The Pulse of the Middle East

ISRAEL PULSE

Israeli expert: 'cyberspace has become a battlefield'

Author Ben Caspit / December 23, 2014

Col. **Gabi Siboni** (ret.) heads the Cyber Security Program at the Israeli **Institute for National Security Studies**. Considered one of the top experts in the field, Siboni publishes numerous studies and position papers on the issue on behalf of the institute. The most recent of these, published the week of Dec. 22, is devoted to the cyberwar between the United States and North Korea.

In April 2015, Siboni will chair the Institute's first major conference for the Institute in Washington. The event is being held in cooperation with major American organizations (including the Cyber Security Forum Initiative), and with the participation of several senior American officials specializing in the field, including Ann Barron-DiCamillo, director of the US Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security. Various Israeli officials will also be participating in the event, including representatives of the Computer Service Directorate of the Israel Defense Forces (IDF) and the economy and energy ministries.

Cybersecurity in Israel is a highly developed field, considered to be among the most advanced in the world. The late Prime Minister Ariel Sharon recognized cybersecurity as a central component of national security as early as 2002, and established the Data Security Authority in the Shin Bet. Israel is also considered one of the most effective countries in the world in everything to do with defending its major facilities and institutions from cyberattacks. Recently, Prime Minister Benjamin Netanyahu established an authority similar to the one founded by Sharon to focus on the defense of civilian installations. During Operation Protective Edge [July-August 2014], Israel came under serious attacks from hackers and various other groups in cyberspace, but the defensive systems in place withstood the challenge, and there was no significant damage.

In a special interview with Al-Monitor, Siboni talks about how we are standing on the threshold of a new era: the era of cyberwarfare. The text of the interview follows:

Al-Monitor: Do you agree that what is happening now between the US and North Korea can be defined as a cyberwar?

Siboni: Certainly. What is happening now is that the things we know in the back of our minds are beginning to seep and slip out. Cyberspace is becoming a real battleground in conflicts between countries. Whenever there is a determined adversary who knows how to exploit the structural weaknesses of Western democracies — in this case, the United States — he can strike at the country's soft underbelly and succeed in ways that cannot be ignored. In the current case, the goal is to prevent a major corporation such as Sony from distributing a film. We are not yet fully aware of the magnitude of this incident. It seems to be passing us by, but given the test of time, it will become obvious that this was a formative event. We must take advantage of it as a pilot case in order to draw conclusions about the future.

Al-Monitor: How would you characterize the structural weakness that democratic states have in dealing with this? Ostensibly, it should be easier to handle, since it doesn't involve the use of physical force, and it does not have a deleterious effect on human rights. Why should it be a problem?

Siboni: Democracies have an inherent structural weakness when it comes to responding quickly and providing a speedy defense network to vulnerable civil societies. Sony is a private company, meaning that protecting it is not a federal affair. In other words, the US government has no reason to intervene. However, when Sony comes under attack and is prevented from distributing one of its films, the incident is transformed into an assault on freedom of expression, freedom of employment and other superlative democratic values. That is why, when President Barack Obama says that he regrets that the CEO of Sony Pictures did not consult with him, his response will hardly deter the other side.

Al-Monitor: What is the solution?

Siboni: The West must realize that their cyberspace is a sovereign space in every way imaginable. They must dive right in to the depths of the web and formulate an approach to defending that space. This should encompass all factors operating within that space, and not just official state institutions. What happened with Sony is an excellent example of this. The state should also regulate everything concerning the defense of cyberspace. I know that "regulation" is practically a four-letter word in the United States, but in this particular field, there aren't many other options.

Al-Monitor: We're talking about a virtual space. Why should it be regulated?

Siboni: Let me give you an example. When someone wants to open a restaurant, he has to go through an almost endless number of regulatory agencies before he can get a license. He most get the approval of the Ministry of Health and the Fire Department, he must prove that the establishment provides disabled access, he needs a business license, etc. There is no reason why large companies that handle information about the general public, such as credit card numbers or personal and medical information, should not be

obligated to protect that information in cyberspace. There is no choice. Cyberspace has become a battlefield. It must not be abandoned.

Al-Monitor: How would you go about doing that in a space that has no beginning and no end? After all, we're not talking about physical boundaries or, for that matter, about anything tangible. The space is entirely virtual.

Siboni: A space like that cannot be sealed hermetically, but there is still plenty of room between not doing anything and doing everything possible. There is a way to prevent North Korean hackers from seizing control of and using your databases. While it is impossible to protect everything, it is possible to protect what is important. Large corporations simply do not invest enough in these protective measures. There has already been a major retail chain [Target] whose database was hacked. The information from millions of credit cards was stolen, causing enormous damage. The state should intervene and determine the necessary steps that every company like that should take. Here in Israel there is legislation requiring that every house that is constructed have a room with cement walls to serve as a shelter. This is essential in a country like Israel, which is threatened by rockets from every direction. When it comes to cyberspace, all countries are threatened all the time, from every imaginable direction and place. In other words, everyone handling essential information online must have some kind of shelter.

Al-Monitor: Do you think that this will happen?

Siboni: Certainly. It's already happening. A company like Sony will be much more secure and protected from cyberhacks ten years from now than it is today.

Al-Monitor: Until now we've been talking about hacking into data bases and other virtual targets. Have we reached a point where it is possible to cause actual physical damage with a cyberattack? Do you agree that what is happening now between the US and North Korea can be defined as a cyberwar? Will there be some point of interface (POI) connecting the virtual world with the physical world?

Siboni: There are already capacities in cyberspace to deal with physical spaces. This isn't science fiction. It's already here. If you succeed in attacking the nuclear reactor of a power station, to interrupt the cooling system or cause some other damage, it is a strategic incident. Technologically speaking, we are already there. That is why it is essential that we develop defensive capabilities. When it comes to this, the attackers will always be more advanced and more determined than the defenders. They have a structural advantage. It is no secret that countries like China and Iran are involved in attempts to gain access to critical infrastructures in the United States and maybe even in Israel too. This does not mean that they will take these steps tomorrow morning and immediately exploit their capabilities. They are saving it for some day in the potential future, when the order is given to attack. The situation today is that the proverbial "red buttons" are not limited to launching nuclear missiles. They also exist to launch cyberattacks against strategic targets. In the future, this will develop into a cold war within the cyberdomain.

Al-Monitor: Will this come at the expense of real world action, in the physical realm?

Siboni: No, it is an additional space, another dimension that will be covered. No world power will give up on its nuclear cruise missiles, its submarines, or its aircraft carriers. When push comes to shove, there is no alternative to them. There will, however, be new cyber capabilities added to this arsenal. This means that the wars of the future, should they break out, will not consist solely of hunks of metal hurtling through the air. They will also include buttons that are pushed and strategic sites that are damaged in cyberattacks.

Al-Monitor: Could these capabilities get into the hands of individual hackers, or will they always remain the exclusive domain of national entities?

Siboni: We divide these capabilities into three different types of attacks:

1. Routine Internet attacks. In these, hackers try to infiltrate a website, such as the website of the Mossad or the Shin Bet, and to interfere with its operation. They try to damage the service, to take the website off from the network for a limited time, to disrupt it. If this happens to an airline, the damage that can be caused is quite complex. This ability is the lowest level of a cyberattack.
2. The second ability level is to penetrate data systems in such a way that it is possible to remove the date or interfere with it. That is what happened to Sony. Sensitive information can then be distributed publicly, it can be garbled, and it could be used for extortion. This is a more complicated level of cyberattack, but it is not the most severe.
3. The most severe form of cyberattack is the possibility of infiltrating operation systems, such as the system that oversees electricity production in Israel's largest power station, Orot Rabin [near the city of Hadera], or at refineries, or to attack the operational management system of the Airports Authority. This means that you are able to interfere with air transportation and to cause accidents, or even to paralyze entire systems. This is the most severe case of cyberattacks. As of now, this area of capabilities is the exclusive domain of developed states. The question is what the future will bring. That question is difficult to answer.

Al-Monitor: Does that mean that in the future, a handful of crazy hackers in a basement could do all that?

Siboni: It is hard to predict, but anything is possible. In order to be able to do that, they would need the technological capacity, intelligence capacity and operational capacity. Plenty of people have the technological capacity. The intelligence and operational capacities are more complicated issues. We're only talking about countries for now, but as we said, in the future, anything is possible. This only continues to underscore the need for sophisticated defense systems just as much as means of attack. Everyone talks about the need to prevent the widespread distribution of weapons of mass destruction, but for now, they almost ignore the proliferation of sophisticated cyber capabilities. It is much easier to share this capacity than it is to build a nuclear bomb. And there is one more

thing to consider. Nations can easily find themselves all sorts of terrorist organizations to support and use them to launch attacks of this kind, without the state actually taking responsibility. This is already happening.

Al-Monitor: Where would you rank Israel in terms of its cyber capabilities?

Siboni: We are very advanced. We excel in it, particularly in cyberdefense.

Al-Monitor: I'm actually more interested in its operational capabilities.

Siboni: I really can't talk about that, but there have already been quite a few reports in the foreign press of cyberattacks allegedly attributed to Israel and the United States together, such as the Stuxnet computer worm that attacked an Iranian nuclear reactor. It is usually said that the sky is the limit, but when it comes to the cyberworld, even the sky is not the limit. It is a limitless world with infinite possibilities.

Read more: http://www.al-monitor.com/pulse/originals/2014/12/israel-sony-cyberwars-us-north-korea-internet-attacks.html#ixzz3Moof3rEo