers, smart watches, and many other technological means. Security agencies in many Western countries mine this data, store it in big data databases, and process it using machine learning and AI. For example, the U.S. military uses big data to detect terrorist movement through the use of drones in combination with other information. Based on this data, the army can identify where terrorists are and predict where they will be in the future.[3] Another example can be seen in the use of the information that exists on social networks. Some have estimated that terrorists and their supporters tweet tens of thousands of times a day—a large number that allows for the processing of big data using AI. The Computing Research Institute in Qatar analyzed more than three million tweets over a three-month period and was able to detect sources of support for the Islamic State of Iraq and Syria (ISIS). The scientists created an algorithm that was able to identify tweeters as opponents or supporters of ISIS with 87 percent accuracy and which could even predict who may be likely to join ISIS at a later stage.[4] According to John Wright, assistant chief constable in the British police, the United Kingdom has been using data retrieval systems for years that combine both open and secure intelligence databases. This is done in cooperation with all relevant security and intelligence agencies and with assistance from parallel international bodies. Wright explained that the data analysis model is based on the connections between Person, Object, Location, and Event, in which each entity is registered in the model

once, but can be linked to other entities, building up a complete profile and network of associations of the monitored subjects.[5]

The following scenario, presented in the Harvard University course "Technology and Operations Management," helps us understand how data are broken down and processed. The scenario describes the capability of the "Palantir" system, used by almost all security agencies in the United States: A foreign national named Mike Fikri purchased a one-way plane ticket from Cairo to Miami, where he rented a condo. Over the previous few weeks, he had made a number of large withdrawals from a Russian bank account and placed repeated calls to Syria. Recently, he rented a truck, drove to Orlando, and visited Disney World by himself. He spent his day taking pictures of crowded plazas and gated areas.

The day Fikri drove to Orlando, he was stopped by a police officer and given a speeding ticket, which triggered an alert in the Central Intelligence Agency's Palantir system. An analyst checked Fikri's name and came up with a wealth of information pulled from every database at the government's disposal: fingerprints and DNA samples for Fikri gathered in Cairo; a video of him withdrawing money from an Auntomated Teller Machine in Miami; photographs of his rental truck's license plate taken by cameras at a tollbooth; telephone records; and a map pinpointing all of his recent movements across the globe."[6] Advocates of AI, machine learning, and big data for the purpose of thwarting terrorism claim that when data processing and synthesis systems (such as Palantir) use AI and are connected to huge databases, the process of identifying those suspected of terrorist activity becomes faster, more efficient, sophisticated, and accurate.

The arguments against the use of AI and big data can be categorized into three types: *generic arguments* expressing concern about the growing use of AI and big data and the implications of these processes on human society as a whole; *utilitarian arguments* that claim that it is impossible to use AI and big data effectively in the prevention of terrorism; and *ethical arguments* that maintain that the possible damage that might be inflicted on innocent civilians due to the use of AI and big data in the field of counterterrorism should rule out the use of this technology.

The first type of argument, the generic, was expressed in an article by Henry Kissinger entitled "How the Enlightenment Ends?" In this article, Kissinger conveyed deep concern about the possible implications of the growth of AI technology in general and of machine learning and big data in particular. He wrote that in the era of big data, the world is becoming dependent on machines informed by data and algorithms rather than by philosophical and ethical norms. Truth is becoming relative and information is threatening to overwhelm wisdom. People become data and data reigns. Kissinger emphasized three concerns in particular that he sees as arising from the development of AI and big data.

The first is the fear that AI will achieve results that its programmers did not intend. In the course of processing big data and machine learning, strategic decisions about the future are sometimes made based in part on information entered as code into the system, and in part based on information collected by the system itself. In this context, Kissinger asked: to what extent can AI be made to understand the context of its instructions and not only the orders themselves? His second concern stems from the fact that

through AI, the computer learns, like humans, through trial and error, only it does so much faster and without any value judgment. Given this, Kissinger claimed that it is not possible, as some programmers have suggested, to plant some sort of software malfunction that would require ethical or logical outcomes and which would contradict the mathematical logic of the algorithms. Kissinger's third concern is that AI will be able to optimize situations in a way that may differ from the way a human would view optimization. The system will not be able to explain, in a way that human beings would understand, why and how it determined that its process was optimal. The question that arises from this is what will happen to human consciousness when people are no longer able to interpret the world in which they live in terms that mean something to them?[7]

A clear expression of the second type of opposition against the use of AI and big data, the utilitarian argument, can be found in the literature analysis published by Timme Bisgaard Munk in 2017. In his article, Munk examined the question of whether terrorist attacks can be forecast by predictive analytics. His conclusion was that this technology raises so many technical and theoretical issues that the attempt to use it for the purpose of predicting terrorism is ineffective, risky, and inappropriate. Munk determined that for every single terrorist that the algorithm finds, it could mistakenly mark 100,000 innocent people. In his analysis of the existing literature, Munk brought up among others the following points:

- Terrorism is not a regularly occurring event; its frequency is low and it is surrounded by other data that produce a lot of noise.
- The rate of terrorist attacks is low and each case may be unique (e.g., suicide bombings). This can lead to errors resulting from a small database and to the risk of overgeneralization.
- There are no clear-cut characteristics that define what should be considered an attempted terrorist attack, and failed attempts are usually kept secret.
- There is no agreed-on profile as to who is a terrorist. There is no profile that applies to all organizations, and there is indeed not even a profile with a high correlation to a specific terrorist organization.
- There is no certainty as to whether and when a person with extremist views will decide to use violent action. The differences between a potential terrorist and a real terrorist is not clear, so any classification algorithms are liable to lead to the inclusion of non-dangerous suspects and the ignoring of those who actually pose a threat.
- Terrorism is a dynamic phenomenon that is constantly undergoing a process of evolution. Therefore, categories that are relevant to examining terrorism today may change rapidly and become irrelevant and ineffective in the future.[8]

In the third group of those who argue against the use of big data and AI are those who oppose the use of these technologies in the field of counterterrorism due to the moral and ethical issues that arise from it. They claim that this technology severely violates the rights of the individual, principally the citizen's right to privacy, freedom of speech, and expression. When the government can define certain statements as constituting illegal and dangerous incitement, and when it has the ability to monitor all statements made by all citizens on social networks and perhaps even in their personal correspondence via e-mail, as well as their daily conduct as expressed in various databases, it should be taken into account that the government may misuse this information and exploit it for the purpose of neutralizing and possibly even physically harming

dissenters and opponents of the regime. According to supporters of this argument, the use of AI and big data technology damages the essence of the democratic regime and, whether consciously or not, transforms the regime into a "digital authoritarian state." In this type of regime, governments will supervise the discourse and behavior of citizens through the use of big data:

