MEIR SHEETRIT

Former Member of the Knesset, former Minister of Intelligence Affairs and the Committee of Atomic Energy, former Minister of the Interior

Thomas GOMART

The floor is yours.

Meir SHEETRIT

Thank you very much. I would like to explain in very simple words what is going on in cyber. As our moderator said, six years ago in Monaco I participated in a session about cyber, in which I explained the threat of cyber, and the bad news is that situation came to be much, much worse. If I told you at that time that you have to take into consideration that whatever you write on your iPhone, SMS, your calls, anything, no matter where you are, everything could be seen by anybody who makes a little effort. Now not only can they do that, they can even reverse your phone in order to take pictures from wherever you are because they can reverse the camera. They can take pictures from your camera of where you are and listen to you. It does not matter where you are, in a meeting, at your home, they can listen to you from far away. I wish, Thierry, that I could once have the opportunity to bring a company from Israel which demonstrates to people here in this room that they can control any phone in the room. They do it for volunteers only. They show you that they can see anything you do in five minutes.

I am trying to explain what has happened in the last six years. The computer system has made great, rapid progress. It is really unbelievable how fast it develops. There is a graph that shows what happens to computers. It is called Moore's Law, and to simplify it Moore's Law says that, as a matter of fact, as you can see here the simplified version of the law states that the processor speed or overall the processing power of computers will double every two years, so since 1960, when this law was introduced by Moore, the computer power has grown 50 billion times. This is a fact. That is what I showed before. In a modern car today – your cars – there are more than 100 chips. The power of computing of my iPhone today, or your iPhones, is greater than the power of the Apollo 11 spacecraft program computer. This shows you that things are changing very, very fast.

Now, what happens as a matter of fact in the world in computing? In the past the infrastructure systems were not computerized. In matter of fact people did not think about it and the only way to harm those systems or to touch them was by direct attack. If you wanted to ruin, let us say, a nuclear power plant you would have to go there and bomb it. You could not do it in any other way. It was especially the same way with the electrical system, electrical power stations, a water way, whatever you want, anything. Today things have changed because of computerization. Then most countries did not computerize their systems, but since 1980 it was the beginning of various system-computing in the world and the infrastructure system in most countries has been computerized. That includes banks, government systems, government agencies, data, telephone exchanges. Today almost everything is computerized.

When everything had been computerized it created dependence between people and computers, and the bad guys said to themselves, 'Now if there are so much data and so many possibilities why can't we use it for our benefit?' That is how the cyber started. Since they digitalized the telephone exchange and the records of institutions, the bad guys started to work and develop as a matter of fact cyber.

Now, what is cyber? The dominant technology of the century is computing, so cyber is computer against society. That is what cyber means, which means people using the computer systems in the world against the people themselves for their benefits. As they say, the extortion, to attack other places, to spy, to do anything else. Until 2010, only the intelligence services of the world were aware of cyber. Nobody cared. Until 2010, nobody cared about cyber. There were several countries, only around 10 – Israel was one of them – that began to concern themselves about cyber. Looking at Israel, Israel's computer warfare unit was established in the intelligence of Israel only in 1993. That was the beginning of taking care of cyber.

It should be remembered that until 1995 every country was developing different computers. There was no standardization of computers. Only in 1995 they started to make standardization for all the computers. It created a lot of problems to those who were fighting against it because you have to learn every computer separately, how it works, how it was built, how you can attach it, etc. When it became standardized it made life much simpler for everybody.

Only then in 2002 because of the development the ISA, the Israel Security Authority, established the NIS, which is National Infrastructures Security, which meant that Israel decided we are not leaving our infrastructure to be attacked by other people or by other countries. Listen to this: today one boy of 20-22 years, which is good in cyber, is much more powerful than a full army. You do not need tanks or aircraft or missiles to make total chaos and destruction of a country. You can do it from your keyboard from home if you have the ability. Things have changed in the world in how one looks at dealing with problems or with attacks. Because Israel has something like 100,000 attacks per day in regular days – in time of war we have one million attacks per day – Israel had to be one of the best. Otherwise we cannot survive. Therefore, we have to develop our power of cyber very, very strongly.

In 2010, the Stuxnet worm was published worldwide. Do you remember? The world turned upside down. Why? Because suddenly somebody from far away ruined all the centrifuges of Iran, preventing them from enriching uranium. This was done from far away. Nobody has been there. Nobody touched it. Nobody attacked it, and still they ruined all the infrastructure of Iran for producing, for enriching uranium. I am not saying who did it because we are speaking about it… It was the United States. It means that physical damage had been done, but nothing had been stolen. It just showed the world that it is possible to act from far away.

Therefore, Israel decided to make an ecosystem which really would take care of all the problems concerning cyber and really it went very strongly. It means giving budgets to research for universities, for industry, for people, putting hours of study in cyber in high schools, supporting all the system, managing it, synchronizing it in order that everybody will know what anybody else does, and it really works quite well. I must just bring you some data about this in Israel. It is data which is very, very interesting. For example, Israel's export of civilian goods and services in cyber was 7 billion dollars this year, which is 8% of the global market of the world. Israel is just 0.1% of the world. Investment in the cyber business sector in the world is very large. Of this total investment, development center venture funds, etc., 18% comes to Israel because Israel is considered to be one of the very strong center of cyber. Between 2012 and 2018 cyber products growth in Israel was 600%. We were not the first in the world, but among the first, but we were the first to take cyber out of the closet to show it to the world.

I have two more points. The Snowden affair is the first one. The Snowden affair exploded in 2014/2015. When the Snowden affair came out it automatically created very high tension between security and privacy because what Snowden published was the fact that the United States was following everyone, reading all their mail, everything else, and they know this information, and this created disbelief in governments. Therefore, in order to solve this problem in Israel, as we suggested, Israel suggested and established a separate unit based on three principles. The first one is in a modern country the intelligence agencies will not track civilians. The second established a new civilian body which does not belong to intelligence because civilian corporate is needed. The third is the body will not belong to law enforcement.

If you really want to protect your people in your country from attacks of outside, how do you do it? Even if you create such a unit, you cannot read all the mails. You cannot do so today. In the future you will not be able to read the mail, we will do so using artificial intelligence – AI – and machine learning, which I will just describe generally. Suppose there is a machine that reads all the Internet transformation in Israel, anything, very fast, immediately, in a very, very rapid system, and then popped out only those e-mails or things that create some suspicion. Those are transferred to the bodies to be detected. Otherwise you do not feel it, so it could be done, and that is exactly the last one, the future: looking ahead, the ability to protect the network can only be done through artificial intelligence and machine learning.

Therefore, in the world today there is a lot of competition in this area and countries are investing billions, hundreds of billions of dollars, in order to develop what we call quantum computers. I will not enlarge on quantum computers, but just to give you an example, Google has published lately that they succeeded in operating a quantum computer with 53 qubits which made a calculation within 200 seconds which would take the largest computer in the world at NASA 10,000 years to calculate. Why 200 seconds? Because that is the only time they can really hold the quantum computer

to work, but it is a matter of time until they create a quantum computer which will hold on. When that happens the sky will not be the limit because everything in the world will change, including your life. Thank you.

Thomas GOMART

Thank you, Meir.