CHAPTER 3

Deep Defense

Past-Future-Present (in This Order)

Strategic challenges require a process of learning. This process is based on the past, future, and present (yes, in this order). Past – to understand the genealogy and the framework we have reached to date. Future – to discover the potential risks and opportunities for the future. Present – to crystallize strategic action trends to avoid risks and seek to fulfill the opportunities. One of the ways to think about the future is the concept of scenarios. Keens Van der Heijden, in his book *Scenarios: The Art of Strategic Conversation*, develops scenarios as alternative ways to describe options for what might happen in the future. He also discusses how to utilize these scenarios in an organizational process to impact the strategy and planning of the organization as a whole and prepare it for action. Heijden explains:

"...today's best strategy may be tomorrow's disaster ... the

ultimate purpose of the scenario planner is to create a more adaptable organization, which first recognizes change and more uncertainty, and second uses it creatively to its advantage."[73]

These days, security leaders are required to build scenarios for security challenges in the Digital Era. These leaders must formulate scenarios for the Artificial Intelligence Revolution as a basis for their planning processes. How can AI be a possible game changer to win a war, and what do we need to do today to prepare ourselves for the near future?[74]

Past (Experience and Challenges for National Defense)

War is the supreme test of a military organization. The primary national security mission is to protect the country and win in war. Historically, many wars have broken out without warning; moreover, some of them began even though neither side wanted a war. However, the adversaries ended up in a difficult and bloody war, and sometimes even found themselves in a war for survival. In addition, the results of war have far-reaching implications, and the results also design the future for many years. In the complex environment of the Middle East, the meaning of a "good" or "bad" war has tremendous repercussions for all sides. In the distant past, until the end of the World War II, a victory or loss in war was usually clear-cut. The winning side conquered the territory of the loser, and everyone knew who won and who lost. In the last 80 years there have been wars that ended with clear victory, there have been wars that ended without any clear defeat, and the struggle over who won and

who lost exists even until today.[75]

From the Israeli perspective, there are wars like the Six-Day War in 1967 and the Sinai Campaign in 1956,[76] in which Israel defeated its enemies and the victory was clear and sharp. Conversely, there are wars such as the Yom Kippur War (1973) when both sides are convinced – even until today – that they won. In the last 20 years, the Israeli military has concluded operations and wars with a feeling of "*hachmatza*" (Hebrew for a "missed opportunity"). For example, the 2006 Winograd Commission (the Israeli government's official commission of inquiry into the Second Lebanon War) argued in detail that the Israel Defense Forces missed an opportunity to defeat Hezbollah and achieve a decisive victory, and all the operations in Gaza over the last 15 years ended without definitive results.

Moreover, over the last few decades and since the end of the Cold War, most wars and conflicts have been asymmetric. The DE empowers this asymmetric reality. Know-how that once belonged to countries became knowledge that everyone can obtain. Since the DE, every man and woman has access to more data on their smartphones than superpowers had 50 years ago. Social media created a reality in which every person can publish whatever he or she wants. In addition, the DE globally empowers the phenomenon of "lone-wolf" terror attacks. This type of attack takes place as "terror due to inspiration." A person reads something on social media or sees a picture about something that happened and decides to go out and commit an attack. Moreover, the ability to self-publish this terror attack is another issue that helps the individual make a decision to do it.

From time immemorial, there have been lone-wolf terrorists, but in the DE this phenomenon has become more and more widespread. As a result, lone-wolf terrorists are a bigger challenge for national security establishments.[77]

Another complex challenge that is growing and becoming stronger is the ability to protect countries' borders from infiltrators, terrorists, underground tunnels, drones, etc. The border wall between the U.S. and Mexico is an example of this challenge. Moreover, protecting borders is also a unique challenge during war, as evidenced by the concept of attack tunnels that Hamas built along the Gazan-Israeli border, and that Hezbollah built along the Lebanese-Israeli border.

In the last few years, Hezbollah in Lebanon has a military challenge for Israel. During the Digital Era, Hezbollah, with support from Iran, has managed to arm itself with more than one hundred thousand rockets that it can use against targets in Israel. In addition, these rockets increasingly have the capabilities of guided missiles. Hezbollah uses the civilian population in Lebanon to empower its capabilities: its fighters and rockets are located strategically among the population and they commit their acts from inside the population centers. Thus it is difficult to identify and produce targets to attack the rocket launchers effectively or use special forces to prevent Hezbollah from using the rockets. In other words, it is difficult to uncover tens of thousands of launchers that are hidden within the cities and villages, and among civilian buildings and homes. Moreover, it is very difficult to attack the launchers without harming countless innocent civilians. For example, in the Second

Lebanon War in 2006, more than 4,000 rockets were fired by Hezbollah into Israel over a period of 33 days. For the next war, the threat has grown dramatically. Hezbollah plans to fire thousands of rockets against Israel every day, including guided missiles against strategic assets in the heart of the country. Preventing Hezbollah from effectively using these rockets and missiles is an extremely important undertaking. The bottom line is that over the last few decades, and specifically during the last few years, Israel finds more and more defense challenges for which our traditional abilities and strengths will not be able to completely defeat the enemy. Therefore, asymmetric conflicts have concluded without clear victories.