> authoritarian regimes will have no compunction about combining such data with information from tax returns, medical records, criminal records, sexual-health clinics, bank statements, genetic screenings, physical information (such as location, biometrics, and CCTV [closed-circuit television] monitoring using facial recognition software), and information gleaned from family and friends. […] People will know that the omnipresent monitoring of their physical and digital activities will be used to predict undesired behavior. […] In order to prevent the system from making negative predictions, many people will begin to mimic the behaviors of a "responsible" member of society.[9]

Moreover, even when security officials acting on behalf of the government and politicians have no malicious intent, the margin of error inherent in this technology is liable to undermine the rights of suspects to fair investigation and trial, cause them irreparable damage, and even endanger their lives. Thus, according to detractors of this practice, just as society saw fit to limit the rights of law enforcement and security bodies to carry out surveillance and wiretapping (either with or without technological means) and to demand the legal authorization and supervision of these measures, it should apply the same logic to the use of AI and big data, treating this technology as a means of mass surveillance and tapping.

Using AI to Counter Lone Wolves Terrorism

In his article "The Journey Towards Clarifying the Perception and Implementation of Intelligence and Operational Superiority in the Digital Era," Col. Y. analyzed the big data revolution in the field of intelligence, stating that the goal of this revolution is to "apply the inherent potential of the digital age to the current systemic challenges facing intelligence. At its center lies the understanding that the surge of information and the possibility of knowing everything about everyone allow for a modernized intelligence and operational response."[10] According to Col. Y., this revolution in the world of intelligence and counterterrorism stems not only from the rapid development of the technology and the creation of the opportunity to integrate it into the world of intelligence, but first and foremost from the urgent need to fill new intelligence gaps in light of the development of new security phenomena, such as lone wolf attacks (which he dubs "inspiration terrorism"). Addressing this phenomenon, Col. Y. said that: "Traditional intelligence was facing a hopeless situation, in which the potential terrorist (who sometimes did not even know himself one day prior to the attack that he was about to become a terrorist) got up one morning and decided to take a weapon in the form of the family vehicle or a kitchen knife and carry out an attack. How can one issue a warning ahead of such an attack? What can be defined as the right place to search for a response? Who can be prioritized as an EEI (Essential Element of Information) for monitoring? The sense of crisis intensified when we felt that time was passing and the irrelevance of the intelligence agencies was continuing, until we realized that the superiority of intelligence was being challenged. We understood that in the face of inspiration

terrorism carried out by individual attackers, the manner in which intelligence had been operating over the past few decades was not sufficient."[11] M. from the Israeli Security Agency (Shin Bet) explained the change as follows: "If in the past intelligence bodies dealt with adversaries who operated as organizations, be they states or organized terrorist and criminal organizations, over the past few years much of the intelligence agencies' attention has been focused on nonhierarchical adversarial networks who create connections that are not based on pre-set organizational structures, and who encourage activity by means of inspiration and dissemination rather than by means of guidance and control. This is a "flat world" of adversaries in which we are dealing with individuals who constitute a threat and who act independently. These changes in the nature of the adversary require the intelligence agencies to change their fundamental understandings and, rather than search for the enemy's model for action, try to pinpoint other types of markers. These markers can include changes in behavior or appearance, an increase or decrease in activity levels, the making of new connections and network and more. Intelligence bodies are being forced to change their conceptions of how to gather information and to amass very large amounts of data while putting in place the relevant sensors to collect and use this data, as well as to change the type of questions they ask about the information that is collected."[12]

Indeed, traditional intelligence—namely human intelligence (HUMINT) and communication intelligence (COMINT)—faced difficulties in issuing warnings about lone wolf attacks, mainly because these intelligence methods attempt to intercept significant conversations between two or more people who share among themselves the secret of their attack plans, whereas lone wolves do not conduct such conversations. In these types of terrorist attacks, the decision to carry out the attack usually begins and ends within one person's sick mind—the lone wolf himself. Moreover, while intelligence may be able to detect various stages of preparation for terrorist traditional attacks (the purchase of weapons, the preparation of explosive devices, training for the mission, etc.), lone wolf attacks do not require long preparations that would set off an intelligence alert. There is no need to purchase weapons, train, or develop any special capabilities. On the other hand, a large number of lone wolves have a social media presence that they use prior to the attack in order to publicize their reasons for carrying out the attack, justify the attack both to themselves and to others, and mainly to be recorded in the pages of history and gain honor and prestige among their peers. This is in contrast to members of terrorist organizations who are sent to carry out attacks and are instructed to maintain information security and refrain from publicizing their intentions; they generally have no need to announce anything prior to the attack because after its execution, whether they be killed during the attack or arrested, the terrorist organization that sent them will broadcast their messages either through letters or recorded videos that they prepared ahead of time and through which they will be remembered and honored.

The intelligence gap in lone wolf attacks created the need to develop new intelligence disciplines and served as the catalyst for the implementation of the big data revolution in the field of intelligence. This revolution is indeed inextricably linked to the development of discourse on social networks and to the harnessing of accumulated information on this and other digital mediums for intelligence purposes. According to M. from the Shin Bet, "A country's residents use devices that are connected to the Internet and that produce

digital footprints, such as smart TVs, smart watches, fitness bracelets, smart cars, digital and biometric ID tags, and more… [T]hey use smartphones and almost all of them have e-mail accounts and active profiles on various social networks."[13] Lt. Col. T. added that "people's willingness to provide a huge amount of information about themselves through social networks and smartphone applications enables the gathering of information in a way that was not possible in the past, and this includes people who are trying to maintain secrecy. Another group of opportunities stems from the availability of commercial technologies for intelligence use."[14] Cambridge Analytica, for example, claimed that they had access to about 5,000 data points on every American voter.[15] Lt. Col. T. noted in this context the development of the capability of processing large banks of images, audio, and research of huge databases. He added, however, that while the logic of commercial companies in the analysis and processing of data from social networks is aimed toward finding broad common denominators and deriving from them the behavior of the masses, intelligence also aims to "find the unusual and the unique."[16]

