المركز العربي للأبحاث ودراسة السياسات
ARAB CENTER FOR RESEARCH & POLICY STUDIES
(Doha Institute)

www.dohainstitute.org

Book Reviews

Israel and Cyber Warfare

***Book Review:** Cyber Warfare: Concepts, Trends, and Implications for Israel*

Dr. Mahmoud Muhareb

Doha, September - 2011

Series (Book Reviews)

Contents

Book Review: Cyber Warfare: Concepts, Trends, and Implications for Israel
Shmuel Even and David Siman-Tov
Tel Aviv: Institute for National Security Studies, June 2011

Israel and Cyberspace

Cyberspace[1] is a new term that has entered into use in recent decades due to the revolution in information technology. Included in the realm of cyberspace are all existing computers and the data inside them, as well as the systems, programs, and open networks available for the use of the general public or those networks that are designed for the use of a specific set of users; additionally, though separate from these aspects, are the parts of the internet that are publicly accessible.

Recent times have witnessed a growing interest on the part of research centers and elites in Israel on the subject of warfare in cyberspace. On June 9, 2011, the Institute for National Security Studies at the University of Tel Aviv organized a one day seminar focusing on this particular subject under the title "Cyber Warfare: Challenges on the Global, Political and Technological Levels". Israeli Prime Minister Benjamin Netanyahu opened the conference, which exhibited an elite group of Israeli researchers and experts who spoke and delivered papers that stressed the importance of war in cyberspace for the security of Israel. In his speech, Benjamin Netanyahu stressed the importance and vitality of this issue for Israel, emphasizing the need for Israel to become a superpower in the field of cyber warfare, and to be a major actor at the global level in this area.[2] On July 4, 2011, the Knesset's (Israeli parliament) "Committee on Science" also discussed the issue of war in cyberspace, hearing from experts and specialists in the field.

In speaking to the "Committee on Science," General Professor Yitzhak Ben-Yisrael, head of the "National Council for Research and Development," pointed to the existence of a gap in Israel in which the country's defensive precautions to protect important civilian infrastructure sensitive to cyber attacks lagged behind the country's defensive precautions concerning military and security infrastructure. He added that cyber attacks occur on a daily basis, and are not science fiction, but a lived reality. He further stated that "some of these attacks are mere nuisance, while other such attacks may cause severe damage. There are many advanced programs and systems that can be deployed in cyberspace that can paralyze and disrupt the work of fundamental state facilities,

[1] The International Telecommunication Union of the United Nations (ITU) defines cyberspace as follows: "Cyberspace: The physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users." Source: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

[2] http://news.walla.co.il/?w=/9/1830693/@@/item/printer

such as the stock exchange, banks, electricity, transportation and communications, and people do not realize the extent of the danger."

Yitzhak Ben-Yisrael also indicated that one of the objectives of the establishment of the "National Cyber Committee" in Israel, the launch of which was announced in May of 2011, has been to create an advanced mainframe computer in one of the Israeli universities. Israel currently has no such computer, and the sale of such a computer to Israel is prohibited because it has not signed the Convention on the Non-Proliferation of Nuclear Weapons. In the context of emphasizing the issue of securing cyberspace, the head of the "Committee on Science" of the Knesset, Meir Shitrit, stated that it is possible to cause the collapse of Israel not with tanks and planes, but through cyber warfare.[3]

In June 2011, in the context of this Israeli interest in cyber warfare, the Institute for National Security Studies at the University of Tel Aviv published the book *Cyber Warfare: Concepts, Trends, and Implications for Israel* by researchers Shmuel Even and David Siman-Tov, both of whom work at the Institute for National Security Studies. The book includes an introduction, four chapters, a conclusion and two appendices, with a total of ninety pages. The authors find that cyberspace has become a new theater of war, joining those of land, air, sea and space. As such, advanced states and their armies are increasing their activities in, and research on, cyberspace, which for these states has become an important source of power. At the same time, it reveals the soft underbelly of these powerful states because the infrastructure upon which modern states rely—such as electricity, water, transportation, telecommunications, the stock market and banks—is dependent on cyberspace for their proper functioning. Military command and control networks, as well as the various types of advanced technology on the battlefield, such as intelligence and data collection systems, and the use of satellites and unmanned aircraft in warfare are also heavily dependent on cyberspace.

The authors noted the favorable features of cyberspace as a theater of battle, the most notable of which is the ability to work at the speed of one-thousandth of a second against enemies that are thousands of miles away, without exposing the attackers or fighters to physical risk.

The advantages of cyberspace make it attractive for use in the conduct of warfare alongside conventional weapons, as was done by Russia, according to the authors, in its war against Georgia in 2008. It can also be used during war against strategic targets, as was the case in the attack on the Iranian nuclear reactor in 2009 (carried out by Israel according to several media sources), an attack the authors consider to have been a founding event in the field of cyber warfare, ushering in a new era in the evolution of the use of cyberspace in warfare.

