MEIR SHEETRIT

Member of the Knesset, former Minister of Intelligence Services, Israel

Good morning. I am glad to be here. It is wonderful to be with you again on this panel. You have heard about some of the benefits of the Internet. It makes our lives much easier and much more comfortable. It gives us more access. I would now like to give you some of the downsides to the Internet. The modern battlefield has been changed drastically. The battlefield today is not only a matter of aircraft, tanks or infantry. Cyber war is now an aspect of warfare. Since the mid-1990s we have seen this type of warfare. The two goals of cyber warfare is, firstly, to paralyse sites and to leave a signature in those sites in order to show you that they have been there, that you are vulnerable and they can get in whenever they want and do whatever they want and, secondly, to damage infrastructure.

In the second Lebanese War between Israel and Hezbollah there were a lot of hackers making strong attacks against Israeli sites. In response, many Israeli hackers attacked Hezbollah sites. We saw the damage to both sides in real time. In order to make a state collapse these days you do not need to conquer it or to physically attack it with your army. You do not need tanks. You do not need airplanes. All you need is a computer and a keyboard. We are not far from that being possible. In the summer of 2007 Estonia was attacked by hackers, most likely Russians, and the state collapsed. Their infrastructure collapsed. Their communications stopped working. Their banks and electricity were shut down. That was just one demonstration of what can be done. With cyber war you can paralyse a state.

One of the aims of hackers today is to have such control over the state that they can make money through blackmail. They can threaten to paralyse a state unless they are paid off. It would make someone very powerful to be in that position and it is not impossible. Part of the aim of those hackers is to have sufficient control over states to be in a position to extort money from them.

I would like to share with you some of Israel's experiences with cyber warfare and how we are approaching it. As you know, we live in a very difficult neighbourhood. I want to share these experiences with you because I think you need to take it into consideration in your countries. We established the INCB, the Israeli National Cyber Bureau, a few years ago. It was only formally established by the government in 2012, but we actually started establishing it five or six years ago. There are many organisations within this bureau and many units throughout the security services and Defence Ministry. All of them are under the authority of the Prime Minister. I will try to explain why.

It is not only a matter of defence because if it was only a security issue all of those units would be in the Defence Ministry. As I said, there can be a lot of damage done to throughout your infrastructure. Therefore you need to protect those infrastructures. To successfully protect them it is not enough to have a small number of people with that task. You have to cover a very large system, which means you always need to prepare your warriors to protect your Internet, your sites and your infrastructure. You have to develop new technologies on an ongoing basis. In order to do that you need to carry out research. In order to have the right research you need to have lots of students who study physics and mathematics at a very high level. You have to take care of many systems in your country in order to have defensive and offensive capabilities if you need them. That is the reason why we put it under the authority of the Prime Minister because you need somebody with enough power to move those systems ahead.

What are the main traits? As I said, one of them is the protection of the government's IT. Every government has e-government sites that people can use to access various government services. If somebody attacks those sites they could paralyse the operation of these government services which people rely on. Secondly, there is the protection of the main infrastructure. These days most infrastructure elements are controlled by computers and if you can gain access to those computers you can do whatever you want in those systems. For example, if you were to take control of the traffic light system in a country. You could change them however you liked. You could put all of them to green. It would be a disaster. It is quite a simple thing. You could also totally paralyse all electricity production in a country if you gain access to the computers that control that country's electrical power plants. The same is true of nuclear power plants. If you can gain access to the computers that control them you can cause a lot of damage.

Protecting this infrastructure is crucial for states to keep their systems operational. That is why we have established so many units with this objective. There is a unit in the Ministry of Public Security which has the responsibility of protecting the main infrastructure connected to and controlled by computers. Special units have also been established to protect our e-government sites from attack.

You have heard of course about the Stuxnet worm that attacked Iran's centrifuges. It was a very, very complicated virus which caused a lot of damage to Iran's centrifuges when it got into them. It took two years for the Iranians to find out about this worm or this virus. When a virus is used in an offensive way, such as that, there is a question as to how the attackers prevent the virus from going back into their own systems. For example, in the case of Stuxnet the virus was so sophisticated that it acted only in certain types of centrifuges that were only used in Iran. The virus would not work if it got into different types of centrifuges in other countries. When the Iranians found it they sent it to a laboratory in Russia and the Russians investigated it and revealed to the world that the virus existed.

I give that as an example because there are no computers in centrifuges. Centrifuges are just mechanical machines with electrical engines which turn them very, very fast, but centrifuges are supervised by computers. If you can get into those computers therefore you can cause a lot of damage to the centrifuges. That is what happened in Iran.

What are the main traits of cyber warfare? The main traits are to attack the major infrastructure elements of a country such as the water supply, electricity, transportation, banks, the stock market, communication and so forth. You can really attack everything and totally paralyse a country. Stuxnet is one example of a cyber war attack. I would like to give you some more examples. In 2007 the attack on Estonia was explored, as I said before. In June 2010 Stuxnet was working in Iran. In March 2011 NASA admitted that within two years 13 successful attacks had been launched against their computer systems and they lost control of the space station.

On the 28th May 2011 Lockheed Martin discovered that their computer systems had come under a very serious attack. They found out that the attackers took all of the plans for Lockheed Martin's new jets, such as the F-35, which are very sophisticated strategic weapon systems. Everything had been taken in those attacks. The suspicion was that the Chinese were behind those attacks. Somebody asked how they knew it was the Chinese because usually people do not attack from sites in their own country. People usually use a server in a different country that is far away so that the attack cannot be connected to them. The Americans answered this question by saying that Lockheed Martin is so well protected that a successful attack would require hundreds of people working towards that goal for at least four years and China is the only country that could facilitate an operation like that.

In September 2011 Iranian hackers broke into the computers of an information security company in the Netherlands and forged documents that allowed them to gain access to the sites of the Mossad, the CIA and MI6. In December 2011 Saudi hackers announced that they had downloaded the credit card details of 400,000 Israelis. In response Israeli hackers broke into the records of Saudi credit cards. That was a big fight at the time. In November 2011 hackers took control of the water pump systems in Illinois and Texas. They did not cause any damage. They just wanted to show the United States that they are not protected, that they are exposed to such attacks. In May 2012 the Flame virus was disclosed, which experts believe to be 20 times more sophisticated than Stuxnet.

We therefore decided that we need an ecosystem to tackle all of those problems. It is not only a matter of attacking and it is not only a matter of defending. You have to have both capabilities and you need them both simultaneously. That is why you need an ecosystem rather than different stations. Things need to be synchronised. In World War II Great Britain's air force was split into three different parts, the first to protect England's seashores, the second to protect England's skies and the third to attack outside of England. That is of course impossible today. The air force is now one entity. So, too, do we need everything that deals with cyberspace to be strongly synchronised in a single system in order to prevent certain situations.

To give you a hypothetical example: we would like to take some information from certain computers somewhere else. At the same time, other cyber units will attack these computers to paralyse them. That would be stupid. We need the computers to remain active in order to be able to take information from it. You therefore need to have very good synchronisation. That is why we need such an ecosystem. Of course there are obstacles and difficulties in achieving that. Why is that? In order to have the ability to do such a thing you need regulation. The government has to make

special legislation to allow the government to protect every infrastructure. Otherwise you cannot protect it. Even if you have the means and the ability, you cannot protect it.

In the United States, for example, one of the problems they have is that the government does not want to take responsibility for the protection of the private finance system because they say it would hurt privacy to do so and therefore they do not want to take on that responsibility. I think that is a mistake because an attack on those systems could easily be made. Suppose you went to a bank in Israel and said you wanted to protect their site against any outside attack. The bank would say that if customers knew protection measures were in place it might mean people were looking into private accounts, which would be a violation of privacy. Again, you need the right legislation which will balance privacy concerns with the need for protection. Privacy is of course very important and those are the obstacles.

As to technology development, changes in most technologies take 10 to 20 years. Look at cars. After the car was invented it took many, many years to make real changes in their design. In the technology of cyberspace a generation is one and a half years and no more. You cannot therefore get an expert to set up a system to protect your country and then forget about it for the next five or 10 years. One day you will wake up with a total disaster. You have to constantly follow up. You have to operate those systems day by day, constantly developing the technology. After a year or a year and a half you will have a totally different technology. If you are not prepared you will have no protection. Everything you did before will be dead. This technology requires constant development and you always have to be on alert.

Having technology is not enough. There are many, many things that can cause damage in a surprising way if somebody decides to attack you. It is not enough therefore to have technology. You need to have the right warriors. General Alexander of the United States said that to be a cyber warrior requires at least 10 years' experience in building networks, defending networks and operating in cyberspace. How many people have experience like that? Very few do. David Dittrich said that we can reasonably conclude that it would take more than 10 years of experience at the highest level of CNO, which is Computer Network Operator, in order to have a capacity for defence and offence in cyber warfare. That means you need to invest a lot of money and time to cultivate cyber warriors. You cannot just get some amateurs to do it. You need professional people who have dedicated their life to that discipline.

In the United States they have three million IT people. 60% of them live in fear because they do not know anything about cyberspace and they cannot protect their own systems. The United States budget for cyberspace is currently USD 4.7 billion a year. I do not know what the budgets of your countries are, but I suggest double it without knowing it. You need much more. You need to invest in it a lot if you want to protect yourselves.

We are therefore speaking about a general ecosystem that is supposed to encompass industry, security, education, the government's proper role and legislation. You have to deal with all of these things and synchronise them. Israel is a target. Israel is the most attacked target in the world. We have almost 100,000 attacks per day. During a period like the Gaza War or the Lebanese War we have more than a million attacks per day. However, the McAfee Threats Reports grades countries according to their level of protection and ranks Israel as the country most prepared for a cyber threat along with Sweden and Poland. Even though there are so many people in so many countries who want to attack Israel, we have the right protection because we were prepared for it. We had to be so. As I said, we live in a very, very difficult neighbourhood, so we always have to be prepared for attacks.

I think that we are usually afraid of what we do not know. If we know about it we are not afraid of it. Therefore our task in every country is to learn about this topic very seriously and to invest the money needed to prepare the right people to protect it. Otherwise we will be in a very bad situation if we have a war of a conflict. I would like to end by saying that in our current situation today we sometimes see one young man who is worth more than a full army division. A good cyber warrior can do more damage than any army division or any air force unit. That is unbelievable, but it is true. Thank you.