The use of big data for intelligence purposes indeed constitutes a new discipline of intelligence that changes every stage of intelligence work from collection, to processing, to formulating the intelligence picture, and translating the information into operational action. Regarding intelligence gathering, those engaged in collection make use of enormous databases, some of them openly available and others not, to gather information on a particular area (a state, a region or smaller area), a specific population, concrete activity, or a particular organization. These data are processed using various algorithms in order to produce a response to the questions that were posed at the outset of the process. These questions may be related to alerts of attacks, a terrorist's location, changes in the activity of an organization or operative, statements on social media, and more. Col. Y. compared the process of question-posing at the outset of traditional intelligence work to working with big data as follows: "According to the traditional approach, for any good question, relevant accessibility can be created in order to expose the adversary's secrets. If it is a question for which no information can be provided, the adversary's logic and thoughts can be defined through a deep understanding and analysis of the situation. In the era characterized by an inundation of information, one must assume that there is no question whose answer cannot be found in data. The trick is to know how to ask the right question from the data, to formulate questions that can deal with the flood of information, and to know that when we do not get the answer, we must assume that we have asked the wrong question."[17] Shin Bet agent M. also emphasized the importance of the question when using big data for intelligence purposes. "In the world of intelligence, the key to creating relevant research using the methods and tools of big data is being aware of the possibility of asking new questions. It must be understood that data not only produces quantitative differences that enable us to answer old questions using new tools, but actually creates a new reality in which totally new questions can be asked. The response to the questions is given by an intelligence agent using a much more sophisticated and complete picture of the enemy and of the environment in which he operates."[18] Lt. Col. T. added that "intelligence questions in the era of big data cannot be answered in the same sequential manner as they were in the past."[19]

On the face of it, intelligence based on big data may provide a response both to focused questions in the field of tactical-operative intelligence as well as in the area of

basic-strategic intelligence. Ben Tzur maintains that in the era of social networks, one can "focus on the individual and obtain a large amount of relevant intelligence about him, ranging from operational intelligence to tactical intelligence to strategic intelligence." In his view, tactical information is likely to include "an outline of a person's day-to-day life (his routine, movements, the places he visits), his occupation, his opinions and beliefs, the people that surround him (family, personal friends, colleagues), his professional activity (commercial/research/other), and all this along with a variety of factors that are relevant to the EEI, without requiring any clandestine intelligence activity."[20] Basic intelligence—the structure of the terrorist organizations, their system of command and control, the nature of their deployment, and more—can be gleaned through a combination of big data systems and the social network analysis (SNA) approach that examines the network and uses algorithms to identify its centers of gravity. In his article, "Network Intelligence Analysis in the Age of Big Data," Major A. explained that in the past, "in the absence of the conception or capability of big data, the main focus of research was link analysis, specific studies of anchors and the connections around them."[21] The SNA approach, on the other hand, examines the network as broadly as possible, and through algorithms and data analysis maps the communities, finds the key actors within them, and pinpoints the organizational centers of gravity. Major A. maintains that through this process, the following questions can be answered: Who are the dominant players in real time for the purposes of targeting or surveillance (without requiring any prior knowledge)? What new, unfamiliar people of interest have suddenly emerged from the woodwork? How does the organization actually function (not necessarily according to the official hierarchical structure, but according to network interaction)? What are the enemy's methods of action?[22]

What then can be learned from big data about terrorism? The use of big data technology in the field of counterterrorism is likely to provide responses to both basic intelligence and tactical intelligence questions referring simultaneously to the intentions and the capabilities of the terrorists. But with regard to the use of big data in issues related to basic intelligence, the technology may be relevant in analyzing and understanding the structure, deployment, goals, and modus operandi of institutionalized terrorist organizations, and sometimes even those of independent networks who have at least a defined command and control system and division of labor. Naturally big data intelligence will be much less relevant for the analysis and understanding of the organization's ideology, and perhaps even for the purpose of analyzing its motivations, cost–benefit considerations, and interests.

One of the central and unique contributions of big data technology in the field of counterterrorism lies in the field of tactical intelligence, and, as mentioned above, mainly in issuing warnings ahead of attacks by lone wolves and independent networks. This technology can also be used to collect operational intelligence for the purpose of offensive action against established terrorist networks and organizations and to thwart lone wolf attacks. At times, big data technology may also be used to supplement the intelligence picture in a way that will enable the implementation of campaigns and psychological warfare against terrorist organizations and large independent networks.

Major A. explained the difference between traditional intelligence and network intelligence based on big data saying that in traditional analyses, the intelligence officer assumes a certain scenario and then searches for it in the data, whereas the network

analysis enables the opposite process: arranging the data as a network and understanding the system without the need for basic assumptions. This way, it becomes possible to understand complex systems, garner new insights, and confirm or refute the intelligence picture without the need to rely on intuition.[23] According to Y., the basic ontology (contextual system) in security and intelligence deals with the system of ties between a person and a certain place. The entities that the systems deal with are people and places that maintain a system of connections between them. "In targeted killings, for example, first the most accurate point is identified, followed by who is also present at that point (are there civilians there? Who else is hiding there?)" Similarly, says Col. Y., in thwarting terrorism, the starting point is the person carrying out the attack. The ontology in a big data system embodies various levels and branches of connections between the different entities (objects, people, places, areas of occupation, etc.).[24]

AI and the use of big data therefore completely alter the nature of the intelligence officer's work. In the past, an experienced and effective intelligence officer was able to identify disturbing trends on the basis of the intelligence presented to him, experience he accumulated over the years, and the content of what he learned during his training. "Gut feelings" combined with the intelligence officer's creativity and wisdom were what often translated intelligence information into operational information or an alert. AI and big data do not make the work of the intelligence officer redundant, but rather, appear to make this work significantly more efficient in a way that a human being could never do alone, and often cannot even understand. In traditional intelligence work, the intelligence officer relied on the cross-referencing of several intelligence sources that together put the pieces of the intelligence puzzle together. In the age of big data, there are many sources of information, often amounting to millions of data points. Col. Y. accurately described the change in intelligence work in the era of big data by saying that "in the conception of intelligence in the information age, superiority does not stem from one piece of information or another, but rather from the wealth of information available and the ability to ask what is of interest to us. When the information is truly infinite, clearly there will be no attempt to try to read all of it … the answers already exist within the information, you just have to know how to wade through it in the most optimal way and to ask the things that interest the intelligence officer…"[25] The millions of items in big data databases usually seem not to have relevance to the intelligence issue being investigated, but their integration may bring about the result and response required. The role of the intelligence officer in these cases focuses on asking the relevant questions, helping to formulate the appropriate algorithms, and translating the results of the AI work into operational intelligence and action in an effective manner. Lt. Col. T. added that the skills required by the new intelligence officer are a combination of professional intelligence knowledge, mathematical and statistical knowledge, and an understanding of programming.[26]

Dilemmas in Using AI in Countering Terrorism

The application of big data technology to the field of intelligence in general, and to counterterrorism in particular, neutralizes some of the traditional dilemmas in HUMINT involved in operating people.[27] However, other ethical dilemmas, including

those involving a clash between liberal values and the effectiveness of the fight against terrorism (such as the invasion of the privacy not only of suspects but the general public) change their form and sometimes even intensify with the intelligence work done through the use of big data. Kissinger, who as mentioned raised questions and concerns about the use of AI and big data in all spheres of life, stressed at the end of his article that these concerns only increase when governments use AI for security and intelligence purposes.[28] Indeed, Israeli intelligence experts also point to the ethical and moral dilemmas that may stem from the reliance on AI and big data in intelligence work.

For example, Lt. Col. T explained that "effective work by intelligence agencies enables and requires the use of big data to breach privacy on a large scale. Moreover, because intelligence agencies influence military action, more so than in cases in which the decision on military action is made entirely by humans, an action based on a machine—whether the machine is deciding, making recommendations, or providing information relevant to the decision—requires a high level of awareness of the action's ethical aspects … "[29] In intelligence work in general, and in dealing with terrorism in particular, the need to preserve liberal values, individual rights, the right to privacy, freedom of speech and protest, and more, in many cases conflicts with the need to protect human life by preventing terrorism. This "democratic dilemma" that reflects the clash between liberal values and the effectiveness of the struggle against terrorism is becoming increasingly intense as it is accompanied by the natural tendency of decision makers and security and intelligence officials to compromise on liberal values and human rights in order to protect human lives—the future victims of the next terrorist attack.[30] These potential victims may be avoided through the use of certain intelligence products, including AI and big data. In the case of big data, human rights violations are abstract and embedded in large numbers in vast databases of information, while the danger to human life resulting from terrorist attacks is tangible and concrete. These moral dilemmas become even more acute when scientists and programmers are unable to explain the guiding principles, work processes, and decisions of AI, which are made via machine learning and the use of big data. This is due to the fact that in order to optimize their work process, these systems are likely to change the guidelines that they were given. In other words, in some cases, as a result of the use of big data and machine learning, it may be possible to catch a terrorist prior to his carrying out an attack, but it is not possible to explain how they got to him.

In an interview given by Yoelle Maarek, vice president of Research at Amazon, titled "The Big Data Revolution from the Perspective of Mega-Organizations," she addressed concerns about the ethical aspects of decisions based on big data (mainly through sophisticated algorithms of deep learning). Dr. Maarek explained that in these cases, "It is very difficult to understand the machine's actions and explain them. The algorithm becomes a kind of 'black box' and we have to rely on it to do its job well." She added, "There has recently been much public interest in the dangers of artificial intelligence, but AI is dangerous only when we are employing stupid algorithms and stupid scientists. I believe in a careful approach of meticulously examining the algorithm and understanding why we get results of one kind or another. … It is not responsible for the scientist to say that the reason he got certain results is because 'that is what the machine decided.' Each step should be monitored so that the analysts can verify the

results. Of course, this is even more important in the case of security and intelligence agencies that use algorithms to make life and death decisions."[31]

While Dr. Maarek believes that the criterion for responsible work by scientists and security officials is that they can explain the results of AI work, in many cases, according to some Israeli intelligence researchers, the situation on the ground is completely different, and they are not, in fact, able to explain the results of big data analyses. M. from the Shin Bet presented a position opposite to that of Dr. Maarek, saying that, "In a world of vast data, there is no point and no need to try to investigate and characterize the activity model of the research object, but rather to use data-based forecasting using algorithms that identify correlations, and not necessarily dependencies. In other words, even if we cannot explain the activity model of the object under examination, and even if we cannot prove that a certain phenomenon stems from it, it is sufficient that the algorithm finds a correlation between the two phenomena for us to use this connection effectively."[32] Major A. added, "A network analysis allows us to attain insights that are not even understood by the object of the research itself."[33] This approach is consistent with the argument that analyses of big data databases may be of great help in responding to the questions: Who? What? When? And where? However, it is difficult to derive from these analyses answers to questions aimed at finding reasons (Why?).[34]

The moral and ethical risks involved in using big data can be illustrated using the following examples: Let's say that, based on AI, a technological capability were to be developed that could warn of an impending terrorist attack about to take place in a few minutes' time by identifying a certain person in the crowd as someone about to launch an attack. Such systems, based on machine learning, may be so sophisticated that their pinpointing of one person or another cannot be explained due to concrete suspicious behavior on his part (e.g., the way he walks or his facial expression). When such systems become common and are used by security officials, a police officer may approach a person in a crowded area and arrest him on suspicion of being about to carry out a terrorist attack. Due to the fact that we are talking about a potential terror attack, this scenario may become complicated due to the possible errors that can be made by security technology systems that are designed to prevent terrorism. As a rule, prior to any use and implementation of a new technology in the field of counterterrorism, an early reliability test of the technology should be carried out. In dealing with terrorism, the main concern is of the technological system producing a "false negative"—that is, a situation in which the system errs and mistakenly dismisses a subject as not being a terrorist. Imagine that a terrorist carrying a bomb passes through a security check at the airport before boarding the plane, and the system fails to identify the explosive device and lets him through. The ramifications of such an error are fatal—the plane may explode in the air.

When we are dealing with suicide attacks in which the terrorist is in a crowded place, is wearing an explosive belt on his body, or carrying an explosive device, and can control the bomb by flicking a switch with his finger, the problem becomes even graver. In these cases, the danger can be neutralized, in most cases, only by firing at the suspect. Any attempt to stop him in another way is likely to lead to the terrorist detonating the explosive device right away and killing those in his immediate vicinity, including the security guards who have approached him to make an arrest. However, shooting in

these cases may not be sufficient, since the shooting must be aimed at killing the suspect, not only causing him injury and neutralizing him. This is because in the situation described, the injury of the suspect will not necessarily prevent the suicide bomber from flicking the switch, thereby killing or injuring the people around him. In other words, when a security technology system casts suspicion on a person as being a suicide bomber and in fact produces a false positive, such a mistake is also liable to cost human lives—the life of the suspect. Therefore, security systems based on big data and machine learning (especially deep learning), about whose decisions developers and operators are unable to make any judgments, may in certain cases endanger human life. If in the future such systems are connected to autonomous robotic weapons systems, the danger will increase considerably.

Another example can be found in advanced facial recognition systems based on AI, big data, and machine learning. Scientists have now developed the ability to identify a person's characteristics according to his features, based on the scanning of millions of people's facial features.[35] For example, some say they are able to identify the faces of homosexuals, compulsive gamblers, drug dealers, and terrorists. These are not biometric systems that measure signs of nervousness or extreme emotions (systems that can be explained and monitored), but rather AI systems that, based on the processing of millions of images, have purportedly developed the ability to identify terrorists. From here, the road to arresting a suspect with the supposed features of a terrorist is short. This could be a person who is not only not a terrorist today but perhaps has no intention of becoming a terrorist in the future. Still, the system warns with a high degree of certainty that at some point in his life he is likely to become a terrorist, judging by his facial features. The system is not necessarily based on an ethnic profile or on any other profile, and as stated, its decisions cannot be explained and therefore cannot be refuted either. How is modern society supposed to treat a person "with the facial features of a terrorist?"[36]

The use of AI in the field of counterterrorism has many clear advantages and likely has proven accomplishments as well. The writings of Israeli intelligence experts teach that the trigger for the development and use of big data systems based on machine learning was the need to find an intelligence response to the growing phenomenon of lone wolf attacks, those carried out by terrorists who are not operationally connected to any terrorist organization.

The importance of AI and big data technology in thwarting terrorism in general and attacks by lone wolves in particular can be learned from the words of the head of the Shin Bet in his speeches in recent years. Shin Bet chief Nadav Argaman testified before the Knesset Foreign Affairs and Defense Committee in March 2017, and explained that "the main perpetrator of terrorism in the field remains the 'lone terrorist.'" He said that "the Shin Bet has made a quantum leap in its efforts to locate and thwart lone terrorists." He attributed this leap, and the Shin Bet's ability to cope with the wave of lone wolf terrorism in the years 2015–2016, to "changes we have made and technological, intelligence and operational developments that we have put into practice."[37] The Shin Bet's great achievements in this area can be gleaned from another briefing given by the Shin Bet head to the Foreign Affairs and Defense Committee at the end of 2017, in which he summarized the service's successes in thwarting terrorist attacks in 2017.

According to data provided by the director of the Shin Bet, over the course of 2017, the number of "unorganized" terrorist attacks (those by individual terrorists and independent networks) decreased from 163 attacks in 2015, to 108 in 2016, and down to 54 in 2017. According to him, following the adjustment of the intelligence-operational response, in 2017 the Shin Bet succeeded in locating more than 1,100 potential lone terrorists, and in 2016, 2,200. In the same Knesset briefing it was stated that "the Shin Bet has invested heavily in technological prowess and the development of new tools and capabilities in cyber and technology. Over the course of the year, the cyber-activities of our adversaries were identified and thwarted, and various activities were carried out that yielded qualitative intelligence that contributed to the prevention of terrorist attacks and the saving of human lives."[38] This trend continued in 2018, according to the Shin Bet chief. At an international conference of homeland security ministers held in Jerusalem in June 2018, Argaman announced that about 250 attacks had been foiled in the first half of 2018, during which time more than 400 Palestinians who had planned lone wolf attacks were arrested. He noted that the Shin Bet has invested in technology that includes "learning systems and artificial intelligence."[39] Furthermore, a statement put out by the Shin Bet stated that "a major blow against terrorism can be made possible by the combination of high quality and dedicated human capital and advanced technology and unique and professional methods of operation. The extensive investment made by the Shin Bet in technological developments in the realms of big data, learning systems and artificial intelligence has led to a major leap in the transition from intelligence utilization to intelligence forecasting for the purpose of thwarting terrorist attacks before they occur."[40] In his introduction to the book *Big Data and Intelligence*, Argaman wrote, "In recent years, the service has taken significant steps aimed at adapting its technological capabilities to new needs, from the issue of storage volume through to complex challenges such as the ability to automatically extract text, visual or voice information, and of course, the ability to identify and distill, from an ocean of data, relevant and accurate information that can provide us with leads that help us to do our job."[41]

An article published on the subject on an Israeli news website stated that "Over the last two years, the IDF [Israeli Defense Forces], the Shin Bet, and the police have been working together to identify Palestinians who have been defined as having the potential to carry out terrorist attacks. As part of this joint work, the security bodies are monitoring content on social networks and other media outlets as part of their efforts to thwart terrorist attacks. … Since December 2015, and until the end of December 2017, some 7,000 Palestinians who met these criteria were identified and 200 of them received warnings by telephone, were summoned to the IDF's liaison and coordination headquarters in their area of residence, and in exceptional cases were even arrested."[42] The numbers, then, are vast. Over two years, the monitoring of social networks yielded 7,000 suspicious or disturbing cases. As mentioned, the Shin Bet claims that in 2016 it succeeded in detecting 2,200 potential lone terrorists, in 2017 1,100, and in the first half of 2018 about 400. Indeed, in a lecture given by Argaman at Tel Aviv University's international cyber conference, he noted that "locating an individual terrorist is a huge challenge. Despite this complexity, the Shin Bet, together with its partners, has succeeded, through technological, intelligence and operational changes, to locate in advance more

than 2000 potential lone terrorists since the beginning of 2016. Groundbreaking technological advances, along with operational work on the ground, have contributed greatly to reducing terrorism and to successfully dealing with the threat of lone wolf attacks." Argaman said that "the Shin Bet is currently in the midst of an organizational revolution at the heart of which is the uniting of all of the technology and cyber sector into one arm. The result is strong and concentrated technological power. The strength of this power stems from a combination of disciplines: cyber in all its variants, along with the classical areas of technology that have developed with the organization since its inception. The Shin Bet's cyber and technology structure is an unceasing startup."[43] One of the moves initiated by Argaman within the Shin Bet that led to a leap in the organization's capabilities was the merging of the signals intelligence (SIGINT) unit, the cyber unit, and the technology unit into one division.[44] According to the Shin Bet's website, "The Information Systems Technology division is in charge of developing new and innovative systems and infrastructures in the field of intelligence/operational technology. The division engages in various activities, in which innovative developments are made in fields such as computer vision, speech recognition, data mining, and neural language processing. Machine learning–based capabilities and deep neural networks algorithms developed in the division help to navigate the growing amount, variety, and pace of information inflow and allow for better and clearer identification of events of interest to intelligence and operations experts. Employees of the Information Systems Technology division are involved in various operational activities. A strong connection to fieldwork is necessary for them to understand its technological requirements as they arise and offer optimized solutions. The systems and infrastructures developed by the division are crucial weapons in ISA's effort to obtain important intelligence in real time and disrupt terrorist intentions in advance. These capabilities are unique to ISA and considered state-of-the-art in the industry and the intelligence community. In recent years, the Information Systems Technology division has received several intelligence/operational achievement awards from the prime minister of Israel for major developments that have significantly contributed to state security."[45]

The evolutionary process undergone by the Shin Bet on this matter was described in 2014 by the outgoing head of the agency's Information Systems Technology division, Ronen Horowitz. According to Horowitz, the Shin Bet has been mining data for many years. "I started running the agency's SIGINT in 2000. We received human resources and money, and we built the first generation of data mining systems. We have been connected to artificial intelligence for more than 15 years. I can tell you with certainty that quite a few terrorists are looking at us from the sky due to our ability to uncover important information from the sea of material online—big data. We are at the forefront of this field in Israel and in the world." Horowitz added that "the fact that today the phone is almost everyone's personal computer is very significant. It accelerated the explosion of data. … The more information you have, the more advantageous it is. In my opinion, human capability reached its maximum long ago with regards to intelligence. We don't have enough ears that understand Arabic, and we don't have enough eyes that know how to read Arabic. The amount of information is endless. From it, only a fraction is relevant, so extraction is required. … [O]nce upon a time there was only text. Today there is video, pictures and speech, as well as traditional text. We

invest a lot in technologies that attempt to extract pieces of information and turn them into data that can be analyzed using advanced methods. … The scientific basis is external, but many of the programs were developed internally, alongside systems that were purchased from huge IT companies. In some cases, we identified Israeli products and startups at the beginning of their journey. We bought the products for the Shin Bet and developed them before they matured on the outside. Active use of big data that can generate alerts—we developed this a good few years ago, and many Israelis were saved because of it. We are looking for a needle in a haystack, with very weak signals and a very sophisticated adversary, and we have had quite a few successes."[46] The Shin Bet director summed up the process undergone by the agency by emphasizing the human aspect. He said that more than a quarter of the Shin Bet's employees have a technological orientation. "We set ourselves the goal of recruiting and developing employees who are capable of coping with the challenges and tasks before us. Our training and career development tracks have been significantly upgraded, and they are now competing in a worthy and respectful manner with the private sector," he said.[47]

It is not hard to argue that AI has been successful in thwarting terrorism through a combination of machine learning and big data. In mid-2017, within a little over a year, Israel arrested 400 Palestinians suspected of planning attacks after monitoring social networks. The new methods used by the Shin Bet and Military Intelligence identified about 2,200 Palestinians as being at various stages of planning and preparing for attacks, mostly stabbings and car-rammings. The IDF and Shin Bet arrested more than 400 of these would-be perpetrators. Some were put on trial and others were transferred to administrative detention without the nature of the suspicions against them being clarified to them or being examined in depth by a legal authority. The names of another 400 were passed on to the Palestinian Authority, whose security forces arrested them and warned them against planning attacks on Israel. The rest of them, and in some cases their parents, received warnings from the Shin Bet and IDF.[48]

However, despite—and perhaps even because of—the success of the use of AI and big data in the field of counterterrorism, and especially in light of the huge number of arrests and foiled attacks that have taken place in recent years in Israel—and likely in other countries as well—thanks to this innovative technology, there is a need to develop clear ethical codes to define norms in counterterrorism activities carried out using big data and AI by security and intelligence agencies. These codes should enable, inter alia, effective supervision of these processes by the legal system.

In this context, we must ask ourselves the following questions: Can we accept big data intelligence systems that come up with 7,000 suspects in two years? What does it mean to define 3,300 Palestinians in two years as "potential lone terrorists"? And if they are "potential" does this not mean that some of them may not end up being lone terrorists? How can the law enforcement system cope with such numbers resulting from information extraction processes using AI? Is it necessary or possible to convict these suspects in court, or can it be that the appropriate solution for foiling and preventing the attacks that they are liable to commit is administrative detention? Can they be guaranteed some kind of proper procedure to defend themselves and prove their innocence when AI systems have indicated the potential danger they pose? As discussed earlier, the fear is that, either under the pretension of or as a result of a sincere and genuine

desire to protect human life and prevent terrorism, liberal principles and basic human rights will be trampled on. In this respect, thousands of suspects and a very large number of detainees should not necessarily be considered as a suitable measure for success and intelligence effectiveness. These numbers may actually indicate the use of a filter that is too broad and has too many holes. If these holes are also invisible, or cannot be measured—if we cannot understand the work of AI—the danger increases exponentially.

It should be noted that the assumptions and assessments in this article regarding Israeli intelligence's practices in the field of AI and big data rely solely on statements made by stockpersons of the security establishment as they were published in the Israeli media and in scientific publications. It is not possible to determine from this information the level of awareness these bodies have regarding the ethical and moral dilemmas involved in the use of big data and what control mechanisms are employed in this context. However, even if the Israeli security and intelligence agencies are aware of the problems and maintain all the required systems of checks and balances, the challenges and concerns set out in this article regarding the integration of AI technology, machine learning, and big data in the realms of intelligence and counterterrorism should serve as warning signs for security and intelligence services in countries that are considering implementing AI systems in their counterterrorism activities.