Future (from the AI Perspective)

In 2040, the national security organizations will be more different than similar to their structure today. They are going to be so different that we cannot even describe what the big issues and top priorities will be. In addition, we cannot even imagine the future structure of these organizations. Infinite data will be organized in such a way that everyone will be able to use it. A few significant, traditional, intelligence positions, such as audio-lingual analysts and aerial-image analysts, which today require thousands of analysts, will almost disappear and be replaced by AI machines. Big data will be the key to finding and understanding rivals and enemies. Data from hundreds of thousands of drones will be part of the basic information about everything. Classified and unclassified data will be on the same

"closed-open-closed network" in a way that you can keep your secrets and at the same time enjoy the advantages of an open network. All of these are just a few examples regarding the changes that will occur by 2040. The more important changes that will take place cannot even be imagined today; the only option is to lay the groundwork and begin the AI journey.[78]

An Example of a National Security Scenario for 2035
Hezbollah in 2035

Welcome to 2035. Hezbollah now has more than 200,000 rockets, including hundreds of guided missiles. In addition, Hezbollah has developed AI capabilities to empower its command and control system and can effectively use all of their rockets and missiles. Moreover, after Israel discovered and destroyed the underground tunnels that Hezbollah had excavated along the Israeli-Lebanese border, the organization armed itself with more than 1,000 AI drones that can penetrate Israeli territory. Hassan Nasrallah, Hezbollah's leader, is 75 years old and is looking for a historic victory against Israel. His senior commanders tell him that they can achieve this goal.

AI in 2035

The reality today (in 2035) is that AI has already increased and accelerated the DE Revolution.

This is the period when AI has begun to address challenges in novel, unusual ways that years ago we could not have

imagined. Problems that humans didn't know how to solve in the past, AI has begun to solve in our lifetime. Challenges that people did not know how to address in 2020, can now be examined with AI.

"Deep Defense:" New Potentials

Deep Learning is the ability to use technology and digital capabilities to go "deeper" and discover and understand issues that were previously "covered" and impossible to achieve. Deep defense is the ability of national establishments to use The Human-Machine Team concept to address security challenges to expose issues in new ways that were heretofore impossible. The first new potential for war is the ability to create "targets in context." The Human-Machine Team has the ability to create tens of thousands of targets before a battle begins, and to assemble thousands of new targets every day during a war. In addition, the ability to create these targets in context means that the military can attack the right targets at the right time. This means finding tens of thousands of hidden rocket launchers, understanding when they are manned with enemy fighters or unmanned, and understanding when it is possible to attack them without harming civilians. Imagine 80,000 relevant targets that are produced before combat and 1,500 new targets created every day during a war. Imagine that we have the constant ability to know whether the targets are manned with enemy fighters or unmanned. Finally, imagine a reality in which the military has the ability to strike "the right targets

at the right time," destroying the target with the least possible collateral damage.

In the past, the "fire effort" that includes several capabilities to attack from afar, such as artillery from mortars and cannons, was an assistive effort in war. However, over the last few decades, the fire effort has become the major effort to win in war. The air forces and the exact weapons – specifically, guided missile fire and missile elimination – have become one of the most important capabilities for victory. This is also the reason that for decades, the armed forces of the world have been trying to improve the connection between the "intelligence factory" and the "fire factory."[79] The ability to decisively win a war requires that every day during the war, you put your enemy in a situation that is worse than the situation he faced the day before. If your enemy's situation gets worse each day, he'll want to stop the war as soon as possible. Therefore, tens of thousands of "targets in context" have the potential to achieve this. During the last several decades, the fire effort has been very important, but most of the targets were created before the war. Meanwhile, during the war many factors change quickly, and striking a specific target at a specific time becomes a special operation requiring outstanding resources. Having the capability to increase the number of targets hit day after day, and strike these targets at the exact preferred time, can force the enemy to decide to end the war as soon as possible.

Humans are the bottleneck that prevent the creation of tens of thousands of targets in context. We cannot process that much information. If we want to create 80,000 targets before the war,

we need thousands of intelligence investigators who need years to work on such a mission. Furthermore, a few weeks or a few months after these targets have been identified, the military cannot possibly know whether any individual target is still relevant. The moment the war begins, many of the original targets will have changed, and it is usually difficult to confirm whether the targets are manned with enemy fighters or unmanned. Interestingly, it doesn't matter how many people you have tasked to produce targets during the war – you still cannot produce enough targets per day. There is a human bottleneck for both locating the new targets and decision-making to approve the targets. There is also the bottleneck of how to process a great amount of data. Then there is the bottleneck of connecting the "intelligence" to the "fire."

