perspectives. Are we going to take human lives based on AI? Are we going to attack a manned target (with people) just because machine-learning decided that this is the right time and place to attack?

# CHAPTER 5

## FAST – A New Concept

This purpose of this entire book has been to reach this moment. In this section, our purpose is to guide the first steps toward realization of the dream of AI. What should we do to fulfill the potential of The Human-Machine Team, and what are the requirements to lead our nations and organizations to the era in which human intelligence and artificial intelligence merge? Our plan is called "FAST": Foundations, Acceleration, and Singularity Time.

The future belongs to the nations and organizations that will build the relevant foundations that enable the AI revolution.[123] These *Foundations* are (1) a campaign to acquire more and more data, both classified and unclassified, as much and as varied as possible; (2) the ability to store and tag all the data based on cloud technology; (3) a closed-open-closed network that deals with the classified data and unclassified data in the same system and on the same network; and (4) to build strong, broad computer power (specifically, to build the foundations with enough

GPU servers to deal with a great amount of data).[124]

The idea of *Acceleration* means that no matter what happens, in 20 years our nations and organizations will possess substantial AI capabilities. Our responsibility is to accelerate the process and to bring (part of) the future into the present. Aggressive acceleration includes (1) empowering regional (edge) capabilities, which means choosing strong concepts and capabilities and empowering them by using AI; (2) automation of analysts' functions, e.g., automation to carry out tasks of image and linguist analysts; (3) automation of military hardware, including weapons, vehicles, and drones; and finally (4) collaboration between human combatants and robotics. Initially, these collaborations should be formulated in small units. The concept of *singularity time* means creating and establishing places (departments, units, organizations, and companies) that will focus on the distant future and on ideas that today seem totally unrealistic.[125] The purpose of this idea is to prepare ourselves for the future and help discover ideas from the future that will also enable the current acceleration of AI.

## "Who Are We in the Era of AI?" ("New Glasses")

We are the same people, but now we have "super-cognition." This means that challenges that were unsolvable in the past can now be addressed in ways that we could not have imagined before AI. The limits of cognition are changing, as are the rules.[126] We can and must check every issue also from the perspective of The Human-Machine Team. Cognition is one of the most important abilities to have created history. Therefore, when a machine can perform human cognition, it changes the potential for humans and machines to "think" together, thereby creating a kind of super-cognition. This revolution gives humans new glasses with which to look at every challenge, every concept, and every mission.[127]

## Key Questions

To discover how countries and superpowers are reacting to the AI era, we should ask ourselves a few key questions. The general, and most important ones are what we need to do tomorrow to fulfill the potential of The Human-Machine Team; what is our vision for AI; and how should we achieve this vision? In addition, we need to ask key questions to understand the potential between AI and other fields, such as: AI and cyber; AI and the electromagnetic spectrum; AI and the intelligence organizations; and AI and the relationship between national security establishments and the free market.

## Foundations

- Fulfill the requirements necessary to enable the AI Revolution
- Campaign to acquire more and more data
- Keep and tag all the data (cloud technology)
- A closed-open-closed network
- High-performance computing

Before we begin our journey to the future, we must understand that one cannot build a second and third floor without the first. A building without a foundation and without sufficient "sewer pipes" will be unlivable and can collapse. The first step to lead AI transformation (and the most complicated and important step) is to build a strong, stable, structural foundation for data. Until this system is built, we cannot begin the task of building the rest. This system needs to order the data and organize the relevant information. The data must be stored in the right places, but the aim is not to just appoint people to manage the information and be responsible for preserving it; the various databases must be connected and fused. In addition, we must decide which type of material will be preserved where, and so on. This begins by mapping what exists in the world, and what the data is in similar organizations and among us in our own organization. The process continues with organizing the relevant servers for this kind of data and crafting the organization's information strategy (which type of information is stored where, in what configuration, etc.). As noted, the importance of this step cannot be overemphasized. If one can invest in only one issue in the Information Age, it should be in the structure of the foundations of the information. Another way to convey the message is to note that in the data-science era, the data is even more important, complex, and challenging than the science.[128]

*Data* is the first condition (prerequisite) for building an AI machine. The more data you have, and the more variety you acquire, the better. National security organizations have access to the data in the public domain, as well as classified data that

only they possess. Therefore, national security establishments fulfill the condition of big data. In addition, the classified data itself is a great amount of classified and varied data; as a result, national security establishments have both the quality and quantity of data required to build AI machines. Data is the first foundation to lead this revolution, so our goal is more and varied data.

The second foundation is the *ability to store, label, and organize the data*. These abilities became a kind of non-issue in the free market, but they represent significant problems for national security organizations. These organizations deal with classified data, and therefore they don't want to expose their data in public clouds. Moreover, classified data is less relevant without the ability to merge it with unclassified data. The reality today is that national security organizations used to keep their classified data on private servers or private clouds, which means that they cannot take advantage of the capabilities of the public clouds that every individual and every company can enjoy. Furthermore, national security establishments have a considerable challenge to store, organize, and clean their data. In addition, it is a challenge to merge the classified and unclassified data as part of the same network.[129]

The third foundation is *high-performance computing*. During the last few years, high- performance computing has improved the ability to address large amounts of data, and therefore improves many organizations in the free market. High-performance computing is a resource lacking in national security organizations.

In addition, we must have *data analysts* to address the data. A data analyst who focuses on the data (which kind we need, how to use it, on which servers, etc.) is a new position both in private companies and in national security organizations.

The bottom line is that the first step is to *fulfill the foundations that will enable the AI Revolution.* This step includes (1) a solution for storing and organizing all the data; (2) a continuous campaign to acquire more and varied data; (3) the ability to enable merging classified and infinite unclassified data. For this merger, we must build the national network as a closed-open-closed network. As discussed earlier, closed for classified data, open to connect the classified and unclassified, and closed after the classified and unclassified data is merged; and (4) to invest enough resources to ensure that high-performance computing is a non-issue. The first step towards achieving high-performance computing is building the capacity of GPU servers in the security establishments. [130]

For comparison, we can look at the following table; it compares the current preparedness of national security establishments to fulfill the AI Revolution and the ability of the free market to implement it.

| | Industry + Free Market | National Security Establishments |
|---|---|---|
| Data | ✓ | ✓+ |
| Ability to Store and Organize the Data | ✓ | — |
| High-Performance *Computing* | ✓ | ✓ |
| Merging Classified and Unclassified Data | ✓ | |

* The combination of cloud technology and artificial intelligence creates a new potential, and many AI innovations are a result of this combination. Therefore, if national security establishments will jump into the cloud revolution, the new potentials for AI innovations will become huge new potentials.

**The Infrastructure to Enable Automation**

Historically, our infrastructure was built for humans. One of the big challenges to lead transformation for automation is the infrastructure. In the near future, there will be autonomous vehicles, autonomous drones, and autonomous robots. The problem in using all these autonomous machines will be the infrastructure that in the past was built for humans, and not for machines. Therefore we need to improve infrastructures such as our roads, gas stations, electromagnetic spectrum, and many others, with the view towards building foundations to enable AI automation. Nation-states that begin to address these challenges now can lead the automation field in the future.[131]

**"Made in China"[132]**

China decided that AI is a new paradigm for ruling the economic market as well as a core element in the competition between China and the U.S. China's vision is that AI has the potential to be a game changer that will take China into the future and lead the world. Therefore the Chinese are planning to accelerate the different fields of AI as much and as far as they can.[133] China is an example of a country that focuses on building foundations for AI with a high priority on data.

The Chinese plan includes four main efforts to develop the relevant foundations to lead the AI era.[134] The *first* step is that the Chinese government has allocated tens of billions of dollars for AI.[135] Their *second* decision is the creation of a new commission of Military-Civil Fusion that is responsible for improving the collaboration between the military and the private sectors. They understand that due to the AI era, China needs to build a new concept of the relationship between the two sectors, including a new concept for AI acquisition. This understanding led to the creation of a new commission that is similar to DARPA (Defense Advanced Research Projects Agency), which focuses on AI and on building bridges

between the military and the private. The *third* and most important decision is to leverage China's lower barriers for data collection in order to create large databases that will "feed" AI systems.[136] From their perspective, the most important asset in order to lead the concept of AI is data. China intends to collect and organize as much data as possible. According to one estimate, they are on track to possess 20% of the world's share of data by 2020, with the potential to have over 30% by 2030. This effort reflects their ambition to achieve a monopoly on data.[137]

*Fourth*, China decided to actively promote the idea that Chinese people should invest and work in American artificial intelligence companies. They believe that a good way to win the race between the U.S. and China is to copy American innovations, especially by Chinese working in Silicon Valley and in other AI companies and universities throughout the U.S. From China's point of view, the strongest power of AI is in the free market, and not in military organizations. Therefore they need to be inside the U.S. private sector and then bring the employees and their knowledge back home.

**Acceleration**

- Aggressive acceleration
- Empowering regional strength
- Automation for more and more actions
- Automation for weapons, vehicles, drones, etc.

## AI Capabilities to Empower Regional Strength

The era in which human intelligence and artificial intelligence are merging enables us to choose our strongest capabilities and empower them using AI. For example, we decided to call cyber a new domain and to establish a "Cyber Command." So should we now establish an "AI Command?" Our answer is that in the near future, AI will primarily be a way to improve and empower our strongest current abilities. Therefore, a few examples for using AI to empower regional strength are (1) using AI to improve our capabilities in the cyber domain (offense and defense); (2) using AI as part of our border security; and (3) using AI to create a large amount of "targets in context."[138]

## AI and Cyber

Cyber is the fourth battlefield domain (air, sea, land, and cyber). Cyberspace is a domain that enables attack and requires defense. In addition, it is a domain that enables varied types of actions to influence reality through data. Russia, China, and the U.S. have all decided that one of their main AI efforts will be to increase cyberspace capabilities. Their decisions include using AI to improve the ability to build cyber-attack tools; to improve defense capabilities to find new viruses; and to enable attackers to find relevant files in their rivals' and enemies' networks.[139] For example, China is developing a department of AI tools for cyber-defense and cyber-attack. They believe that cyber is a strong domain in China and that AI is a relevant innovation

that can empower their cyber capabilities. As a result, China decided to establish a new unit that will focus on cyber and AI to enable the acceleration of this specific new ability.[140]

## Machine-Learning and Cyberspace – A Case Study

In cyberspace, there are myriad viruses and cyber-attack tools that can act against your network.[141] There is no option to "clean" your network of viruses. Viruses mutate all of the time, and viruses create new viruses. In addition, there are people and computers that want to attack your network for different reasons.[142] One of the challenges is that even when a cyber-attack tool is caught, it is still possible for the cyber-attacker to alter this tool a bit and to use the new version of the virus to attack again. For that reason, we don't have any choice in cyberspace. We are required to deal with viruses and cyber-attack tools 24/7. The mission is not to clean the network, but rather to build our network with the ability to "live" with some viruses and to choose which of them we need to totally destroy.[143]

## Recruiting Effort for Machine-learning to Solve the Problem

Machine-learning has the potential to deal with infinite data; it can even identify cyber-attack tools from big, known data and discover new cyber-attack tools that were previously unknown. Additionally, it can learn through past viruses how to discover potential new viruses. Machine-learning also has the potential to make predictions about new viruses and new cyber-attack tools in a way that a human brain cannot do alone. As we discussed, there are three main floors that are required to build machine-learning to solve this problem: (1) we need data to build a model to suggest the new viruses or new cyber-attack tools; (2) training and tuning to improve the model; and (3) making predictions and using the model to improve our defense in cyberspace. It is important to realize that machine-learning can also help cyber attackers create new viruses that will be difficult to detect.

### The First Floor – Data to Create a Model

The first floor is data to build a model. The basis for machine-learning in this case is data regarding viruses and cyber-attack tools from the past. The data needs to be as big and as varied as possible, including data about the viruses, their characteristics, the ways they try to "hide," and so on. When we have enough data, we need to prepare and organize it in a manner that allows the machine to work with it, including the servers, the way in which the information is stored, and the ability to link between different parts of the information. The last step for this section is building a model. For example, a file or code that looks like "x" has great potential to be a new virus. Building a real model is both complicated and challenging.

There are at least two ways to build the concept for a model. We may choose strong features, and if these features exist, there is a good possibility that there is a new virus. Another option is

building a model that is based on a quantity of features (hundreds or even thousands). This model will be robust because of the quantity and variety of features. The best option is to build the model with a few strong features as well as with a large number of varied features. A robust model should be created through a "control group" of viruses that we know for certain are dangerous.

### The Second Floor – Training and Tuning

Once we have the model of the suspect viruses, we can begin 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 suspicious viruses. During training we can improve the preciseness of the model. For example, the model might give more priority to "shape patterns"[144] than to other features, and because of this focus, there is the potential for mistakes. With training, we can make small changes to a few parts of the focus or to the priorities of the model. When we finish training, we have an improved model. Then with the data and the best model, we can apply it to the real world and check this model with new data and see the results.

### Third Floor – Evaluation and Prediction

This is the time for evaluation. We can use real data and real experiences, like the machine-learning is going to encounter at the end of the process. For our example, we can use the model to discover new viruses with new data. The end of this step is the option for hyperparameter tuning. For example, if during the evaluation we see that one feature is stronger than the others, we can decide to give it more priority. Now, when we have data and the improved model, we can go to the last and final step of prediction – putting the model on the machine – and the machine can begin to identify and suggest viruses and cyber-attack tools.

### Borders with an "AI Wall"

Defending our nations' borders is a challenge that has become more and more complicated. The wall between the U.S. and Mexico, and the underground tunnels that Israel faces along its borders with Gaza and Lebanon, are just a few examples of these challenges.

The Human-Machine Team enables a new potential to use AI to build a "smart area" for protecting borders. The ability to connect various bits around the border through machine-learning can help control these areas and protect the borders. The smart area is required to define the location, to organize the relevant sensors in the context of the operational problem, and to prepare the "channels" of the information in the context

of that same location. In addition, we must organize a team to utilize the information of the "smart space." All of these factors together can achieve an improved operational response. When we implement this concept, we will succeed in building an "AI Wall" to empower our efforts and improve security along our borders.

### Russia and the Idea of Acceleration

We have already mentioned President Vladimir Putin's "AI is the future. 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." This was a signal to several sectors in Russia (including the government, universities, industry, and the general population) to focus on the field of artificial intelligence. From the Russian perspective, AI is a main area to help the digitization of their economy. In addition, military power is an aspect of Russia's grand strategy, so AI is also a part of its warfare planning. Traditionally, Russia has had challenges in taking their amazing ideas from concept to the development of real, new technologies. They are trying to change this basic situation with an internal focus on artificial intelligence.[145]

The Russian vision for the next few years is to realize Putin's resounding words by *accelerating* the capabilities of AI in Russia. Their ambitions are to *empower the self-respect* of the Russian people, to *improve their economic situation* and *GDP*, to *reverse the technological brain drain* from Russia to places like Silicon Valley in the U.S., and to build *control systems* based on AI. In addition, they want to develop AI as a relevant *strategic tool* to address allies such as China, and as part of their efforts against rivals and enemies. For example, in its efforts in Syria, Russia takes more and more steps to improve its military capabilities in the arena by using artificial intelligence.

### How Does Russia Plan to Realize Its AI Vision?

In order to achieve these goals, Russia has built a *road map* that includes five core steps. The main concept is to take specific issues and accelerate them by using AI. For them, acceleration means achieving new abilities as fast as they can, and forcing the nation and organizations to improve their foundations to enable this acceleration. *First*, Russia decided to build AI capabilities to empower their regional strength. This means developing AI in their propaganda, in their "fake news" efforts, and in the electromagnetic spectrum, and as part of cyberspace. *Second*, they decided to focus on robotics and automation, including the automation of large vehicles such as tanks. The goal that the Military Industrial Committee set is to succeed in achieving a reality in which 30% of Russian military equipment will be robotic and autonomous by 2025. *Third*, to support these transformations, Russia is investing hundreds of millions of dollars,[146] and they are developing new, professional AI departments in universities and institutes in Russia. In addition, they decided to create a defense research organization, roughly equivalent to DARPA, dedicated to autonomation and robotics, called the Foundation for Advanced Studies.

*Finally*, they are trying to improve the relationships between national organizations and the private sector to help keep the Russian "brains" inside of Russia.[147] For example, Kryptonite is a Russian company that works on creating "civilian IT products based on military developments in information security, including blockchain." Specifically, Kryptonite's work involves "cryptography, machine-learning, big data, quantum computing, blockchain, and the security of telecommunications standards."[148]

### "Singularity Time"

*Singularity time* is thinking and establishing places (departments, units, organizations, and companies) that will focus on the distant future and on ideas that today seem totally unrealistic.[149] It also implies starting to build our organizations using concepts from the family of general AI (and not only from narrow AI). As previously discussed, general AI – sometimes called Artificial General Intelligence, or AGI – is a machine that can replace an entire human being, or at least has the level of cognition that is equivalent to that of a human. General AI refers to a notional future with an AI system that exhibits intelligent behavior, feelings, and context at least as advanced as a person, across the full range of cognitive tasks. General AI is in contrast to narrow AI, which refers to specific capabilities and not to the whole system.

The purpose of this idea is to prepare ourselves for the future and to help discover ideas from the future that will also enable the current acceleration of AI. Moreover, this concept includes the necessity of building basic infrastructure foundations, such as roads and highways, that will facilitate the use of autonomous vehicles.

### Next Generation Unit

"Good morning, car. Please take me to my office." This is an AI reality that can be achieved in the near future. The day the car answers, "No, I decided not to drive you today" will be a singularity moment. The situation where one morning a machine will decide to attack a target "for its own reasons" is an example of a singularity moment. In this example, the AI machine has intelligent behavior, feelings, and context that are at least as advanced as a person's, across the full range of cognitive tasks.

We cannot imagine the future of AI in 2040, 2050, or beyond. Personally, I believe that the concept of a self-aware "Terminator" robot is unrealistic and will not be part of our lives. However, today it is important to establish a unit in national security establishments whose responsibility is to build tools for the distant future. This pioneering effort will help us take responsibility for the future, create the future, and be prepared if such a singularity time does arrive. Finally, the unit will have the option to dream without limits, which will help broaden today's narrow AI capabilities.

One way to take responsibility for the future is with "singularity time labs." The idea of these labs refers to establishing new labs with the idea of focusing on the distant future and

on concepts that today seem totally unrealistic. Culturally, the labs need to be under the umbrella of a few big universities; in addition, there need to be government labs, financed by government bodies such as the Department of Defense, and at the same time have environments similar to and connections with new startups.