Over the years scientists have invented new technologies that, over time, have become a real danger to the lives of many people and perhaps even to humankind. For example, technologies have been developed to optimize the production and use of fuels and other energy sources have caused severe environmental pollution and global warming. Nuclear weapons that were designed to deter adversaries themselves endanger world peace. The cracking of the human genome led to enormous medical achievements but at the same time poses serious dangers to humankind. The common denominator of all of these technologies is the need for tight regulation and strict supervision. The same applies to the development of AI technology, machine learning, and big data. There is no dispute about the many advantages inherent in this technology, but the risks involved in the development of AI-based technologies, especially those used in the areas of security, intelligence, and counterterrorism, mandate the formulation of rules and guidelines for their use, and effective mechanisms for monitoring the implementation of these rules. This task is not only the burden of computer scientists or security officials, but rather that of the legislative, executive, and judicial branches, and indeed that of society as a whole.

Recommendations

The development of guidelines for the use of AI and big data technology for the purpose of thwarting terror attacks and intelligence work is a long and complex process. It requires joint work by computer scientists, security experts, terrorism experts, strategists, jurists, and philosophers. These experts should consider, inter alia, the following principles:

1. Despite the natural tendency to grant the security forces involved in counterterrorism lots of room to make their own choices, when it comes to the use of AI and big data in

the field of intelligence and the prevention of terrorism, a fastidious approach must be taken that will limit infringements of citizens' privacy, as this technology is liable to bring along with it the violation of the rights of many citizens.

2. AI technology combined with big data should be treated as a means of mass surveillance and tapping. To that end, the use of databases that involve compromising people's privacy should be conditioned on the prior approval of a judge and on the scope and nature of the terrorist threat at the time.
3. The way that AI and big data are used for intelligence and counterterrorism purposes should be monitored regularly by the judicial and legislative branches.
4. Each database to which the system is given access should be assessed, along with the level of potential encroachment on privacy that may occur through the use of this database. (This assessment would be done based on the type of information available in the database, the manner in which it is obtained, and the number and identity of those who may be harmed by its use).
5. Clear criteria should be defined and established for the use of databases for the purpose of thwarting terrorism, and the meeting of these criteria should be objectively monitored. For example, it can be determined that:
    - Permission to use big data databases that involve a high level of privacy breaches will be given only by court order and for the purpose of locating concrete terrorists.
    - Permission to use big data databases that involve a high level of privacy breaches will be given only for the purpose of gathering basic intelligence—identifying trends and processes without any identifying details of suspects.
    - Permission to use big data databases that involve a high level of privacy breaches will be given only for the purpose of predicting concrete attacks, while preserving the anonymity of the information.
    - Permission to use big data databases that involve a low level of privacy breaches will be given for the purpose of initial identification of suspects, with further investigation via monitoring, wiretapping, or other means to be carried out by court order.
6. The use of AI and big data technology to prevent terrorism should be avoided when the results of the algorithms cannot be explained.
7. Before approving the use of AI and big data in the field of counterterrorism, the various algorithms must be carefully examined in order to minimize false negatives and avoid false positives.
8. The incrimination of "potential terrorists" identified using big data technology should be considered only when there is additional supporting incriminatory evidence, and should not be based on the results of the analysis of big data and AI alone.
9. With regard to the identification of "potential lone terrorists," each case should be examined on its own merits and the exact point of any suspect identified by AI should be defined on a scale representing the degree of risk of the realization of one's terrorist potential. In other words, how far off is the suspect from carrying out the attack—is he in the initial/advanced stages of radicalization? Has he made preparations for the attack? This can be referred to as the "ticking bomb scale." The treatment of each suspect must be adapted to the level of risk he poses.
10. The ticking bomb scale should define the precise stage at which a person with extremist views becomes dangerous and is liable to use violence.
11. Caution must be exercised so as not to build algorithms based on cultural or ethnic bias. Objective criteria should be maintained as much as possible.
12. Because "lone wolves" in many cases suffer from mental illness, and because the family is often unaware or even opposed to the suspect's radicalization, a family-based treatment approach should be adapted to suspects identified in big data analyses who have been defined by the ticking bomb scale as being low risk.
13. The number of alleged foiled attacks carried out as a result of using AI and big data should not be used as a measure of the success and effectiveness of the security forces.

(An extreme lack of proportion between the actual number of attacks and the number of foiled "potential attacks" may serve as an indication of a slippery slope and an unjustified "over-foiling" of attacks).

14. Administrative detention of suspects found using AI and big data should be avoided as much as possible. It should be ruled that any suspect detected by AI be brought before a judge to look at each case on its own merits.
15. The principle that, with regard to counterterrorism, AI systems should only support decision making and should never be autonomous decision-making systems must be adhered to.
16. In the field of counterterrorism, reliance on big data databases and AI results and data originating from foreign intelligence and security agencies should be avoided as much as possible.
17. The relevance of AI and big data algorithms should be examined periodically, in accordance with changes in the scope and nature of the phenomenon and in light of the evolution of modern terrorism.

Conclusion

In conclusion, Supreme Court President Aharon Barak referred in the past to the complex role of a judge in a democratic society that finds itself repeatedly hit by terrorist attacks, saying: "I hope that Israeli society will not find itself with a naïve judge who sees everything as a security problem. The rule of law is the country's security. I hope that Israeli society will not find itself with a naïve judge who sees basic rights as the be all and end all. A constitution is not a prescription for suicide. I hope that Israeli society will find a reasonable and cautious judge who tries to see all aspects of the picture, who is aware of his creative role, who tallies the different interests objectively, who applies the fundamental principles in a neutral manner, and who tries to find the delicate balance between majority rule and the basic rights of the individual, a balance that represents the democratic equation of the regime."[49] We can take Justice Barak's remarks and apply them to the challenges of the use of AI and big data in counterterrorism, and say that: We hope that the international community will not find itself with a naïve scientist and security official who see the need to solve security problems as the ultimate and supreme goal. The need to protect the rights of individuals in society is no less important than the need to protect their security. We hope that the international community will not find itself with naïve scientists and security personnel who see these basic rights as the be all and end all. Values and rights are not a prescription for suicide. We hope that the international community will find reasonable and cautious scientists and security officials who try to see all aspects of the picture, who are aware of their creative role, who tally the different interests objectively, who apply the fundamental principles in a neutral manner, and who try to strike a delicate balance between effectiveness in the fight against terrorism and the liberal democratic values of society. A balance that represents the democratic equation of counterterrorism.

Notes

1. Henry Kissinger, "How the Enlightenment Ends," *The Atlantic,* June 2018, https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/.

