Israeli Defense in the Age of Cyber War

by Gil Baram

From the early days of statehood, technology occupied a prominent place in Israel's national security concept as it sought to establish a qualitative edge over its vastly more populated and better endowed Arab adversaries. In the past few years, a new technological challenge, that of cyber warfare, has grown to the point of becoming among the most critical threats to Israel's vital infrastructures in both the civil and the military-security sectors. Energy, water, communications and traffic networks, and an economy that relies heavily on computers must be viewed as being at risk. To respond to the new, evolving threats, Jerusalem must revise certain aspects of its security concept so as to ensure cyber superiority as an inseparable part of its national defense capabilities.

The Israeli government needs to be deeply concerned with defending its critical infrastructures from cyber-attacks, both in the civil and the military-security sectors. Energy, water, computer, communications and traffic networks, and the economy must be viewed at risk. A terrorist hacker could destroy a city's water system by attacking pressure level controls or purification systems.

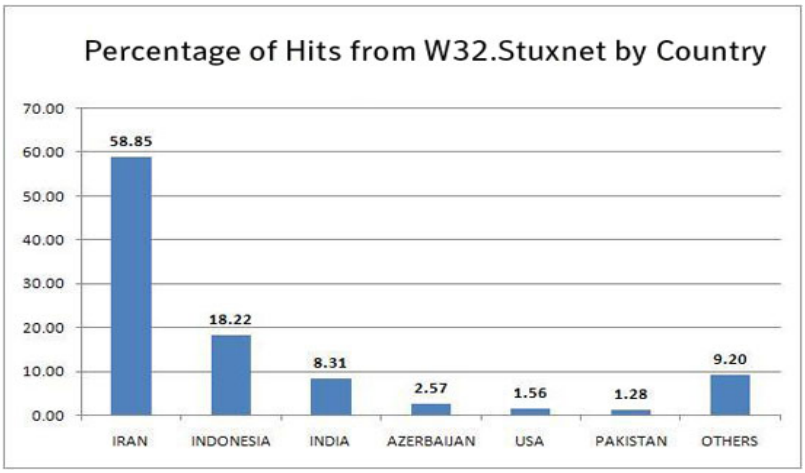
What Is the Cyber Threat?

Cyber warfare is commonly defined as "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."[1] A virus or a worm is essentially a program, often self-replicating and usually destructive, loaded onto a computer without the user's knowledge or wishes. A denial-of-service attack is a

1 "Cyber Warfare," RAND Corp., accessed Sept. 16, 2016.

disruption to a user's access to a computer network caused by malicious intent.

Countries conduct cyber-attacks mainly for political reasons to achieve strategic, economic, diplomatic, or military advantages by attacking military, government, or civil computer infrastructures. Cyber-attacks, like kinetic attacks, have a range of options—including denial of service attacks, vandalizing websites, espionage and information gathering, as well as attacks that can cause physical damage as did the Stuxnet worm that hit the Iranian centrifuges and was exposed in 2010.[2]



Advanced cyber capabilities are an effective way to deter Israel's enemies. One such example was the "Stuxnet" virus, attributed to a U.S. and Israeli operation, in which the functioning of centrifuges belonging to Iran's nuclear program was disrupted. Computers in other countries were also affected.

The vast progress made in computer and information networks has created a new reality in which military communications infrastructures are often connected to their civilian counterparts. Both infrastructures are increasingly dependent on computers, and their protection is critical for both civilian and national security purposes. Once it was recognized that computers were weak points, cyber warfare technologies began to emerge, designed to attack an adversary's data assets and even cause significant physical damage remotely to systems without employing conventional or non-conventional weapons or sending soldiers into the battlefield. At the same time, security agencies and armed forces worldwide have been developing cyber defense capabilities to protect these vital infrastructures.

This dependence on cyber technologies is a global phenomenon and has put at risk national and public infrastructures that were once regarded as inaccessible and well-protected. Israel, which has been under threat since its inception, has needed to adapt its national security posture accordingly.

In the traditional Israeli approach to security, much effort is invested in intelligence, early warning, and deterrence so as to minimize the expenditure involved in maintaining a continuous state of alert. In this context, three problems that underlie every cyber-attack should be mentioned. The first is the problem of attribution, i.e., who

[2] See, for example, Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2012), p. 6; Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities* (New York: Oxford University Press, 2015), p. 32.

ordered the attack and who launched it? The second is the difficulty in establishing the results of the attack and determining the extent of its success. The third problem is that of evidence: It is often difficult to determine whether the event under investigation occurred due to a technical failure or as a result of a cyber-attack.[3]

The Israeli "security triangle" has involved deterrence, early warning, and a decisive operational victory.

Israel's National Security Concept

The formulation of Israel's national security concept dates back to the pre-state era and continued to evolve in the face of the many threats that the nascent state had to address after its war of independence. Having concluded that the threat posed by its Arab adversaries was a given and persistent reality with which Israel was destined to contend in the foreseeable future, in October 1953, Prime Minister David Ben-Gurion presented a document to the cabinet regarded ever since as Israel's official national security doctrine.[4]

Peace was the ultimate strategic goal of Ben-Gurion's security concept. However, since peace was likely to remain elusive, he argued that the proposed security concept would at least make the Arab states accept the existence of a Jewish state, if only begrudgingly.[5] Essentially, the Israel that Ben-Gurion envisioned strove to have long periods of quiet and to hold off military confrontations as much as possible. However, if the need arose, it had to win a quick victory because of its small size and limited human resources. To this end, two principles were adopted. The first was the idea of "an army of the people" that could be rapidly mobilized and comprised mainly of draftees on mandatory military service and reserves. The second principle became known as the "security triangle": deterrence, early warning, and a decisive operational victory.[6] Ben-Gurion argued that Israel must forestall any Arab attempts to change the post-1948 war status quo by adhering to these three elements.

In Israel's national security concept, *deterrence* refers to developing defensive and offensive capabilities that will discourage the country's enemies from attacking it. Classical military theory maintains that deterrence is created when one side intimidates the other to the point that it avoids reverting to armed force, realizing that the likely costs of this move would far exceed its anticipated gains. Once this fear dissipates, deterrence no longer exists, and aggression is likely to follow. Jerusalem perceives deterrence as "cumulative" because it regards each of its wars as one round in a series of hostile episodes.[7]

Early warning denotes receiving advance warning about developments in neighboring countries that could put Israel's security in jeopardy. Early warning is critical if Israel and its economy are to keep functioning normally under what has been, for most of its existence, a permanent Arab military threat. Without early warning, Israeli forces would have to maintain a constant state of readiness that would undermine the

3 Yitzhak Ben Israel and Lior Tabenski, "An Interdisciplinary Look at Security Challenges in the Information Age," *Military and Strategic Affairs*, Dec. 2011, p. 33.

4 Yitzhak Ben-Israel, *Tfisat Habitahon shel Israel* (Tel Aviv: Ministry of Defense Publishing House, 2013), pp.125-53.

5 Ibid., p. 35.

6 Gideon Taran, "Mavo litfisat bitahon: musagei yessod umarkivim merkazyim," in *Mavo Lebitahon Leumi* (Tel-Aviv: Ministry of Defense Publishing House, 2002), pp. 21-36.

7 Ben-Israel, *Tfisat Habitahon shel Israel*, pp. 64-5.

economy and the nation's strength. As demonstrated by the opening stage of the October 1973 Yom Kippur War, early warning capabilities are vital if reserves are to be mobilized and forces moved to the front in time. Advance warning also enables the launch of a preemptive attack if necessary.[8]

Israeli troops during the October 1973 Yom Kippur War. As demonstrated by early victories by Arab armies in the opening stage of war, early warning capabilities are vital if reserves are to be mobilized and forces moved to the front quickly.

Achieving a *decisive operational victory* is predicated on building sufficient military power to win a conflict if early warning fails. A decisive operational victory compels an adversary to conclude that there is no point in going on fighting, reflecting not only the actual balance of power on the battlefield but also a psychological state by which political and military leaders perceive their situation.[9]

These three elements have underlain Israeli strategy from the country's early days and have served as guidelines for all the security agencies involved in building and operating its military power. By adhering to these principles, Israel has managed to cope with its quantitative inferiority and unique geostrategic position as a state under a constant military threat.[10] But nothing is static, and geopolitical changes and global technological advances have forced a rethinking of this strategy.

A New Paradigm?

Israel's success in implementing its national security concept eventually drove several Arab states to a grudging acquiescence in its existence. However, rapid technological developments within the last few decades and the momentous regional events of the past few years have seriously challenged this traditional security concept.

Increasingly, the Israeli government has invested considerable resources in promoting security-related technological research and in developing new, highly sophisticated combat means. The Israel Defense Forces (IDF) have aspired to base their power on advanced weapons and creative technological solutions, resulting in

8 Roni Amir, "Torat habitahon hi hasiba lekishlon hahatra'a be-1973," *Maarachot*, June 2013, p. 57.

9 Ben-Israel, *Tfisat Habitahon shel Israel*, pp. 62-3.

10 Avner Simhoni and Avriel Bar Yosef, "Tfisat habitahon—shimur veidkun," *Maarachot*, June 2012, pp. 13-4.

the IDF becoming the most advanced army in the Middle East.[11]

The history of Israel's wars demonstrates that, over time, the IDF has significantly improved its use of technology while the importance of technological measures in the battlefield has grown. The 1973 war drove the IDF to develop its electronic and electro-optic capabilities by using computerized systems such as electronic weapon systems and radar systems. The ultimate goal was to improve the country's fighting capabilities and enhance its performances on the battlefield. According to former IDF major general Yitzhak Ben Israel, this war had a direct effect on the development of advanced weapon systems and the military doctrine of Israel.[12]

Over the years, the importance of computer warfare and cyber warfare technologies has not escaped the attention of those in charge of Israel's national security. The IDF identified the enormous potential of computers and engaged in various types of computer warfare as early as the 1990s. Initially though, the focus was on "information security," the term commonly used to describe the protection of computerized systems. The need for such security stemmed from the view that protecting sensitive information (classified or sensitive business information) was of the utmost importance. In time, the meaning of computer security expanded to include other threats such as denial of services, disabling vital, computer-based processes, and causing damage to computers in a way that could harm physical infrastructures. On a national level, the protection of computerized systems is now referred to as "cyber defense."[13]

The IDF has aspired to base its power on advanced weapons and creative technological solutions, resulting in it becoming the most advanced army in the Middle East. The unmanned ground vehicle, Guardium, pictured here, makes it possible for Israeli soldiers to defend the country while not risking their lives.

In 2002, the Ministers Committee on Security Affairs issued a resolution titled "Responsibility for the defense of computerized systems in the State of Israel" (resolution 84/b), which outlined the defense principles for Israel's critical

11 Yitzhak Ben Israel, "Bitahon, technologia usdeh hakrav haa'tidi," in *Mirkam Habitahon*, H. Golan, ed. (Tel Aviv: Maarachot, 2001), p. 270.

12 Yitzhak Ben Israel, "Lekahim Technologim," *Maarachot*, Oct. 1993, p. 9, 12.

13 Rami Efrati and Lior Yafeh, "The challenges and opportunities of national cyber defense," *Israel Defense*, Aug. 11, 2012.

computer-supported infrastructures. The country's response to the cyber threat faced by its essential national computer systems is based on this document.[14]

Israel's future as a democratic, open society depends on the capability to protect the country's vital computer networks.

Following the resolution, a steering committee was established later that year, tasked with compiling a list of steps to be taken to defend the nation's vital computer systems. The committee convened periodically and formulated the principles of defense and the bodies required to take special precautions. The National Information Security Authority, which operates under the Israel Security Agency (ISA) law, was also created in 2002. It guides organizations that have been deemed vital on matters of computer security and network protection and oversees the implementation of information security and protection instructions.[15]

In April 2006, the Committee on Israel's Defense Doctrine headed by Dan Meridor, a former deputy prime minister and minister of intelligence, submitted to then-defense minister Amir Peretz a proposal for an updated national security concept.[16] The committee recommended adding the term "defense" to the three previously mentioned components of the national security triangle and to update its defense strategies accordingly.[17]

Augmenting the National Security Concept

Defense is an extremely important concept in cyber warfare because effective defense guarantees that the country's vital systems continue functioning. Developing operational capabilities in the cyber arena is essential to safeguarding Israel's national strength. Its economy and its future as a democratic and open society depend largely on the capability to protect the country's vital computer networks from any disruption of normal life. The growing dependence on computer systems both in Israel and around the world has given rise to new challenges that require an immediate national-level response.[18] Since the Meridor committee submitted its report, cyber warfare technologies have been increasingly used on the modern battlefield.[19]

In 2009, Lt. Gen. Gabi Ashkenazi, then chief of general staff, defined cyberspace as a "strategic and operative combat zone for Israel."[20] Following this statement, in 2010 a cyber headquarters was set up in the Israeli National Signals Intelligence (SIGINT) and Code Decryption Unit, or 8200 as it is commonly known, to coordinate and direct military cyberspace operations.[21] A cyber defense department

14 Prime Minister's Office, "Background for the Establishment of the Bureau," Jerusalem, accessed Sept. 23, 2016.

15 "Cyberwellness Profile—Israel," International Telecommunications Union, Geneva, Jan. 22, 2015.

16 *Haaretz* (Tel Aviv), Apr. 24, 2006.

17 Shai Shabtai, "Israel's National Security Concept: New Basic Terms in the Military-Security Sphere," *Strategic Assessment*, Institute for National Security Studies, Tel Aviv, Aug. 2010, pp. 9-10.

18 "Hameizam hakiberneti haleumi: hatza'a lehakamat tochnit leumit livniyat yecholot kibernetiot beshiluv heibetei mehkar ufituah, kalkala, akademia, ta'asiya vetzorhei habitahon haleumi," Science and Technology Committee, Tel Aviv University, Nov. 2012, p.18.

19 Yitzhak Ben Israel, et al, "Lohama Kibernetit—he'archut medinat Israel lemitkafot al rishtot mahsehvim vetikshoret," Protocol 95, Science and Technology Committee meeting, July 4, 2011.

20 Hanan Greenberg, "Virus bimkom matos," *NRG*, Nov. 11, 2011.

21 *Haaretz*, Jan. 1 2012.

was also established in the C4I Corps, a combat support unit responsible for all areas of tele-processing and communications in the IDF. Although most of its activity is classified, this department is known to facilitate land, air, and sea operations in an era when the IDF is significantly dependent on computers and communication networks. The department works in cooperation with most of the defense force's elite units and uses varied, advanced technological means to counteract enemy cyber-attacks.[22]

In June 2012, defense minister Ehud Barak revealed that Israel had the capability to launch offensive cyber-attacks.

In June 2015, IDF chief of staff Gadi Eizenkot decided to establish an independent cyber branch in order to lead the cyber warfare activity of the forces.[23] This branch will join the Israeli air force, navy, and GOC army headquarters as a main service branch that will oversee the military's cyber warfare strategy. Eizenkot has also instructed military intelligence director Herzl Halevi to form a special think tank to review the military's cyber framework.[24]

At the Second International Cyber Conference held at Tel Aviv University in June 2012, then-defense minister Ehud Barak revealed for the first time that Israel had the capability to launch offensive cyber-attacks. While stressing that in warfare of this kind preference should be given to defense rather than to offense, he revealed that Israel had both capabilities.[25]

To date, there is no publicly available document outlining Israel's official strategy on ways to deal with cyber threats, though the Israeli government resolution 3611 provides the national governance roadmap for cybersecurity.[26]

In 2011, the National Cyber Bureau was established to formulate an official cyber defense concept, determine state-level preparations in this field, and supervise national procedures and cooperation. In February 2015, the Israeli government approved the establishment of the National Cyber Security Authority under the supervision of the National Cyber Bureau. This operational authority has several missions: threat analysis and early warning; active defense operations; operating the CERT-IL (Israel National Cyber Event Readiness Team) and creating national regulation for the emerging cyber professions.

In April 2016, the National Cyber Security Authority began its official work. Its primary function is to oversee "cyber defense actions so as to provide a comprehensive response against cyber-attacks including dealing with threats and events in real time." The authority's director is subordinate to the head of the National Cyber Bureau, defined as the head of the national cyberspace operation. In 2016, the new authority was slated to recruit more than one hundred employees.[27]

22 "Cyber Command: Defeating the Enemy that Can't Be Seen," Israel Defense Forces blog, Jerusalem, Dec. 22, 2015.

23 Shmuel Even, David Siman-Tov, and Gabi Siboni, "Structuring Israel's Cyber Defense," *INSS Insight*, Sept. 21, 2016.

24 *BreakingIsraelNews* (Beit Shemesh), June 22, 2015.

25 *Haaretz*, June 6, 2012.

26 "Cyberwellness Profile—Israel," International Telecommunications Union, Geneva, Jan. 22, 2015.

27 "Cabinet approves establishment of National Cyber Authority," Israel Ministry of Foreign Affairs, Jerusalem, Feb. 15, 2015.

In April 2014, hundreds of Israeli websites—banks, schools, nonprofit organizations, newspapers and government agencies—were attacked by hackers from the "Anonymous" collective as part of an anti-Israeli operation called "Op-Israel." Israel's national Computer Emergency Response Team was able to repel these attacks quickly, and most of the websites continued working normally.

Cyber Warfare in Action

Israel is perceived as a world leader in cyber capabilities. In a report that examined the cyber preparedness of twenty-three countries, Israel received the highest score (4.5 stars out of 5). The report's authors praised Israel's defense systems and noted that the country was well prepared to handle a cyber-attack.[28]

Such attacks are not mere theoretical dangers. In May 2013, following an Israeli airstrike on Damascus, a group called the Syrian Electronic Army claimed it had attacked the remote monitoring and control system that manages the main water infrastructure of Haifa.[29] Again, in April 2014, hundreds of websites, including those of banks, schools, nonprofit organizations, newspapers, and government agencies were attacked by hackers associated with the Anonymous collective as part of an anti-Israeli group operation called OpIsrael. Jerusalem was well prepared for these attacks as the national Computer Emergency Response Team reported that most of the attacked websites were operating normally.[30]

At present, the Israeli government stands at the forefront of using cyber technologies against the threats the country faces in all arenas. Cyber warfare leans on independent Israeli capabilities, combining local inventiveness with international technologies.[31] The approaches Jerusalem takes also merge with and reinforce the three original requirements of Israel's traditional national security concept:

(a) Deterrence: Advanced cyber capabilities may be an effective way to deter Israel's enemies. One such example was the Stuxnet operation attributed to the United

28 *Homeland Security News Wire* (Mineola, N.Y.), Feb. 2, 2012; "Cyber-security: The vexed question of global rules," p. 66-7.

29 *The Jerusalem Post*, May 25, 2013.

30 RT Television Network (Washington, D.C. and London), Apr. 6, 2014; *Ynet* (Tel Aviv), Apr. 7, 2014.

31 Amos Yadlin, "Hameimad hehadash shel halehima—cyber," *Meimad Malam*, Jan. 2010, p. 4.

States and Israel, in which the functioning of centrifuges belonging to Iran's nuclear program was disrupted.[32] The event has been widely viewed as a turning point in cyber warfare, demonstrating that governments are able to launch cyber-attacks that can be extremely effective.[33] While the effectiveness of cyber deterrence is still being debated,[34] the Iran-Stuxnet event offers an interesting case study. While Tehran did not stop its nuclear pursuit, the Stuxnet revelation may have prompted other enemies of Israel to reconsider the use of force against it in the coming years.

Cyber warfare allows Israel to initiate operations against remote targets without risking the lives of citizens and soldiers.

(b) Early warning: Advanced cyber technologies can enable the collection of large quantities of accurate information about an adversary's intentions and future plans. By using such capabilities, Jerusalem can gather much high-quality information about its enemies and block access to its own databases at the same time. Thus, Israel's security agencies can provide the defense establishment with effective warnings about an adversary's intentions in order take the necessary measures against them at the right moment.

(c) Decisive operational victory: By applying their advanced cyber tools, Israeli forces can gain advantages in combat that could tip the scales in the country's favor. For example, during the 2007 attack on Syria's nuclear reactor, which has been widely attributed to Israel, Syria's radar systems were incapacitated by a hostile code that transmitted apparently normal signals.[35] This enabled the Israeli air force to penetrate Syrian airspace undetected and target the nuclear complex, destroying it completely.

While during Operation Protective Edge in Gaza (July-August 2014), Israeli forces focused most military operational protection efforts on rocket and tunnel attacks, evidence has emerged that the IDF had also to deal with cyber threats during the fighting from such radical factors as Iran, Hamas, and Hezbollah. In the words of the IDF's cyber defense division commander: "It wasn't like this in previous operations. For the first time, there was an organized cyber defense effort alongside combat operations in the field. This was a new reality."[36]

Although Israel's cyber protection agencies neutralized these attempts quickly

32 *Ynet* (Tel Aviv), Nov. 29, 2011; *The New York Times*, June 1, 2012.

33 *The New York Times*, June 1, 2012; Bruce Schneier, "The Story behind the Stuxnet Virus," *Forbes* (New York), Oct. 7, 2010.

34 For studies on the problems of cyber deterrence, see, for example, Martin Libicki, *Cyber Deterrence and Cyberwar* (Santa Monica: Rand Corporation, 2009); Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs*, Dec. 2011.

35 *Wired* (San Francisco), Apr. 10, 2007; *Haaretz*, Aug. 3, 2012.

36 "The Attack against Israel You Haven't Heard About," Israel Defense Forces blog, Aug. 22, 2014.

and easily, it appears that Tehran had invested much effort in developing effective attack measures against Israel's critical infrastructures.[37] This was publicly confirmed by both Prime Minister Binyamin Netanyahu and then-defense minister Moshe Ya'alon in September 2014 after the fighting.[38]

Conclusion

Today's cyber threats are the direct outcome of the critical role computerized systems play in national infrastructures and modern life. