The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case

Gil Baram

The past decade has witnessed rapid developments in computers and information technology, leading to far reaching changes in almost all areas of life, including the military and defense spheres. Many changes have occurred in the nature of warfare and the design of military forces, owing, among other things, to developments in strategic thinking and the formulation of military doctrines that are tailored to a changing reality. In the 1990s, attempts to assess the consequences of the transition to the information age for defense endeavors led to the emergence of the notion of a "revolution in military affairs – RMA." This notion was conceived as a result of new technological innovations that improved the quality and availability of intelligence, the flow of information, and the precision of weapons. In the ensuing years, especially in the 21st century, advanced technologies for cyber warfare were developed, changing the face of the battlefield and the pattern of modern military action.

The cyber technology used in warfare affects the way the latter is conducted. A country possessing this technology enjoys battlefield superiority, high quality and comprehensive intelligence, a precise and rapid attack capability, the ability to protect essential infrastructures, enhanced command and control capabilities, and so on. These capabilities contribute to a nation's power, and strengthen its national security. Cyber warfare technologies have the potential for enormous advantages, along with new and unfamiliar risks. Given the sweeping innovation in this field, the understanding of its nature and consequences has only begun.

Gil Baram is a Masters student in Security Studies at Tel Aviv University and a research fellow at the Yuval Ne'eman Workshop for Science, Technology, and Security.

Many countries, headed by the US and Israel, have intensified their cyber activities in recent years. While this activity constitutes a source of strength for them, it also exposes their weak points; this is because the infrastructures essential for the functioning of each country have become dependent on computers. Discovering the optimal way of handling the threat posed by the technological development of cyber warfare has been a key challenge facing Israel in recent years.[1]

Israel's national interest focuses on maintaining its security against those seeking to harm it and undermine its very existence. This interest, along with Israel's geopolitical location, necessitates superiority in cyberspace as an integral part of its ability to defend itself against conventional and cyber attacks, and an integral part of its deterrent attack capability in the Middle East theater and beyond.

Israel is considered a global leader in its ability to handle cyber attacks. A comprehensive report that examined the preparedness of 23 countries in the cyberwar sphere accorded Israel the highest rating – four and a half stars out of five. The report indicates that at any given moment, Israel is subject to about one thousand cyber attacks. This figure particularly impressed the writers of the report, who praised the Israeli defense systems and noted that Israel was well prepared to deal with a cyber attack against it.[2]

The development of Israel's operational capabilities in the field of cyber warfare is a key element in maintaining its national strength. Its economy, industry, security, education, and preservation as a democratic, open, and established society depend mainly on its ability to protect its essential computer networks against an attack liable to disrupt its way of life. The increasing reliance on computer systems in Israel and throughout the world has brought new challenges with it, demanding immediate solutions at the national level.[3]

The aim of this article is to present the role of cyber warfare technology in Israel's security doctrine and to examine Israel's preparations for dealing with the cyber threat by evaluating three necessary levels: (1) formulating a regular strategy for handling the threat posed by the development of cyber warfare technology; (2) allocating resources and budgets; and (3) effecting changes in the manner in which Israel builds its forces. An assessment of government publications will presumably demonstrate the importance of this topic for decision makers and the resources they allocate for dealing

with it. The aim here is to portray the situation in Israel and attempt to point out the existing gaps in this field.

The article is based on current literature on the subject as well as unclassified public information that includes newspaper reports, press releases, government documents, and interviews with key people in the field. There are few official publications in Israel that deal with how to handle the cyber threat, especially in comparison with Israel's cyber attack capabilities. Therefore, given the nature of security in Israel, one can assume that a great deal of information on cyber operations and their budget allocations remains classified.

A number of difficulties encountered in this research are attributable to the fact that since this research field is relatively new, there is still not sufficient historical knowledge on the subject of the effect of the development of cyber warfare technology on changes in the existing strategies and the way forces are built. Nevertheless, because the field is very important, it is preferable to begin studying it in depth despite the existing knowledge gaps. While this study focuses on cyber warfare, which comprises the country's defensive and offensive preparations, it does not deal with the use of computers for communications and warfare management. Since computers are currently used in many communications and military operations, this area is very wide-ranging, and exceeds the scope of this article.

The Role of Cyber Warfare Technology in the Israel Security Concept

The many changes that have occurred in cyber warfare technology are challenging the current defense doctrine, and necessitate a renewed assessment of its basic concepts. A situation has emerged in which protecting essential energy, water, computer, communications, transportation, and economic infrastructures is of supreme importance in the civilian and the defense sectors alike. The necessary adjustments in the defense doctrine should therefore be made in order to be able to provide a solution to the new threats.[4]

In April 2006, a proposal was submitted to then-Minister of Defense Amir Peretz for a revision of Israel's security doctrine. A committee headed by Dan Meridor whose members included the chairman of the National Security Council, the head of the Israel Security Agency, the

official responsible for security in the defense establishment, and others prepared the proposal. The committee report indicated that Israel had entered an era of major and rapid strategic changes, including far-reaching technological changes.[5] Among other things, the committee recommended adding defense to the three traditional elements (deterrence, alertness, and decision),[6] and recommended in particular the procurement of unmanned aerial vehicles and the protection of the national computer systems against penetration by hostile parties.[7]

In the wake of the committee's discussions, the possibility of adding a fourth basic term to the "security trio," namely, "defense" or "protection," was raised.[8] Israel did in fact invest a large proportion of its budget and defense efforts in passive protection. In addition to passive protection tools, the "defense" idea was expanded to include tools for attacking individual targets aimed at thwarting high trajectory barrages and terrorist attacks below the escalation threshold.[9]

Defense is of supreme importance in the realm of cyber warfare because effective defense ensures that a country's essential computer systems continue to operate. Furthermore, advanced cyber capabilities enable a country to protect its critical infrastructures effectively, thereby providing a solution to the need for an active defense, as noted in the Meridor Committee report.

For a long time, it was common practice to refer to the protection of computer systems as "information security," reflecting the idea that the most important thing to be protected was sensitive information (classified or business information). Over the years, this approach evolved to encompass other threats besides an attack on information: disruption of services, paralysis of essential computer-based processes, and so on. At the national level, the concept of protecting computer systems has been extended, and can now be called "cyber defense."[10]

Since the committee report was published, the use of cyber technology for various warfare needs on the battlefield has risen steeply. It would therefore be appropriate to assess the role of cyber warfare technology in the processes of updating Israel's security doctrine.

A look at the history of Israel's wars reveals that technology has played a more important role from one war to the next, and has become more sophisticated with time. Basic differences exist between Israel and Arab countries, and there is a clear quantitative asymmetry. If we take

the major quantitative gaps into account, Israel's relative advantage in diverting warfare to the technological plane stands out. It is easier for Israel to contend with the Arab world in sophisticated air battles and cyber operations (according to foreign sources) than in throwing stones or hand to hand fighting. The quantitative gaps become less significant and high quality weapon systems and personnel become more valuable when more advanced technologies are involved. The IDF excelled at identifying the great potential inherent in computers, and began using various types of computer warfare as early as the 1990s.[11]

Dealing with the threat posed by cyber warfare technological developments fits in with the Israeli security doctrine: home-grown Israeli capabilities are used, relying on "Jewish" developments and inventiveness in combination with global technologies. This field is well known to young people living in Israel, which was dubbed the "start-up nation,"[12] and is based on the importance of quality over quantity.

It is evident that the three original pillars of the Israeli security doctrine are relevant for dealing with the cyber threat:

a. *Deterrence*. Advanced cyber capabilities will enable Israel to create deterrence against its enemies. One example is the Stuxnet virus, attributed to the US and Israel, which was perceived as a major advance in the two countries' cyber attack capabilities and the power of their effect, was widely reported in the global media, and helped strengthen Israeli deterrence.[13]
b. *Warning*. Cyber capabilities enable Israel to amass a large volume of information about its enemies while simultaneously denying them access to its own stores of information. Israel can thus be effectively alerted to their intentions against it.
c. *Decision*. Israel is one of the world's leading countries in cyber capabilities. These capabilities afford it an advantage in battle through the use of advanced cyber tools, which can tip the outcome in its favor. It is important to note that both the concept of deterrence and the concept of decision in the cyber sphere are elusive, and their significance in a cyber context has not yet been fully realized. Nevertheless, it is now clear that cyber superiority combined with advanced kinetic capabilities is likely to prove decisive in battle.

From Israel's inception until the present day, its security doctrine has rested on the principle that quality is more important than quantity. Cyber

warfare technology is consistent with this principle: the use of cyber tools, which requires the training of expert manpower rather than the exertion of great physical force, facilitates operations that help bolster Israel's deterrent capability, and garners it great prestige in the international arena.

Thus it appears that integrating cyber warfare capabilities into Israel's security doctrine can be relatively simple, if indeed this is done soon. These capabilities are consistent with the three basic principles on which the security doctrine is based. Furthermore, developing independent cyber warfare capabilities and tools clearly embodies the principle of quality over quantity: all that is necessary is a high level of trained manpower for developing systems that make it possible to carry out operations against remote targets without risking human life and without requiring many resources.

Formulating a Regular Strategy for Cyberspace

The cyber threat is a result of the critical role played by computer systems in the national infrastructures and everyday life. This virtual space was generated by the decentralized development of various systems and sectors in the context of accelerated economic and technological development, without any significant connections to security. When the need to deal with the security aspects of the cyber realm arose in recent years, it sparked the question of who was responsible for its security.[14]

Information security and protection of computerized infrastructures are not new topics in Israel. Israel was one of the first countries in the world to recognize the importance of protecting essential computer systems. As early as 1996, the government made decisions about the best method of defense against cyber attacks.[15] The Tehila Project ("Government Infrastructure for the Internet Age" – The Governmental Internet Service Provider), whose purpose was to protect the connections of government ministries to the internet and provide secure internet surfing for government ministries, was launched in 1997.[16] Later, in 1998, the Law for Regulating Security in Public Organizations, which dealt with defining essential computer systems and their security, was enacted.[17]

The Decision to Establish a National Information Security Authority

Israel does not have a regular publication in which it publishes its policy vis-à-vis dealing with the cyber threat. Most of the existing information is based

on media reports and academic research. At the same time, a number of published official decisions are shedding light on the situation. In February 2002, a ministerial committee for national security made a decision on the subject of "Responsibility for Protecting Computer Systems in Israel" (Decision B/84). This decision designed the outline for the protection of critical computerized infrastructures in Israel, thereby providing a basis for implementing the Israeli response to the cyber threat to essential national computer infrastructures. The decision provided for the establishment of two special agencies: a steering committee for regular examination of the identity of public and private entities essential for Israel's functioning, and a national authority for the protection of computerized systems.

Following the ministerial committee's decision, a steering committee was immediately convened, headed by the chairman of the National Security Council. The steering committee's goal was to formulate an array of measures for the protection of the country's essential computer systems. The committee set forth the principles of the protection doctrine, the threats involved, and the agencies that would be obliged to take protective measures.[18] It also acted as a team for guiding the National Information Security Authority for securing computer infrastructures in the Israel Security Agency (ISA).

The National Information Security Authority, which was established the same year, operates in the framework of the ISA Law. The Authority guides the entities defined as essential in matters of computer security and protection of networks, and supervises the implementation of information security and protection. It is also authorized to enforce sanctions against entities that fail to comply with its guidelines. Significantly, the various security agencies take independent action to protect critical infrastructures without any official guidance from the Information Security Authority.[19]

The Decision to Establish the Israel National Cyber Bureau

In November 2010, the Prime Minister authorized National Research and Development Council chairman General (ret.) Prof. Isaac Ben-Israel to present a working plan for a national initiative for coping with the cyber threat.[20] The initiative team's recommendation included the establishment of a national cyber defense bureau for promoting cyberspace defense in Israel (recommendation 1A) and expanding the ISA's authority to the civilian sector.[21]

The key document in the matter is the Cabinet resolution of August 7, 2011 on the subject of "promoting national capability in cyberspace."[22] This decision provided for the founding of the National Cyber Bureau, and established its goal as "promoting national capability in cyberspace and improved handling of its current and future challenges." One of the Bureau's jobs is "to recommend a national cyber policy to the prime minister and the government, provide guidance for the relevant parties concerning the policy decided... implement this policy, and control its implementation."[23] The decision to establish the bureau, which was announced publicly, indicated significant progress in the government's handling of the cyber threat, and constituted a turning point on the issue.

While government agencies, military branches, and defense establishment entities are protected under the law, most of the business sector and ordinary civilians remain without adequate protection in this area. The business sector is not subject to official supervision, and is not subordinate to any national agency whatsoever that is responsible for checking its ability to handle an attack on its essential computer systems in an emergency. This is a significant weak point for Israel, whose economy depends on the production and export power of its business and industrial sector.[24]

Decision makers in Israel expect the next war to include the use of cyber warfare tools. In spite of this, there is currently no official agency in Israel directly responsible for the protection of the business sector. It is true that a national authority cannot replace the managers responsible for their businesses, but since some of the private organizations in the economy provide essential services for the continuation of normal life on the home front, there are grounds for government intervention in guidance, regulation, and supervision.[25]

With the establishment of the National Cyber Bureau, its chairman, Dr. Eviatar Matania, stated that in his opinion, there were five areas concerning cyberspace in which the state should intervene:

a. Creating a system-wide perspective on the national level: Cyber defense requires multi-system assessment because public systems and private and business systems are highly interdependent.
b. Pooling of resources, actions, and information: Pooling means consolidating resources from various sources into a single integrative

entity for the sake of handling the threats facing Israel in an optimal manner.

c. Creating international cooperation: Israel should take the initiative in creating such cooperation by partnering with allies throughout the world.
d. Creating an arrangement in cyberspace: Standardization, licensing, and approval, as well as introducing a system in which organizations and individuals are able to protect themselves according to clearly defined standards.[26]
e. Promotion of processes by the state: Just as the state acted in the 1960s to promote aviation in Israel by establishing an aeronautics faculty at the Israel Institute of Technology (Technion), so it should supply tools and leverage as incentives for academic and industrial development in the cyber field.[27]

According to Matania, the goal of the National Cyber Bureau is to draft a general plan of action in the field of cyber defense: strengthening security in organizations by creating an arrangement tailored to the databases, encompassing various sectors, as well as an individual arrangement for each sector. Another element involves devising national programs, cooperation, and information sharing, especially between the defense and civilian systems.[28]

The substance of the Bureau's activity concerns the regulation, integration, and promotion of general government activity affecting the cyber realm from a broad perspective, both military and civilian. The Bureau acts in the spirit of the Cabinet decision, together with the relevant entities, to formulate a defense policy, devise a national defense doctrine, and generate cooperation between all the entities operating in the field. It also formulates comprehensive programs and constructs mechanisms for nurturing human capital in the cyber field; develops technological and research infrastructures in the universities and industry; promotes cooperation among the private business sector, the public sector, industry, the universities, and the defense establishment; promotes public awareness of the cyber threat, and so on.[29]

All this activity indicates that Israel has correctly identified the looming threat to its national infrastructures, and has acted to set up a defense apparatus at the national level. Two watershed events were the establishment of a national information security authority in 2002, and the

Cabinet decision in 2011 to "promote national capability in cyberspace" and to establish the National Cyber Bureau. Nevertheless, the Israeli government has not yet disseminated a regular and unified strategy in this matter to the public.

Israel is one of the world's leaders in cyber capabilities. Typically, however, this is not appropriately reflected in the institution of a regular strategy or in a clear statement of an official course of action. It appears that Israel has yet to formulate a strategy in this field,[30] and that most of the information comes from press releases and media reports, rather than from official government sources. The government has taken an official decision in the matter, but has not yet published an orderly strategy.

Allocation of Resources

This section will examine the budget and resource allocations for coping with the threat posed by the development of cyber warfare technology, on the assumption that a budget assessment will make it possible to draw conclusions about the importance of the subject for decision makers in Israel.

In 2007, the National Research and Development Council initiated and financed research on the topic "Indices for Science, Technology, and Innovation in Israel," in cooperation with the Central Bureau of Statistics. The purpose of the study was to examine the budget allocations for scientific and technological matters in Israel. The study showed that Israel had spent NIS 30 billion annually on civilian research and development (R&D) over the past decade. An examination of the proportion of GDP invested in R&D showed that Israel led the world in 2009 – 4.3 percent, as compared with a 1.8 percent average in Organization for Economic Cooperation and Development (OECD) countries. Most of this investment in Israel (79 percent) comes from the business sector. Direct government spending on civilian R&D totals NIS 5 billion, in addition to the funds allocated for R&D in the defense sector.[31]

The figures show that Israel and its business sector invest considerable amounts in R&D in the technological field. To this can be added the various budgets distributed over the past year for R&D in applied and theoretical topics in the cyber sphere.[32] The total figure means that we can assume that R&D in the cyber field is being budgeted because its growing importance

for the nation's security has been acknowledged. The exact allocations have not been publicly disclosed.

One of the principal items in the 2011-2012 state budget consists of allocations for the "defense and public order category." This category includes the allocation from the general state budget for defense and public order. Funds from this budget are allocated to various defense agencies responsible for the cyber sphere. The budget for this category totaled NIS 61.8 billion in 2011 and NIS 63.4 billion in 2012. From these sums, the highest amount was allocated for spending on activities of the Ministry of Defense, which accounted for 18 percent of the total budget spending.[33] It can be assumed that the Ministry of Defense also invests considerable amounts in the development of cyber warfare by agencies for which it is responsible.

Another recommendation by the National Cyber Initiative team was to establish a national R&D program for building cyber capabilities in cooperation with the defense establishment, the universities, and industry. The plan included a recommendation for directing the existing national resources and adding resources where necessary. The aim of all this is to place Israel among the five leading countries in the world in cyber capabilities by 2015.[34] While this does not necessarily involve military-security development, it is highly probable that at least some of the money will be allocated to cyber security development.

The Cyber Bureau Budget

In the August 2011 Cabinet decision to establish the National Cyber Bureau, it was decided that an allocation for the bureau would be made, via the Office of the Prime Minister, from Ministry of Finance sources.[35] The full budget allocated for the Bureau's activities is not mentioned in the decision – only a minor amount (NIS 4.5 million) allocated for "establishing and operating the Bureau" in 2011.

The Cyber Bureau budget is currently NIS 2.5 billion for the next five years – about NIS 500 million per year. Of this, NIS 100 million will be allocated from the state budget as a designated amount for the Cyber Bureau, and NIS 400 million will be given following a process of pooling money from various sources.[36] According to Major Tal, a senior figure in the Cyber Bureau, the Prime Minister regards the cyber field as being of the greatest importance, and is actively promoting it. There is a desire to

develop the field, and the budget allocations reflect this. The cyber threat is gathering steam, and a long term program to guarantee its budget is being planned.[37]

A May 2012 Knesset Finance Committee meeting explicitly allocated money for the continuation of the Bureau's activity, in addition to the already allocated budget.[38] The Bureau's request, as submitted for the Committee' approval, included NIS 12 million for two main items. The first was an operating budget, including payment of salaries to Bureau staff, the creation of computer infrastructures, and physical security for the classified agencies required for infrastructures of this type. The second was the initial budget funding for the Bureau's regular activity.[39]

In recognition of the importance of links among the universities, industry, and the Cyber Bureau, the Bureau, in cooperation with the Ministry of Science and Technology, allocated NIS 50 million over three years for scholarships and research in various sub-sectors of the cyber sphere in order to make Israel a global leader in the field.[40] In addition, the Chief Scientist of the Ministry of Industry, Trade, and Labor announced an NIS 80 million allocation for Project KIDMA[41] for the purpose of promoting R&D and entrepreneurship in cyber security.[42] Here, too, one can assume that some of these scholarships will be allocated to areas dealing with cyber warfare.

Given the paucity of statements dealing with this budget, it is difficult to make an accurate estimate of government investment in Israel for the purpose of coping with the cyber threat. Nevertheless, the figures presented above show that the threat posed by the development of cyber warfare technology has not escaped the attention of Israeli decision makers, and that considerable resources are being channeled into this field.

Public disclosure of cyber budget allocations began in 2011. Taking into account the defense establishment's leading role in the handling of cyberspace over the past decade and the secrecy surrounding it, it is almost certain that various allocations in this field are not openly publicized. At the same time, following the official Cabinet decision in August 2011 to establish the National Cyber Bureau, information about allocations for military buildup and R&D in the field began to be made public.

Changes in Force Buildup

Cyber warfare technology has altered the weapon systems used on the modern battlefield, rendering them more precise and effective. Following the many changes that have taken place in Israel's external environment, the security challenges facing it have multiplied, and the importance of intelligence in Israel's security doctrine has increased. Israel is now at the forefront of technology, and has integrated cyber technology tools on all fronts in order to deal with the threats against it.[43]

Developments of this type have had a considerable effect on the principles of warfare and the changes that have occurred in the structure of armies, including the IDF. Upon examining the role of technology in Israel's wars, Prof. Ben-Israel asserted that a more technologically advanced battlefield signifies that flexibility and versatility play a more crucial role in modern warfare. For example, the Yom Kippur War clearly demonstrated that constructing electronic weapon systems against the enemy's known threats was insufficient; it is necessary to construct them so that they will be able to handle changes made by the enemy in the electronic parameters of its systems during the course of the fighting.[44]

Following is an analysis of the principal changes in the government and defense establishment agencies in Israel, given the growing recognition of the risks resulting from the development of the cyber threat and the appearance of cyber technology on the battlefield.

The National Cyber Bureau

In August 2011, the Prime Minister announced the establishment of the National Cyber Bureau, whose main function is to strengthen capabilities for the defense of Israel's critical infrastructure systems against terrorist cyber attacks by either foreign countries or terrorist groups.[45] The Bureau, which has been operating for over 18 months and is in the throes of a growing process, currently consists of four main departments: security, civilian, intelligence and situation assessment, and organization and policy. In addition, a control room that operates 24/7 and is in continuous contact with the security agencies dealing with the field has been established in Jerusalem. The control room facilitates a comprehensive perspective of all the threats as well as the possibilities for coping with them, so that when a cyber attack against one agency takes place, it will be possible to know in real time which other agencies should be protected.

The Cyber Bureau is responsible for three main areas:

a. Formulating Israel's official security doctrine in cooperation with the agencies responsible for defense. The doctrine operates on two levels: increasing the general level of security and increasing the level of national security.
b. Developing infrastructures and promoting Israel's leading position in the cyber field, among other things by increasing its human capital and supporting the topic of scholarships for cyber-related research.
c. Taking the lead in national cyber processes, such as by regulating the security market, creating national security infrastructure through legislation and emergency exercises, bolstering relations with various countries, and so on.[46]

The decision to establish the Bureau was an important step in Israel's engagement with the cyber challenge. It is still vital, however, to ensure that the Bureau acts according to a national strategy, to be formulated as soon as possible. Given Israel's procrastination in setting an orderly and publicly declared strategy, it is highly important that the Bureau be granted wide-ranging authority. Only then can it begin to narrow the national gap in comprehensive strategic management of all the civilian and military entities operating in the cyber sphere.[47]

The National Information Security Authority

The oldest entity dealing with the various aspects of information security is the National Information Security Authority, a branch of the Israel Security Agency (ISA). This authority grew out of a unit that handled conventional information security for decades, until it became responsible in 2002 for instructing all the national civilian infrastructure entities in defending against a possible cyber attack.

The ISA was legally sanctioned to regulate agencies like the Israel Electric Corporation, Mekorot National Water Company, Israel Railways, and the natural gas companies. The categories of regulation include issuing instructions about how to prevent a remote hostile takeover liable to cause severe damage to critical systems by pressing a key, and the like. In recent years, the list of entities instructed by the Authority has been extended as a result of national recognition of the growing cyber threat.[48]

Tsafrir Katz, who until recently headed the ISA Technology Division, provided a rare insight into what goes on there when he said that 20 percent

of ISA personnel were technology specialists. The character of the ISA has changed since the 1980s, when it was not technologically inclined. For several years, it was necessary to develop new forms of employment for younger people. From his perspective, this revolution continued throughout the past decade.[49]

The Israel Defense Forces (IDF)

In 2009, then-Chief of Staff Lieutenant General Gabi Ashkenazi defined cyberspace as "a strategic warfare and operating space for Israel." An IDF cyber bureau was then established to coordinate and guide the IDF's cyber endeavors for the General Staff. This bureau was founded in Unit 8200 of the IDF Intelligence Branch.[50]

A cyber defense department, most of whose activity is classified, was set up in the C^{4}I Corps (Teleprocessing Corps). The department enables operations on land, sea, and in the air to be conducted in an age when the IDF relies more than ever on computer technology. The department operates in cooperation with most of the IDF's elite units, utilizing an array of technological means to neutralize the enemy's cyber attacks.[51]

In order to protect the IDF's computer systems, the C^{4}I corps developed a training program called the "Cyber Defense Course." In May 2012, the corps' first class completed the course. After a few months of intensive study, the soldiers were qualified to carry out defensive computer-mediated operations based on the developing technological reality.[52]

Ministry of Defense

In January 2012, it was reported that the Ministry of Defense was about to set up a special administration for cyber warfare, which would coordinate all operations by security agencies and the defense industries involved in developing advanced systems in the field. During that year, special cyber warfare sections were established in the main defense industries, namely, Elbit Systems, the RAFAEL Armament Development Authority, and Israel Aeronautics Industries. Israel Military Industries is also considering entering the field.[53] It has not yet been decided who will head the new administration, but according to defense sources, the decision to establish a new authority "will raise the endeavor to a new level."[54]

Israeli Law, Information, and Technology Authority

The Israeli Law, Information, and Technology Authority (ILITA) was established by the Ministry of Justice of Israel in September 2006 to become Israel's data protection authority. ILITA's mission is to reinforce personal data protection, regulate the use of electronic signatures, and increase the enforcement of privacy- and IT-related offenses.[55] It also acts as a central knowledge base within the government for technology-related legislation and sizable governmental IT projects, such as e-gov (available online government).[56] ILITA is currently investigating the particulars of an event in which a large amount of personal information, including credit card data, was published on the internet by parties identifying themselves as Saudi Arabian hackers.[57]

"Available Government" – e-gov.il (Tehila)

The "available government" system was established in the Ministry of Finance's Accountant General's Department in 1997 as the Tehila unit. Its purpose is to enable people to carry out a broad range of operations through the internet, at the same time ensuring the security of the transferred information and safeguarding the user's privacy. The system utilizes many resources to safeguard privacy, including an expert information security team and some of the world's most advanced security technologies.[58]

Israel has done a good job of identifying the features of the cyber threat and making many corresponding changes in the way it constructs its forces: a National Information Security Authority has been established to deal with protecting the country's critical infrastructures; military agencies have instituted very important changes: the IDF Cyber Bureau was set up in Unit 8200, and the C^4I Corps has begun to develop a special cyber training program; the most important change was the establishment of the National Cyber Bureau, whose objective is to integrate cyber defense into both the various defense agencies and the civilian sector. A Law, Information, and Technology Authority has been set up to take responsibility for maintaining internet privacy and the security of personal information. It appears that over the past decade, particularly in the past two years, the state, recognizing that the cyber threat is liable to affect all facets of life, has stepped up its treatment of the cyber threat by establishing advanced designated entities.

Conclusion

Israel has been extremely efficient in identifying the features of the cyber threat arising from the development of cyber warfare technologies. It has begun to make the necessary changes, and there appears to be a close connection between how the cyber threat is addressed and national security. The handling of the problem focuses on three aspects: (1) defense organizations, the IDF, the intelligence community, and the defense industry, which as of now are taking independent action to protect their systems without direction from the ISA; (2) critical national infrastructures, which are subject to cyber attack, and which are being directed by the National Information Authority; (3) the private sector, in which civilian companies are exposed to cyber attacks. Although this aspect is partially addressed by ILITA, the bulk of the problem is not addressed at all.[59]

The cyberwar is raging in full force, and Israel is a leading player in it.[60] The dry facts are impressive: a National Cyber Bureau has been established in the Office of the Prime Minister; grants totaling millions of shekels will be allocated for cyber research and educational activities in each of the next few years; responsibility in the IDF for cyber affairs has been divided between the Intelligence Branch (offense) and the Teleprocessing Branch (defense); and the National Information Security Authority is expected to broaden its operations.[61] It appears that the treatment of cyberspace is gathering momentum in a number of key aspects: information about government activity concerning the cyber threat is being openly published, special budgets have been allocated for research in the field, and an attempt is being made to provide the National Cyber Bureau with a regular budget. At the same time, various agencies have been set up or have been greatly developed for the purpose of handling the growing cyber threat in an optimal manner.

The rapid technological changes that have occurred in recent years have affected the priorities of decision makers in Israel in various ways. Official Cabinet decisions have been publicized, and special agencies have been designated to address the cyber threat. Nonetheless, although at first glance it appears that Israel has made great strides in dealing with the growing cyber threat, there is still room for taking additional measures in order to achieve a clearer definition of the preferred policy for handling the matter comprehensively.

Notes

1 Isaac Ben-Israel et al., "Cyber Warfare – Israel's Preparation for Attacks on Computer and Communications Networks," in Protocol No. 95 – A Meeting of the Science and Technology Committee, Monday, July 4, 2011, http://www.knesset.gov.il/protocols/data/html/mada/;2011-07-04.html.

2 According to a report published in February 2012 by an international defense think tank (Security and Defense Agenda – SDA), in cooperation with the McAfee information security company, "Cyber-Security: The Vexed Question of Global Rules – An Independent Report on Cyber-Preparedness Around the World with the Support of McAfee." The report gave the US a four-star rating, http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf. See also Ehud Keinan, "Report: Israel More Prepared for Online Attacks than the US," *Ynet*, January 31, 2012, http//www.ynet.co.il/articles/0,7340,L-4183126,00.html.

3 A discussion paper at the High Committee for Science and Technology entitled "The National Cyber Venture" – a proposal to devise a national plan for building cyber capabilities that includes R&D, economic, academic, industrial, and national defense needs aspects, Tel Aviv, November 2012, p. 18.

4 Shmuel Even and David Siman-Tov, "Warfare in Cyberspace: Concepts, Trends, and Implications for Israel," Memorandum No. 109 (Tel Aviv: Institute for National Security Studies, 2011).

5 Ze'ev Schiff, "Meridor Committee Report: Concern that Middle Eastern Countries Will Acquire Nuclear Weapons in the Wake of Iran," *Haaretz* website, April 24, 2006, http://www.haaretz.co.il/misc/1.1100503.

6 Shay Shabtai, "Israel's National Security Concept – New Basic Terms in the Military-Security Sphere," *Strategic Assessment* 13, no. 2 (2010): 8-10.

7 Amir Buhbut, "Changing the Security Concept," *NRG Maariv*, April 24, 2006, http://www.nrg.co.il/online/1/ART1/076/915.html.

8 The government did not officially approve the proposal due to disagreements between the leaders. Nevertheless, the "defense" element has unofficially become part of the Israeli security concept.

9 Shabtai, "Israel's National Security Concept," pp. 8-10.

10 Rami Efrati and Lior Yafe, "That's How You Build a National Cyber Defense," *Israel Defense*, August 11, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2960.

11 Isaac Ben-Israel, "Technology Lessons," *Maarachot* 332 (1993): 13.

12 Amos Yadlin, "Cyber-Warfare – A New Dimension in Israel's National Security Doctrine," *Mabat Malam*, January 2010, p. 4, http://www.intelligence.org.il/KotarPort.aspx#http://malam.barebone.kotar.co.il/KotarApp/Viewer.aspx?nBookID=94837032&sSelectedTab=tdBookinfo%231.undefined.3.fitwidth.

13 Reuters News Agency, "Stuxnet Virus Used on Iran Was 1 of 5 Cyberbombs," *Ynet*, November 29, 2011, http://www.ynet.co.il/articles/0,7340,L-4168852,00.html.
14 Efrati and Yafe, "That's How You Build a National Cyber Defense."
15 Lior Tabansky, "Protection of Critical Infrastructure against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (2011): 72.
16 For more information about Tehila, see the final section, which discusses the design of forces.
17 Efrati and Yafe, "That's How You Build a National Cyber Defense."
18 "Protection of Computer-Based Systems," from the National Security Council Counter-Terrorism Bureau website, http://www.nsc.gov.il/NSCWeb/Templates/CounterTerrorismActivities.aspx.
19 Tabansky, "Protection of Critical Infrastructure against Cyber Threats," pp. 72-73.
20 In November 2010, the Prime Minister ordered the formation of a special team to formulate a national plan for placing Israel among the five leading countries in the cyber field. Work on this task, called the National Cyber Initiative, was led by the National Council for Research and Development, headed by Prof. Isaac Ben-Israel. The team, which included members from key agencies involved with the cyber realm in Israel, was composed of a number of sub-committees that examined the essential elements for coping with the cyber threat, and analyzed national welfare from an economic, academic, and national security perspective.
21 "The National Cyber Initiative," from the National Research and Development Council 2010-2011 report, July 2012, pp.10-17, http://knesset.gov.il/committees/heb/material/data/mada2012-10-15.pdf.
22 The decision was taken following comprehensive staff work by a national team headed by National Research and Development Council chairman Prof. Isaac Ben-Israel.
23 "Promoting National Capability in Cyberspace," Cabinet resolution No. 3611, August 7, 2011, from the website of the Office of the Prime Minister, http://www.pmo.gov.il/Secretary/GovDecisions/2011/Pages/des3611.aspx.
24 Efrati and Yafe, "That's How You Build a National Cyber Defense."
25 Yehuda Konfortes, "Wanted: An Iron Dome for Cyber that Will Protect the Home Front," *People and Computers*, February 1, 2012, http://www.pc.co.il/?p=79406.
26 Yossi Hatoni, "Dr. Eviatar Matania: Cyberspace Requires a Business and a National Policy Treatment – Not an Easy Task," from the CyberSec Conference that took place in February 2012, *People and Computers*, February 12, 2012, http://www.pc.co.il/?p=80025.
27 Ibid.
28 Speech by Dr. Eviatar Matania, 2nd International Cyber Conference, Tel Aviv University, June 9, 2012.
29 Efrati and Yafe, "That's How You Build a National Cyber Defense."

30 Except for publishing the Cabinet's decision to establish a National Cyber Bureau.

31 "National R&D Policy as a System of Integrated Tools," from a speech by Isaac Ben-Israel at the 2011 annual Herzliya Conference, http://www.herzliyaconference.org/_Uploads/dbsAttachedFiles/OriSlonim2.pdf.