The Human-Machine Team has the potential to bring about a revolution in the possibility of creating targets in context. A team consisting of machines and investigators can blast the bottleneck wide open. Machine-learning has the potential to deal with big data, a function that a human brain cannot perform alone, but many decisions can be made together. The Human-Machine Team is capable of learning and drawing conclusions from big data in order to make predictions, and from these predictions creating targets and also answering the question of whether the targets are relevant in real-time.[80] This potential requires organizing all the layers of information in a way that we can build a "targets machine" based on all the data and sensors in the field; moreover, this team helps monitor ethical issues. Therefore, the decisions are not "machine

decisions," but rather mutual decisions that are a result of synergetic learning.[81]

The second new potential is to use The Human-Machine Team concept to understand the changing reality of the enemy during war. As Carl von Clausewitz wrote, "War is the realm of uncertainty." The big picture of a war, and the picture of every single battle, change during the war. Moreover, since the enemy does not know how its own forces will perform during the war or exactly where they will be located, it is also going to be difficult for the friendly side to find these enemy fighters and understand the big picture. Google Maps and Waze are able to provide constant, minute-by-minute big pictures of traffic and incorporate the details of every road; these apps help drivers make decisions. Within the limitations of the metaphor, The Human-Machine Team has the potential to use AI to get a snapshot ("the trees and the forest") of the enemy at every moment and in every location to help the military forces fight and defeat the enemy. This potential is based on the new intelligence capabilities in the period of AI, such as speech-to-text and data-mining, which are good examples of the new capabilities available to create a "military Waze."

The third new potential is to use The Human-Machine Team to be a game changer to build a "smart border" (or "smart area") to control the borders, to figure out changes along the borders, and to use drones or other robotics in these areas. The Human-Machine Team enables a new potential for using AI to build a smart area for protecting borders. The ability to connect various bits around the borders through machine-learning can

help control and protect these areas. The smart area is required to define the location, organize the relevant sensors in the context of the operational problem, and prepare the "channels" of the information in the context of that same location.

The fourth new potential is the "influence or shaping effort" in the AI period. In the DE, truth and falsehoods are mixed. The development of media, and especially social media, contributed to this shaping of reality. Today, everyone can be a kind of media station with their own cellphone. The simplicity of tweeting, posting, and texting caused the influence or shaping effort to be a relevant part of the "act of war" as well. The shaping effort also has the potential to be a main part of either a victory or a loss; in the era of The Human-Machine Team, it can be much more relevant. For example, machine-learning can help create "influence in context," which means that different audiences and different individuals will receive the relevant data by the relevant media that has the greatest chance of influencing them. (The following sections will discuss how to develop intelligence organizations to realize this idea.)

The fifth new potential is to use The Human-Machine Team to understand ourselves. The notion that "War is the realm of uncertainty" means that we also cannot know where our forces will be positioned and how they will react during the war. One of the challenges of making decisions in war is the fact that we cannot understand our own military forces. AI has the potential not to just get a snapshot of our enemy, but also to get a "smart snapshot" of our military forces in real time to use as a tool to help make decisions.

Present: How to Develop "Deep Intelligence" + Three Case Studies

Strategy is the science of what we need to do today. Therefore, in the present we need to crystallize strategic action trends to avoid risks and seek to fulfill the opportunities. One strategy for bringing military organizations into the future is through the novel idea of The Human-Machine Team. This is a new concept that allows the utilization of AI to win a war and to achieve a strategic decision. The DE is a main factor in enabling asymmetric conflicts in which stronger and larger military forces do not necessarily have an advantage over smaller ones. The Human-Machine Team has the potential to regain the advantage.

Deep Intelligence

Intelligence and intelligence organizations are broad issues, each of which can fill an entire book of its own. There are people who used to describe the DE as an Information Revolution or the Information Age. The information that used to be "backup" for helping make decisions became the issue in and of itself. The data that used to be in the "back" has moved to the front. Therefore, intelligence in the period of AI requires a revolution to help deal with the new paradigm and to address the new risks and new opportunities. The next few years are going to be in between paradigms.[82] In this section we will try to provide a few ideas and first thoughts for the beginning

of the journey to realize the revolution of intelligence in the period of AI.

A Short Background

Intelligence has existed since the dawn of history. For thousands of years, intelligence has included people who work as spies or watchmen for a leader or commander by providing him or her with information. Intelligence organizations exist today based on the way they have been designed over the last 100 years. Our intelligence organizations were established in the period between WWI and WWII. Organizations all over the world use different functions and abilities to stay one step ahead of their enemies and rivals. There are national bodies that customarily describe this idea with the concept of "intelligence supremacy," a concept that refers to the ability to be not only one step ahead of our enemies but also a base for power policy and power activation.

One of the ways that intelligence organizations used to respond to the questions and challenges they had to address was to create specific accessibility to relevant places, attain important bits of data, and use them to piece together the "intelligence puzzle." The aim of all this activity was, and still is, to provide the intelligence picture (a clarification of reality); to point to possible future scenarios; and to offer recommendations about the ways in which this reality could be affected.[83] The dream of every intelligence officer was to be a "fly on the wall" in the mind of the intelligence object.

Intelligence organizations used to be created for various functions, including research intelligence, technological organizations (first of all for collecting data), and special forces for intelligence missions. Traditionally, intelligence bodies were based on human intelligence, technology, and operations (in this order). During the past few years there have been changes in these organizations, most of them as a result of cyberspace. The cyber domain taught us that the whole world is interconnected. This means that – at least theoretically – one can go anywhere in the global digital network. By utilizing the cyber dimension, one can provide a response to any vital information, even complex information. However, it is possible to look at all the changes over the past few years as just "stretching logic," which means that the main mission and main concept have not changed.[84]

In Essence (General Perspective)

Intelligence in the era of artificial intelligence represents another leg in the journey of clarifying the concept and using intelligence and operational superiority (in context and for specific missions) in the Digital Era. The concept of intelligence in the DE can be summarized thus: to apply the potential of the Digital Era to the systemic challenges that intelligence now faces. Alternatively, a different concept of intelligence-operational superiority, based on the understanding that the information explosion and the ability to strive to know "everything about everyone" makes an updated and different intelligence and

operational response both possible and required.[85]

The intelligence endeavor in the DE can be described as a different approach to intelligence (and operational) superiority. For example, Google's approach to the information explosion is different from that of its predecessors. One day a friend showed me a joke that was circulating on the network:

Q: "Where is the best place to hide a corpse?"

A: "On page 2 of a Google search, where it will never be found."

This joke is kind of an "aha!" moment" and captures the truth of the matter quite simply. As intelligence personnel, over the years we grew accustomed to reading hundreds and thousands of items to find a piece of a puzzle in one of these items, and then we tried to connect it to another puzzle piece in another item. Finally, we would try to construct the full picture. In actuality, most of the items do not necessarily contribute in any particular way to understanding the whole. Hence, the task of the research officer is to "separate the wheat from the chaff" and find the relevant data from within the mountains of items.

Google has a different approach. When I ask Google a specific question (and have not just woken up in the morning and begun reading through the myriad news items that arrived during the night), I am not prepared to go to page 2 of a Google search and read the title of one of the answers that appears there. I expect Google to provide me with the answer on the first page and in one of the first titles. I don't look at the second page. If I don't get an answer, I don't despair, and certainly don't say to myself, "Okay, Google doesn't know." Instead, I say to

myself, "Google knows everything, but I didn't ask Google the right question." Moreover, Google has never asked me to prioritize one population group over another. Google presumes, under the aegis of the Information Age, to know everything about everyone, even if that means knowing everything about billions of people.[86]

In a nutshell, this needs to represent the novel approach of intelligence in the DE. Superiority does not stem from one or another piece of information, but rather from the information explosion itself and the ability to ask about whatever interests me. When the information is truly infinite, then clearly one cannot expect to read all the items, and there is no need to reset the columns. The approach is different. One can and must wander among the bits of information. According to this approach, the answers can already be found in the existing information. One just has to know how to optimally navigate through it and ask the questions that interest the intelligence officer.[87]

Keeping in mind the limitations of the metaphor, we can liken the situation to the global breakthrough that occurred around the cracking of the Enigma Code. Even before then, there were geniuses who deciphered codes, but the British and the Americans knew that cracking the Enigma Code would require 20,000 people who would have to work for 20,000,000 years. Therefore, they built a machine to help them crack it. This machine was the first step in the invention of the supercomputer, which changed the course of human history. This is similar to what is happening in our era when it comes to

information, its use, and its significance.[88]

Hence, the intelligence analyst continues to be relevant (the relevance and importance have actually increased), but the conversation between human and machine is changing. Due to the fact that AI is accelerating the DE Revolution, it is also accelerating the revolution of the intelligence organizations as we know them. In other words, we can frame it with the understanding about traditional learning and synergetic learning. Intelligence is a process of learning about your rivals and enemies. The Human-Machine Team, which creates synergetic learning, is a new process of learning as well as a new way to shape and to influence.[89]

The Importance of the Question

Throughout the years, Jewish tradition has encouraged its people to know that asking questions is their right, their responsibility, and even their duty. This encouragement to ask questions is exemplified by the Four Questions that are asked at the beginning of the Passover Seder meal and are the basis for the retelling of the entire Exodus story. Intelligence, too, focuses on the responsibility to ask the right questions, thereby making it possible to pinpoint precise, vital bits of information and clarify a complex reality. These questions provide a fundamental compass for intelligence activity.