[3] http://www.calcalist.co.il/Ext/Comp/ArticleLayout/CdaArticlePrintPreview/1,2506,L-3523149,00.html

The authors consider the fact that many states have used cyberspace in warfare, development operations, and preparations confirms that the arms race in cyberspace has begun. They point out that many countries have, in recent years, established various institutions and bodies specializing in the use of cyberspace as an arena for warfare, and have developed military and security strategies for cyberspace.

The authors began their book's first chapter, "Cyberspace and Security: A Conceptual Framework," with definitions and explanations of terms related to the subject of cyberspace. The authors go on in this chapter to deal with the following topics: the features of cyberspace as an arena for warfare; cyberspace: the new content of traditional security terms; the strategic environment of cyberspace; espionage and soft electronic warfare; and the war in cyberspace.

The book's second chapter is entitled "Attack Operations and Inhibiting Factors in Cyberspace". The chapter covers the following subjects: prominent offensive operations in cyberspace; the factors that led to the increase of knowledge in cyberspace; the use of cyberspace for the purposes of the war: inhibiting factors; terrorism in cyberspace; an international convention for the organization of activities in cyberspace; and a summary of encouraging and inhibiting factors for the use of a weapon of cyber warfare in conflicts between states.

The book's third chapter – which appears under the title "Looking Over the Sea: The Preparedness of States for the Cyberspace Challenge" – deals with the preparations undertaken by several important states, their strategies, and the institutions they have set up in order to ensure security against the risks inherent in cyberspace. These countries are: the United States, France, Germany, Britain and China.

In their fourth chapter, the two researchers dealt with the importance and vitality of cyberspace to Israel, and the institutional measures taken by Israel to protect its cyberspace. The researchers forward a strategic recommendation that Israel should follow to defend its cyberspace. They also propose measures for the integration of cyberspace into Israel's national security strategy.

The authors argue that the state of Israel has become "computerized"; its government institutions and its various facilities and companies are dependent upon the Internet. Furthermore, many of the citizens' transactions with state institutions and various other facilities in the state are carried out over the Internet. The researchers stress that information technology contributes directly and indirectly in the growth of the Israeli economy, as Israel is one of the many states that is advanced in the development of information technology. The volume of the internet economy in Israel in 2009 reached fifty billion shekels (one dollar is equal to three and a half shekels), which is equivalent to 6.5 percent of Israeli gross domestic product. According to estimates, in 2015 the Internet economy in Israel is expected to reach eighty-five billion shekels, which would equal 8.5 percent of projected Israeli gross domestic product.

Israel's Measures to Defend its Cyberspace

The authors state that Israel has taken a series of measures during the past decade and a half in order to protect and defend its cyberspace. The most important of these measures have been as follows:

Government Infrastructure for the Internet Era

In 1997, Israel established the "government infrastructure for the internet era" project within the Israeli Ministry of Finance. The goal of this project was defined as safeguarding and securing the use of the Internet in the government ministries and institutions. As part of this project, the "Center for the Protection of the Government of Israel's Information" was established and entrusted with multiple tasks, including: following the development of methods for protecting information around the world, coordinating between government ministries and institutions in order to find solutions for the problems of protecting information, and conducting research on this topic.

Creating the Official Authority for the Protection of Information

In 2002, the "official authority for the protection of information" was established within the General Intelligence Service (Shabak). This "authority" was entrusted with the tasks of protecting the infrastructure of the most important and vital computers in Israel against the risks of so-called "terror threats," "sabotage," and espionage activities. The authors point to the existence of a committee within the Israeli National Security Council, among the powers of which are to allow the General Intelligence Service's "official authority for the protection of information" to expand the list of institutions that it monitors in order to protect the information in those institutions. The authors state that the work of the "official authority for the protection of information" is beset with many shortcomings, particularly because it does not cover all institutions and facilities in Israel and because it is subordinate to the General Intelligence Service (Shabak), a deterrent against free and comfortable interactions with many of the institutions the authority deals with.

The Creation of the Cyber Unit in the Israeli Army

In 2009, Gabi Ashkenazi, Chief of Staff of the Israeli army, stated that he considered cyberspace as an area of both strategic and operational warfare. Accordingly, the Israeli military set up the "cyber unit" within Unit 8200 of the Israeli Military Intelligence (AMAN) with the purpose of guiding and coordinating the activities of the Israeli Army in cyberspace. In a December 2009 lecture at the Institute for National Security Studies, Amos Yadlin, then head of Israeli Military Intelligence, noted that one of the most important dangers lying in wait for Israel, and which may cause it harm, lies in the possibility that computers critical to Israel would be penetrated. Amos Yadlin explained that the cyber unit of the Israeli military aims to provide good defense for the

internet networks operating in Israel, as well as carry out attacks against external targets over cyberspace.

The Creation of the Information Systems Management Unit

On March 27, the Israeli government approved the establishment of an "information management unit," which is subordinate to the director general of the Israeli Ministry of Finance and is directly responsible for all government computerized communications systems, including the "government infrastructure for the internet age" project.

The National Cyber Committee

On May 18, 2011, Israeli Prime Minister Benjamin Netanyahu announced the establishment of the "national cyber committee" in Israel. Netanyahu said that the main objective of this body would be to enhance Israel's capabilities for the defense of critical infrastructure systems against "terrorist attacks" in cyberspace that may be carried out either by foreign states or "terrorist organizations". According to Netanyahu's statement, Israel is vulnerable to attacks in cyberspace as everything that is computerized may be exposed to such cyber attacks which may cripple critically important facilities and institutions – such as electricity, water, telecommunications and transportation – thereby crippling the state itself.

In addition to the functions relating to the defense of Israeli cyberspace, the authors suggest that the national cyber committee's tasks will include the support and development of Israeli companies specializing in defense as it relates to cyberspace. In this way, the committee would facilitate Israel's securing of a larger share of cyberspace, which is growing very rapidly on a global level.

The authors go on to explain that there are three important factors driving Israel to hasten the process of taking precautions and security measures in cyberspace, which are as follows:

First, as an advanced state with computerized facilities and institutions, Israeli cyberspace is exposed to the risk of being attacked, and such attacks may lead to a paralysis in Israel's vital infrastructure.
Second, Israel faces enemies that are motivated to harm it as soon as they have the chance, whether these enemies are states, organizations, or individuals.
Third, there is an opportunity for Israel to develop not only advanced defense capabilities in cyberspace, but also its capabilities of using cyberspace in war.

A Strategy for the Defense of Israeli Cyberspace

The authors suggest that the Israeli government adopt a national strategy for the defense of Israeli cyberspace along the following lines:

1. The recognition of cyberspace as a new national arena, the defense of which should be a particular priority (along with other arenas such as land, air and sea) through a comprehensive vision and the cooperation of all relevant parties.
2. The establishment of a body and a central command for the defense of cyberspace at the national level.
3. Dealing with the development of vital infrastructure and security systems as a top priority while also carrying out the defense of other components, such as the defense of information in universities and research centers and the defense of companies that have an impact on the Israeli economy that are not classified as part of the state's infrastructure.
4. Building a dynamic and comprehensive defense system in cyberspace, such as the system established by the US Department of Defense.
5. Permanent cooperation in the arena of cyberspace between the public sector, the security sector, and the private sector.
6. Cooperation with foreign countries, particularly the allied states, on the issue of cyberspace.
7. Passing specific legislation pertaining to cyberspace and ensuring this legislation's implementation on the ground.
8. Assisting the general public in increasing its awareness of cyberspace, the development of the public's defense capabilities in this area, and the granting of incentives to companies and individuals to acquire defense software while increasing control and monitoring of companies developing such software.
9. The use of the most advanced and up to date technological aids and devices related to cyberspace.
10. The formulation and development of Israeli deterrence policies, including the ability to carry out injurious and direct response against any party engaged in aggression against Israeli cyberspace. This would be the included in the mandate and tasks of the Israeli defense establishment.

Cyberspace in Israel's Security Strategy

The authors emphasize that the addition of cyberspace as a new theater of warfare – in addition to the battlefields on land, air, sea and space – requires the integration of cyber warfare into the Israeli strategy for and conception of security. This requires the change and development of the conception of the basic terms pertaining to Israeli security doctrine. For instance, the concept of "strategic environment" in cyberspace differs from the traditional concept of the "strategic

environment" in the Israeli security doctrine in which it revolves around traditional geo-political threats. Furthermore, the concepts of space, time, and distance in cyberspace differ from their traditional conception as the speed of an attack carried out over cyberspace against a target geographically located hundreds or thousands of miles away is one-thousandth of a second. The authors argue that it would be very difficult for Israel to implement a policy of deterrence, considered to be the cornerstone of Israeli defense policy, in a war carried out over cyberspace due to the difficulty of determining the identity of the party carrying out a cyber attack.

The book's authors state that defense in cyber warfare poses a new kind of challenge to Israel, as an enemy would be able to carry out attacks with lightning speed and identifying the enemy can only be done with great difficulty. The authors recommend that Israel learn and benefit from the concept of "effective defense" in cyberspace, a concept followed by the United States in its approach to cyber warfare. The "effective defense" approach relies on sophisticated intelligence capabilities to determine the source of activity over the Internet, and on dynamic cyber defense systems capable of instant automated responses without human intervention. "Effective defense," the authors continue, depends not only on advanced technology, but also on a tightly controlled network with stringent rules and procedures, a culture that understands the risks involved, strict discipline, defense of the sites, and strong human control.

In light of the Israeli army's recognition of cyberspace – along with the other arenas of land, air, space and sea – as an arena of warfare, the authors also recommend making changes in the Israeli army and setting up a special military force – akin to the infantry, navy and air force – dedicated to cyber warfare.