2. Timme Bisgaard Munk, "100,000 False Positives for Every Real Terrorist: Why Anti-Terror Algorithms Don't Work," *First Monday* 22, no. 9 (September 2017), https://doi.org/10.5210/fm.v22i9.7126
3. Rick Delgado, "How Big Data is Aiding in the Fight Against Terrorism," Datafloq, https://datafloq.com/read/amp/big-data-aiding-the-fight-against-terrorism/1035 (accessed 5 November 2018).
4. James Ovenden, "Fighting ISIS with Big Data," Innovation Enterprise Channels, https://channels.theinnovationenterprise.com/articles/fighting-isis-with-big-data (accessed 5 November 2018).
5. "Using Big Data Effectively in the Fight Against Terrorism," Defence Contracts Online, https://www.contracts.mod.uk/do-features-and-articles/using-big-data-effectively-in-the-fight-against-terrorism/ (accessed 5 November 2018).
6. Mike M, "Defeating Terrorism with Big Data," *Harvard Business School Digital Initiative*, 17 November 2016, https://rctom.hbs.org/submission/defeating-terrorism-with-big-data/
7. Kissinger, "How the Enlightenment Ends."
8. Munk, "100,000 False Positives."
9. Nicholas Wright, "How Artificial Intelligence Will Reshape the Global Order," *Foreign Affairs,* 10 July 2018, https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order
10. Col.Y., (Heb.), "The Journey Towards Clarifying the Perception and Implementation of Intelligence and Operational Superiority in the Digital Era," *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 12.
11. Ibid, 14.
12. M., (Heb.), "Angels in the Skies of Berlin—New Intelligence Questions in a Data-Saturated World," *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 56.
13. Ibid., 59.
14. Lt. Col. T., (Heb.), "Intelligence Derivatives of the World of Big Data," *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 26–28.
15. Colin Koopman, "How Democracy Can Survive Big Data," *New York Times*, 22 March 2018, https://www.nytimes.com/201829/03/22/opinion/democracy-survive-data.html?rref=collection%2Fcolumn%2Fthe-stone&action=click&contentCollection=opinion&region=stream&module=stream_unit&version=latest&contentPlacement=15&pgtype=collection
16. Lt. Col. T., (Heb.), "Intelligence Derivatives," 26–28.
17. Col. Y., (Heb.), "The Journey," 17.
18. M., (Heb.), "Angels in the Skies of Berlin," 60.
19. Lt. Col. T., (Heb.), "Intelligence Derivatives," 28.
20. Ben-Tzur, (Heb.), "The Social Networks and the Individual," in *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 70.
21. Major A., (Heb.), "Network Intelligence Analysis in the Age of Big Data," in *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 49.
22. Ibid., 54.
23. Ibid., 50.
24. Col. Y., (Heb.), "The Journey," 17.
25. Ibid., 13.
26. Lt. Col. T., (Heb.), "Intelligence Derivatives," 29.
27. Boaz Ganor, *The Counter-Terrorism Puzzle: A Guide for Decision Makers* (New Brunswick, NJ: Transaction Publishers, 2008), 51–53.
28. Kissinger, "How the Enlightenment Ends."
29. Lt. Col. T., (Heb.), "Intelligence Derivatives," 30.
30. Ganor, *The Counter-Terrorism Puzzle*, 147–178.
31. Dudi Siman Tov and Lt. Col. T., (Heb.), "The Big Data Revolution from the Perspective of Mega-Organizations," interview with Yoelle Maarek, Vice President of Research at Amazon, in *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 34.
32. M., (Heb.), "Angels in the Skies of Berlin," 56.

33. Major A., (Heb.), "Network Intelligence Analysis," 50.
34. Shira Patel (Heb.), "Big Data in Intelligence Work—Roles, Applications and Limitations," in *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 144.
35. ."Our Technology," Faception, https://www.faception.com/our-technology (accessed 5 November 2018).
36. See, for example, Justin Huggler, "Facial Recognition Software to Catch Terrorists Being Tested at Berlin Station," *The Telegraph*, 2 August 2017, https://www.telegraph.co.uk/news/2017/08/02/facial-recognition-software-catch-terrorists-tested-berlin-station/
37. "Knesset Foreign Affairs and Defense Committees," Knesset.gov.il, last modified 20 March 2017, https://main.knesset.gov.il/Activity/committees/ForeignAffairs/News/pages/pr200317_1.aspx
38. "Knesset Press Release," Knesset.gov.il, last modified 24 December 2017, http://m.knesset.gov.il/News/PressReleases/pages/press24.12.17a.aspx
39. Yehoshua Breiner, "Shint Bet Chief: We Foiled About 250 Attacks Since the Beginning of 2018," *Haaretz*, 13 June 2018, https://www.haaretz.co.il/news/politics/1.6173611
40. Itzik Saban, "ISA Foils 250 Attacks Since Beginning of Year," *Israel Hayom*, 13 June 2018, https://www.israelhayom.co.il/article/563493
41. Nadav Argaman, (Heb.), "Introduction," in *Modi'in Halacha VeMaaseh*, Big Data and Intelligence, May 2018, 7.
42. Yaki Admaker, "The Silence is Misleading? We Thwarted 400 Significant Attacks This Year," *Walla News*, 24 December 2017, https://news.walla.co.il/item/3121680
43. Or Heller, "The Shin Bet is in the Midst of an Organizational Revolution," *Israeldefense*, 27 June 2017, https://www.israeldefense.co.il/he/node/30145
44. Amir Bouhbut, "A Network of Agents, an Interrogation System, and a Cyber-Terrorist Network," *Walla News*, 25 December 2017, https://news.walla.co.il/item/3121844
45. "Information Technology," Cyber Technology, The Israeli Security Agency, https://www.shabak.gov.il/english/cybertechnology/Pages/technology.aspx (accessed 5 November 2018).
46. Amir Rappaport, "Thanks to Cellular Technology: Israeli Intelligence Jumped a Class," *Makor Rishon*, 21 November 2014, https://www.makorrishon.co.il/nrg/online/1/ART2/648/073.html
47. Heller, "Organizational Revolution."
48. Amos Harel, "Israel Arrested 400 Palestinians Suspected of Planning Attacks After Monitoring Social Networks," *Haaretz*, 18 April 2017, https://www.haaretz.com/israel-news/how-israel-uses-big-data-to-fight-palestinian-terror-1.5461381
49. Aharon Barak, *Judicial Discretion* (New Haven, CT: Yale University Press, 1989), 506.