32 "An Appeal for Scholarships in the Field: Cyber Defense and Advanced Computing," Ministry of Science and Technology and the Cyber Bureau, Office of the Prime Minister, http://exactsci-info.tau.ac.il/exact_sciences/site/temp/cybersco.pdf.

33 *State Budget Proposal for the 2011-2012 Financial Year, Main Points of the Budget and the Multi-Year Budget Plan*, Jerusalem (2010).

34 A paper for discussion by the National Council for Research and Development on the subject of the National Cyber Initiative – a proposal to establish a national program for building cyber capabilities that will combine R&D, economic, academic, and industrial aspects with national security needs, Tel Aviv, November 2012, p. 20.

35 "Promoting National Capability in Cyberspace."

36 From an interview with Prof. Isaac Ben-Israel at Tel Aviv University on the subject of the Cyber Initiative, August 5, 2012.

37 From an interview with Major Tal, a senior Cyber Bureau department head, at the Cyber Bureau in Ramat Aviv, August 23, 2012.

38 Ibid.

39 Protocol No. 1069, Meeting of the Knesset Finance Committee, Monday, May 1, 2012, www.knesset.gov.il/protocols/data/rtf/ksafim/2012-05-01-02.rtf.

40 "Prime Minister Netanyahu approved the National Cyber Bureau budget and work plan," from the Office of the Prime Minister's website, June 6, 2012.

41 The head of the National Cyber Bureau announced the launching of the KIDMA – Promotion of Cyber Security Research – Program on November 13, 2012. The program is a result of cooperation between the Bureau and the Chief Scientist of the Ministry of Industry, Trade, and Labor aimed at promoting R&D and entrepreneurship in cyber security in order to maintain and bolster the competitive potential of Israeli industry in this field in the global market.

42 A memorandum from the Chief Scientist: "The KIDMA – Promotion of Cyber Security Research – Program for improving the capabilities of Israeli industry in the cyber security sphere," November 21, 2012, http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf. See also "NIS 80 Million for Cyber Promotion," *Israel Defense*, December 30, 2012, http://www.israeldefense.co.il/?CategoryID=760&ArticleID=3796.

43 Shmuel Even and Amos Granit, *The Israeli Intelligence Community – Whither? Analysis, Trends, and Recommendations*, Memorandum No. 97 (Tel Aviv: Israel Institute for National Security Studies, 2009), p. 64.

44 Isaac Ben-Israel, "Technology Lessons," *IDF Publishing House*, 332 (1993): 10.
45 As discussed in detail in the section dealing with the formulation of strategy.
46 From an August 23, 2012 interview with Major Tal.
47 From a speech by Prime Minister Benjamin Netanyahu at the 1st International Cyber Conference at Tel Aviv University, June 9, 2011.
48 Amir Rapaport, "A Cyber Attack on National Infrastructure," *Israel Defense*, December 8, 2011, http://www.israeldefense.co.il/?CategoryID=536&ArticleID=1421.
49 Amir Rapaport, "Responding Quickly in Order to be Relevant," *Israel Defense*, April 3, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=2153.
50 Amir Oren, "The IDF's New Battlefield is Found in Computer Networks," *Haaretz*, January 1, 2010, http://www.haaretz.co.il/misc/1.1182490.
51 "Computer Professions – A Cyber Defense Course," Communications and Teleprocessing Corps website, http://www.tikshuv.idf.il/site/General.aspx?catId=60698&docId=76101.
52 Hadas Duvdevani, "The first IDF cyber course has been completed. The goal is three classes a year," IDF website, May 3, 2012, http://www.mako.co.il/pzm-soldiers/Article-595ec4bc4611731006.htm&sCh=3d385dd2dd5d4110&pid=1093150966.
53 "Disclosure: A New Cyber Administration," *Israel Defense*, January 12, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1657. No other reports about the administration in the Ministry of Defense have been published; a reasonable assumption is that the information is classified.
54 Amir Rapaport, "Disclosure: Cyber Defense Exercise," *Israel Defense*, January 19, 2012, http://www.israeldefense.co.il/?CategoryID=512&ArticleID=1706.
55 From a September 5, 2012 interview with ILITA head Adv. Yoram HaCohen in the government compound in Tel Aviv.
56 The Law, Information, and Technology Authority (ILITA) website, http://www.justice.gov.il/MOJHeb/ILITA/.
57 A press release by the Law, Information, and Technology Authority, Ministry of Justice Spokesman's Bureau, http://www.justice.gov.il/NR/rdonlyres/4C39E414-E501-48C2-9C53-8EB533FD8B7D/32913/dover5.pdf.
58 "All About Available Government," Available Government website, http://e.gov.il/AboutUs/Pages/AboutUs.aspx.
59 Yossi Hatoni and Gabi Siboni, "There is an entire layer of organizations that is unprotected against cyber attacks," from the CyberSec Conference at the Institute for National Security Studies on February 12, 2012, *People and Computers*, February 15, 2012, http://www.pc.co.il/?p=80466.
60 Foreign reports attribute Stuxnet, Flame, and other cyber events to Israel.
61 Amir Rapaport, "A Cyber Attack on National Infrastructure."