CHAPTER 4

Challenges and Difficulties

Today's nations and organizations were developed with characteristics and culture that matched the Industrial Revolution. However, the DE is a novel, high-level paradigm, and because of AI, we are on the threshold of the acceleration of the DE Revolution. As a result, nations and organizations need to adopt a digital transformation strategy for this era.[111] This transformation is a huge challenge. The future belongs to nations and organizations that will succeed in dealing with the new challenges and difficulties that arise due to the era of AI.

In this book, we focus on the structural and cultural challenges for digital transformation in the security establishments. The first step is to address the challenges for digital transformation that organizations in various fields of interest are facing today.[112] Furthermore, there are additional, unique challenges for security establishments, for which there are at least three reasons: 1) the culture of the security establishments; 2) the characteristics of the security mission; and 3) the necessity to

use infinite amounts of classified and unclassified data at the same time.

Intelligence organizations have unique challenges because they have a responsibility to deal with both "the secrets" and "the unknown." Information and knowledge are at the core of intelligence organizations. In addition to their internal work, these organizations also need to communicate with all branches of the military and with other intelligence organizations. To complicate matters, all this communication goes on at the same time on the same network. As a result, intelligence organizations have built-in challenges to achieve digital transformation. It is challenging to be part of the military network, guard the secrets, and deal with the unknown all at the same time. Despite the challenges, intelligence organizations must pursue and succeed in their digital transformation programs. Those that do not succeed at this will also fail to accomplish their goals.[113]

Six Unique Challenges

The first and most complex challenge is to build a "closed-open-closed" network. Is it possible to develop a closed network that is actually an open network at the same time and on the same network? Such a network is, on the one hand, a closed network that nobody outside the system can access, and on other hand it behaves like an open network to access the entire internet. In other words, closed to the outside world for classified data, open for the security organization to connect

the internal classified data and the external unclassified data, and closed after the classified and unclassified data are merged. A further advantage of this system is that every member of the organization can also use his or her private smartphone to access the internet. For a day-to-day example, we can ask how it is possible to build a network in which someone who works for a security organization can take a picture with his private smartphone, send the information to the classified network, and merge it with the classified data. (In this example, the network must be open to send the picture and then closed due to the classified data.)

A closed-open-closed network means to enable infrastructure to build machine-learning in such a way that part of the data will be public from the internet, and part of it will be classified information that is not on the internet. The machine can then use the different types of data at the same time. Such a network means that the private classified cloud and the public cloud can communicate with each other all the time without the user experience being compromised. A closed-open-closed network means that security organizations can operate from public places such as WeWork,[114] and at the same time use an internal security network.

It is necessary to build a closed-open-closed network so that security organizations can continuously and simultaneously deal with classified and unclassified data as part of their daily routines. Today, most of the information and knowledge that security establishments need to operate on a daily basis is unclassified. However, the classified data is critical. More often

than not, the infinite amount of unclassified data is irrelevant without the classified data. At the same time, the classified data may have substantial gaps without the unclassified. Some security organizations simply copy information from the internet to the internal network, but this provides only a partial solution that leaves large gaps. Today, the ability and the potential for people and machines to reorganize the different types of data is a required condition to successfully address security challenges.[115]

The second challenge is the requirement to build a cloud for a large amount of classified data. In the past, we did not have enough data. In the current reality, due to the Information Revolution, security establishments also have big data. Since a lot of this is secret, security organizations use private servers. However, to deal with all the data, we must migrate to the cloud. Today there are clouds for a great amount of data only in companies such as Amazon, Google, or Microsoft.[116] How can the security establishments use the "Amazon cloud" and feel secure? How can this public cloud communicate regularly and securely with a private cloud? The foundations of the information infrastructure are the unseen, yet indispensable sewer pipes (the channels for data) that – if compromised – make the neighborhood unlivable. Clouds are an important component of this information infrastructure. Without a good solution for clouds, and without a systematic and thorough treatment of the "channels," digital transformation in security will fail. In other words, without the ability to store the data (including classified data), and without the ability to use this data easily for various

missions, nations and organizations will not successfully make the AI Revolution real. The decision of the CIA to work with the Amazon cloud is just the first step.[117]

The third challenge is the fact that in the security establishments, different organizations use different networks. From time to time, different departments in the same organization even use different networks. For example, the Air Force uses a different network than the intelligence agencies, the Army uses a different network than the Navy, and so on. It is difficult for organizations to give up using their own private networks, since a network is the basis for an organization's independence. Today, a good network is a condition for success. Usually, organizations feel that they cannot trust anyone from outside their organization to build and operate their network. Consequently, how can different organizations with different networks feel and act like they have the same network? How does the concept of the "flat world" manifest in security organizations that have different networks, and where every organization has its own secrets?[118]

The fourth challenge is due to the mission. How can security establishments achieve this complicated, challenging transformation and at the same time be prepared for war? How can security establishments reach the next high-level paradigm and at the same time be prepared to achieve victory in a war that is based on the existing paradigm? One of the main characteristics of a military organization is the responsibility to be prepared for war at all times, 24/7. The possibility that a war may erupt at any given moment makes preparedness the top priority.

For example, the Second Lebanon War that Israel fought against Hezbollah in 2006 broke out when the IDF was in the middle of transformation. Therefore, along with many achievements, difficulties broke out during the war, owing to the fact that it broke out in the middle of this transformation process. The IDF had one foot in the past and one foot in the future, and thus there were challenges. In the public market, when you build the next generation, the previous generation continues to behave as it behaved before, and you just stop training to improve the old model. For example, when Apple works on the next generation of the iPhone, the previous iPhone continues the way it worked before. However, in the military, we need to build the next generation and invest time and money for this purpose, but at the same time we must be prepared for the supreme test of war. It is a huge challenge to take your organization to the future, while simultaneously improving your preparedness to win a war that can erupt at any minute. Part of this challenge is that you need to keep and utilize your previous abilities while transforming the organization for the use of next-generation abilities. Finally, it is very difficult to dream up the innovation, do the transformation, and improve your preparedness in the same organization with the same resources.

The fifth challenge is due to the organizational DNA of the learning process in the security establishments. Digital transformation means taking your organization into the future. It also means taking advantage of new opportunities that the DE provides. Historically, national security establishments learn,

first of all, from crises. An effective way to learn in military organizations is from a turning point. These organizations do not usually learn from potential opportunities to succeed, which is usually the normal process in the private sector. Security establishments are constantly in the process of addressing big challenges; in addition, they are usually hampered by a lack of resources, which is the reason that it is so difficult for them to invest money based on abstract issues for which they do not know exactly what the return will be. This is especially difficult when security establishments have concrete issues and emergencies to which they must allocate their precious resources.

This is but one of the reasons that most of the changes in security establishments take place only after crises. In addition, it is difficult, if not impossible, to conclude that the crises arose as a result of data. Information is everything – and everything is information. Since information is everything, it is hard to identify the crises that occurred due to problems around data infrastructure. The bottom line is that security establishments are used to learning from crises, and it is challenging to understand that there was a crisis because of data.

The sixth challenge is the cultural challenge to use outsourcing capabilities before inside abilities. Over the last few centuries, security establishments used to be the "No. 1" source to develop weapons and invent military capabilities. For example, the U.S. Air Force is also the force behind the acceleration of airplanes for use in the private sector. The best airplanes are always in the Air Force (companies such as Lockheed Martin and Boeing are a kind of "inside ability," because even though

they are considered industry, the company "in essence" is part of the U.S. security system). In the digital fee, it is just the opposite. The free market will always have much more money, data, experience, and manpower to enable it to be at the forefront of digital technology.

In digital transformation, outsourcing capabilities are crucial. For digital capabilities in the security establishments, the concept of outsourcing needs to be like the concept of "inside abilities." Typically, security establishments use outsourced capabilities for approximately 20% of their products and required capabilities; to succeed in the Digital Revolution, they need to use outsourcing capabilities for 80% of their products and outputs. The bottom line is that national security establishments traditionally use "inside units" before "outside companies." To deal with this challenge, we must change our culture.[119]

Three More Challenges from the Perspective of War

A war is a singular event. By contrast, machine-learning is a continuous process that is based on the ability to learn through big data from both the past to the future.[120] The process of machine-learning is built upon several steps, each one taking place after the other.[121] During war, however, everything changes. In addition, the desired outcome is not to lose the war and then to prepare for the next one by learning from the defeat. New data will be acquired during war, and obviously we cannot gather and prepare for data that we do not yet have. The ways the enemy will act during war will change, so it is

also impossible to choose a model based on experience from previous wars and use it during a current war. Is there a way to use AI in a singular event?

The mode of operation in war reveals an additional challenge. How can we "run the war machine" when there is a "monopoly on data" and a "monopoly on firepower?" Intelligence organizations have a monopoly on the data; most of the relevant information is classified, and the unclassified information is not useful without the classified. The result is that this monopoly creates difficulties during routine times of operation, but the difficulties intensify during a crisis (or war). War is based on the various forces acting independently. The ability to use data in war is based on having the independence to access it. The reality that intelligence organizations have a monopoly on their data (and other military organizations do not have the data in their information systems) does not allow the option to leverage the data in these other organizations. It is a delusion to think that intelligence organizations know how to use the data for other organizations. The second part of the problem is the monopoly on the firepower capabilities effort.[122] For example, there are capabilities that only the Air Force has, and only those in the Air Force have the responsibility and the ability to use them. The reality that other organizations have a monopoly on the data, and a monopoly on the "fire," precludes the ability to use the data in all of its power and realize its full potential.

Finally, when we address life and death during war, we must take into consideration the legal aspects as well as the ethical

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