According to the traditional approach, any successful question can lead to relevant accessibility, thereby exposing the secrets of the other side. If it is a question to which there

is no answer in the available information, deep insights can still enable us to identify the adversary's logic, thoughts, and so on. In the era of information explosion, however, one can assume that for (almost) every question, a possible answer can be found in the data. One needs to know how to probe the data for the right items, construct questions that can contend with the information load, and understand that when an answer is not obtained, we must assume that we have not asked the right question.[90]

If the foundation of the information has been properly organized, the main thing we have to do is improve our ability to ask relevant questions. In addition, one can relate to a question that was asked by someone else as a potential feature for The Human-Machine Team. If an analyst searched the information about a certain matter and the information was understood in a specific way, this can reveal something new about the information. For example, if an analyst checked who was usually asleep at 11 p.m. and in the last month was awake between 1:00 and 4:00 a.m., both the question and the answer can be new features to identify indicative signs. Another example is if an analyst checked all the new greenery planted in a specific area in which it seemed that there was no reason , this knowledge can also be an indicative sign for this location. Each month, intelligence organizations ask hundreds of thousands of questions that produce hundreds of thousands of answers. Combined, these questions and answers create potentially relevant features that we can use to upgrade the power of The Human-Machine Team to achieve impressive capabilities of machine-learning.

The new knowledge can also be created from combining a few questions. For example, an analyst could decide to check all the suspects who did not sleep in their homes during the last two nights in a specific area, and who also discussed weapons purchases during the past week. This question, plus the names of the suspects produced by this question, can now be a combination of "relevant features" for machine-learning. As discussed in the section about machine-learning, the more features that can be provided to the machine for the process of learning, the better the results.[91]

Intelligence in the Era of Artificial intelligence

Automation

The first new opportunity is to automate intelligence processes in a way that can create new abilities that were not been possible before. Under this umbrella, there are new opportunities to do the same things, only faster and on a larger scale. For example, Speech-to-Text (STT) can replace audio-lingual analysts. Today, intelligence organizations have thousands of audio- lingual analysts. They are required to listen to enemy discussions or read enemies' internal data and translate the original language back to their countries' native languages. The idea behind STT appeared decades ago and has not been replaced. Today, we have the conditions and the abilities to fulfill this concept. In five years, we will still need audio-lingual analysts, but more than 80% of their tasks can be replaced by machines. Another example is machine-learning to replace

image and video analysts. Similar to audio-lingual analysts, every intelligence establishment has thousands of image and video analysts. Recently, AI machines have been learning how to replace some of these analysts' functions. Furthermore, in this area, we also have the conditions and abilities to fulfill this idea and carry out tasks using AI machines.

Completion of Puzzles That Were Previously Unsolved

A "havruta"[92] of The Human-Machine Team creates new ways to solve puzzles that were previously unsolved. One of the new abilities to enable this new potential to use AI to solve puzzles is based on "the power of the internet." Intelligence organizations previously used unique capabilities to acquire classified data. Over the years, we got used to the fact that the big secrets were found in isolated offices. Similarly, in the cyber era, the prevailing notion is that the major secrets are harbored in classified "internal networks." Accordingly, in many cases, the more intimate and internal the information, the more difficult it is to obtain this information, the higher its classification – and usually its relevance as well. For us, in the Information Age, the greatest challenge is not necessarily the ability to create intimate accessibility of one kind or another, but the ability to exhaust the relevant information within the infinite amount of information in general, and on the internet in particular.[93]

It appears that intelligence organizations have not yet achieved this revolution and certainly have not internalized it. Great efforts are still being invested in creating additional

accessibility. However, we assert that whoever wins the competition to leverage the existing information on the internet on behalf of their own organization's intelligence challenges will be a step and a half ahead of other organizations.[94] One of the secrets of success in the coming years will be precisely the ability to use the power of the internet to the benefit of the security intelligence entities.[95]

Influencing and Shaping Reality

In the DE and in the Information Age, data is part of the reality. In other words, when we influence the data, we alter reality. This is a novel, basic situation for the intelligence establishments. Intelligence organizations have been using data, for the most part, to make recommendations. Today, due to their responsibility over data and expertise with data, intelligence organizations have the opportunity and responsibility to shape and transform reality. "Influence or shaping effort" in the period of The Human-Machine Team is a new opportunity for intelligence organizations. This mission includes intelligence for shaping reality, and not only for describing it.

The Digital Era, and specifically social media, have established a new reality in which facts and fake realities are blurred. Thomas Friedman described it thus: "I fear we are seeing the end of 'truth,' that we simply cannot agree any more on basic facts…what we are experiencing is an assault on the very foundations of our society and democracy, the twin pillars of truth and trust."[96] From time immemorial, people have attempted to

shape reality. Beginning in the Garden of Eden, Adam tried to "influence" God's thinking about what exactly happened. The development of media, and especially social media, dramatically augments the potential to shape reality.[97]

Today, anyone can be a sort of media station with his or her own smartphone. The ease of tweeting, posting, and texting made the "influence effort" a relevant part of the "act of war" as well. The influence or shaping effort also has the potential to be a decisive factor in victory or loss. The shaping effort in the period of AI can be much more relevant. For example, machine-learning can help create "influence in context," which means that different audiences and different individuals will receive the relevant data from the relevant media that has the greatest chance to influence them. This new concept also requires different people and cultures. Russia is an example of a country that is becoming more and more active in using data to influence reality. An extreme example is the accusation that the Russians influenced the 2016 U.S. presidential election with a data campaign that possibly included AI capabilities.

New Potentials and New Opportunities for Our Enemies and Rivals

The first risk is that our enemies and rivals will be a few steps ahead of us and will take the lead in this competition of artificial intelligence. The free world that led the Industrial Revolution has also succeeded in leading in cyberspace. The U.S. and U.K., as well as Israel, have achieved cyber advantage.

Currently, Russia and China have marked AI as a field in which they plan to lead on a global scale, and have invested resources to accomplish this goal. "AI is the future not only for Russia but for all humankind…whoever becomes the leader of this sphere becomes the ruler of the world." These resounding words, spoken by President Vladimir Putin in September 2017 to students on their first day of school, show why we need to keep at least a few steps ahead of our enemies and rivals in this field.

When we speak about cyber, the strongest capabilities are still "government capabilities." When we speak about AI, the greatest capabilities are in the private sector. Therefore, our enemies and rivals can be a few steps ahead by simply purchasing and utilizing the best systems from the private market. The key to addressing this risk is to create novel ways to collaborate between cyber capabilities and AI capabilities.[98]

We Don't Have 70 Years

As we discussed, the idea of artificial intelligence, which first appeared 70 years ago, has begun to change our lives only during the last few years. The development of the foundations (channels) for big data that enable us to use all of the data allows us to take the idea of machine-learning and create the conditions to fulfill the concept of AI.[99] Therefore, it is a risk for security establishments that it will take another 70 years to fulfill the concept of AI in their organizations. The factors that have changed, and now help us realize the concept of AI, have not yet been implemented in security establishments.

The first difference is the need for "channels" for a great amount of classified data. The second difference is the process of machine-learning that requires thousands of experiences. However, each conflict or war is a singular event, so we don't necessarily have relevant experiences for any particular war. The third difference is enemies who try to confuse the conditions and prevent the ability of the machine to learn from the past to make predictions. The risk here is that security establishments will become confused by the differences, and this confusion will prevent them from embracing the potential for the future.[100]

The challenge and the risk stem from trying to develop just "one floor" of the required changes without building all of the floors simultaneously. If someone tries to build AI machines without a systematic effort to first organize the data, it will fail. On the other hand, the data to be organized is infinite and the task of organizing the ground floor will never be complete. Therefore, the risk is that we will spend decade after decade organizing the data without taking our organizations to the future of artificial intelligence. In addition, each war or conflict is a singular event, but the data is not singular; therefore, we need to use the data to address the singular event and build models based on the data for the conflict/war, and not based on the characteristics of the event.[101]

From the Data Perspective: Unmonopolize on the Data

Traditionally, intelligence organizations have had a "monopoly on the data." Most of the relevant information is classified. The unclassified information is not useful without the classified, resulting in the intelligence organizations' monopoly on the data. For years, intelligence bodies avoided transferring information to operational entities out of concern that they would make improper or irresponsible use of it. Similarly, even within the intelligence community itself, the collection units did not transfer most of the raw information to the research units. This was supposedly done for reasons of compartmentalization, but also for practical and doctrinal reasons. According to the approach used in the past, if one provides access to raw visual information about complex decoding to everyone, they may make improper use of it and jeopardize sources. Making SIGINT (signals intelligence) information available to analysts was viewed the same way. In the Information Age, however, there is no ownership of information; it should belong to everyone. For comparison's sake, no one avoids making medical information available on the internet out of fear that, God forbid, I may make improper use of it if I need the information to treat one of my children. Basically, the information belongs to everyone, and anyone can ask whatever they want and decide whether and when to turn to an expert or make decisions by themselves.[102]

The monopoly of data creates difficulties during routine times of operation, but the difficulties intensify in times of

major crisis and war, which are based on the independence of the various forces. The ability to use data in war is based on having the independence to access it. The reality in which intelligence organizations have a monopoly on their data (and other military organizations do not have the data in their information systems) does not enable the effective leveraging of the data. It is an illusion to think that intelligence organizations know how to use the data for the other military organizations. As intelligence organizations, we have to say good-bye to the ownership and monopoly on data without diminishing the responsibility to keep the classified data as confidential information.

Continuity of the Data

In the DE, the capabilities to create the necessary manipulations and the intelligence investigations are based on continuity – that is, the continuum between the kinds of material, various kinds of information, and various intelligence entities. Traditionally, different kinds or types of information could be analyzed separately, and then a human analyst could try to connect them into one picture. This is also the idea of intelligence as a process of putting together a puzzle. Data science is neither a branch of SIGINT (signal intelligence) nor an extension of VISINT (visual intelligence); neither is it an updated way to do research. Data science requires, and is conditional on, continuity and the ability connect the dots of different kinds of data in one processing of the data. Furthermore, according to

this approach, even when there is 80% continuity in the data, there is a possibility that without continuity of the other 20%, all of the information will be worthless. This is because the real power lies in the ability to ask, and to clarify, the continuum as a whole. For example, we have to structure intelligence so that we can ask machine-learning questions according to the following formula: who a person is (1) who spoke to someone in Iran (2) and lives 100 meters from a suspicious place (3) and was observed during the past hour (4) driving north (5) and did not sleep at home last night. This query pertains to various kinds of sources. What is needed is the ability to manage and clarify investigations of this kind.[103]

"Targets Machine" – A Game Changer to Achieve Victory in War – Case Study (1)

From Data to Prediction

Machine-learning is a technology to learn through the big data that you have to generate the information you don't have. Machine-learning for manufacturing targets means discovering unknown places and figuring out thousands of new targets. A "targets machine" uses data to answer questions about your enemy's hiding places and to draw conclusions from data to make predictions. This machine has new potential to deal with big data that a human brain cannot do alone.[104] The process is built upon several steps, each one occurring after the other. The main steps are gathering data, preparing it, choosing a model, training, evaluation, hyperparameter tuning, and prediction.[105]

It's All About the Data

Nowadays, almost everyone is personally targeted by machine-learning – not to discover the location of your missiles, but when Facebook uses machine-learning to suggest possible friends. Basically, it is similar when we discuss the targets machine. *The first step* is the data. The machine needs enough data regarding the battlefield, the population, visual information, cellular data, social media connections, pictures, cellphone contacts, etc. The more data and the more it is varied, the better. Then, in *the second step*, the data needs to be organized in a way that a machine can access and process it. This includes the servers, the way in which the information is stored, and the ability to link between various elements of the information. The basis for everything is data. Without enough relevant data, without varied data, without preparing the data in a way that the machine can process it, nothing will be achieved. Many failures to build machine-learning have occurred because of problems with data. Data is the key to success. We can say that when we talk about the idea of "data science," the "data" are more difficult and more critical than the "science."[106]

Model

The next step is to choose and create a model. For example, the Facebook model shows how a machine can take the data and learn about potential friends. A targets machine needs to build a model to create new targets and figure out whether

or not they are manned. It can be a model that includes a few strong features based on classified data that enables the connections of specific pieces of information to specific places on the map. In addition, it can be a model that builds on a lot of small, diverse features – hundreds or even thousands of them. For example, people who are with a Hezbollah member in a WhatsApp group, people who get new cellphones every few months, those who change their addresses frequently, etc. In this example, the power will be from the quantity and variety of different features. The model can be built by analysts, and at least part of it can also be built by a machine.

The model will be more complicated. The best option is to build the model with a few strong features and with a large quantity of varied features. A strong model will then be created through a control group of targets that we know for certain already exist. Finally, after gathering the data, preparing and organizing it, and choosing and building a model, the first floor of the target machine is ready.

Training and Tuning

After we have a model, we can go to the *next level* of training and tuning. Training the machine involves checking the model and improving the machine. You can think of it like a runner who wants to improve his or her speed by studying running styles. After choosing a model to improve the style, he/she needs to train, using the model again and again. The importance of training is to check the model, improve it, and be more

precise. When building the targets machine, after we have the model of new targets, we can begin the training. We can take the model and start to check it again with the data. The training will help improve the machine, check if the features work, and find the relevant targets. During the training, we can improve the model's accuracy.

For example, this process can help understand whether the model gives more priority to picture patterns than to other features, and because of this focus, if there are mistakes. As a result of training, we can make small changes to a few parts of the focus or to the priorities of the model. When we finish the training, we have an improved model.

Evaluation

The next step is evaluation – which means jumping into the real world. Evaluation is testing our model with data that has never been used for training. The results never have 100% compatibility with the model. This step is first to determine if we have a good model for a targets machine – or not. Usually a 70% or 80% match is good enough. This step also helps improve the model, which is why the step after training and evaluation is tuning, specifically "hyperparameter" tuning. The testing in the real world helps to choose the hyperparameters and give them more weight in the model.

A targets machine can use the model with data that has never been used to check places and find new targets. The end of this step is the option for hyperparameter tuning. For example, if

we see during the evaluation that one feature is stronger than the others, we can decide to give this feature more priority. This is the second floor of machine-learning: training, evaluating, and tuning. Now, when we have data and the improved model, we can go to the final step of prediction.[107]

Prediction for a "Targets Machine"

Prediction is the step when the machine can begin to answer questions. For our example, we can put classified and unclassified data in the model, and the machine can start to think and suggest new targets. Prediction is when the value of a targets machine is realized. Agrawal, Gans, and Goldfarb in their book, *Prediction Machines,* give an amazing definition of prediction:

> "PREDICTION is the process of filling in missing information. Prediction takes information you have, often called 'data' and uses it to generate information you don't have."[108]

From their perspective, prediction is a fundamental ability of human intelligence, and prediction can generate information about the present and the past.[109] Usually, we think that prediction is for the future. For me, understanding that prediction is first of all about the past, and the present was a real "aha!" moment.

Usually, machine-learning takes place when there is data that we have that provides data or information that we don't

have. Only the activities will be in the future, but the conclusions are from the past or the present. A targets machine can learn from the data and the information it has about Lebanon and Hezbollah, and suggest new places where rocket launchers may be hidden.

The Human-Machine Team to Address Lone-Wolf Terror Attacks – Case Study (2)

Artificial intelligence also has the potential to influence the continuous campaign (sometimes called the campaign between wars). The Human-Machine Team can also influence the ability to find terrorists before they commit a terror attack. One major example of a type of crisis that intelligence organizations in Israel face is the phenomenon of "terror by inspiration," which takes the form of lone-wolf terror attacks. A potential terrorist wakes up one morning and decides to perpetrate an attack using a kitchen knife to stab a victim, or the family vehicle to run people over. Sometimes the person doesn't even know a day before that he or she is going to commit such an attack. In these cases, traditional intelligence agencies are helpless. How can such an attack be predicted or prevented? What can be prioritized as an essential piece of information to be monitored in lieu of something else?

Indeed, time after time we have found ourselves without a relevant, adequate response to lone-wolf terror attacks. The crisis was so severe in Israel that in October 2015 we found ourselves going from terror attack to terror attack and from

funeral to funeral. Each time we said to ourselves in retrospect, "Wait a minute! There must have been some sort of indication here that, if we'd paid attention to it, maybe the attack could have been prevented." As time went on and the intelligence units continued to be irrelevant, the sense of crisis intensified. We realized that the superiority[110] of the intelligence agencies to address terror attacks in advance was indeed being challenged. We understood that when it came to terror by inspiration perpetrated by lone wolves, the way we had done our intelligence work over the last decades was insufficient.

Since everyone has the potential to be a lone-wolf terrorist, it is impossible to check all of the people all of the time. A mission like this, similar to solving the Enigma Code, requires more than 20,000 analysts and more than 20,000,000 years. The way to tackle this complicated challenge is with a team consisting of humans and machines, and through the "bounces" and "passes" between this human-machine team. The first step is human. Humans must identify the limits and give examples of characteristics from past lone-wolf terrorists. Then humans and machines together need to formulate the characteristics of potential terrorists, using experience from the past to make predictions for the future. The next step is the prediction that a machine creates through the big data about specific suspects. Finally, humans check these suspects and decide how to act. This concept and process has helped us address these challenges and to prevent tens of lone-wolf terror attacks every month.

The Human-Machine Team for a "Smart Border" – Case Study (3)

A "smart home" is an everyday example of the new capabilities based on AI that are accessible to homeowners. A smart home uses various types of data in one specific place to improve the quality of our lives by using bits. Digitization creates the ability to represent, arrange, and process the real world through bits. The great jolt that changes our lives is the ability to take different kinds of data and transform them into binary digits. AI has the ability to take all these bits and use them within the context of a specific place, thus transforming a "normal" house into a "smart" house. The idea of a smart area is to use The Human-Machine Team to protect places such as our borders. The ability to connect the bits around the border through machine-learning can help control and protect them. (Another example is a "smart movable protected area" that friendly forces operating in enemy territory can utilize to better protect themselves from multiple threats.)

The basis for a smart border is the connection between the place and the person who does something in it (intentionally in that order, i.e., starting with the place). In the DE, one can fuse visual information and networked information in a given spatial cell. This fusion can deal with a warning, and in general help provide a different response to operational needs in a geographic context. The smart border begins with defining the space. Its starting point is the choice of the spatial cell we optimally want to reach (it could be across the border, or where

there is suspicious activity, etc.). Within the specific spatial cell, one must create the ability to fuse the various sensors within the context of the operational problem that has been defined. For this spatial cell, it is also necessary to organize all the data within the context of that same location. In addition, we must organize task-specific sensors, and attune an intelligence and operational entity to utilize the information of the smart space. All of these factors together can achieve an improved operational response.

We can begin to build a smart border by choosing a section of the border and building a proof of concept. The first step will be to organize all the data on this area: history, familiar faces in this area, geographic layers, etc. Second will be to organize various kinds of sensors to "control the area" – e.g., cameras, registering cellular identities, drones, etc. The third will be to build a system to connect the different types of data to each other; the fourth to design machine- learning to identify unusual phenomena and, lastly, to build an analyst group to deal with this machine and improve the smart border every day based on every experience.

PART 2

FAST

FOUNDATION,
ACCELERATION,
AND SINGULARITY TIME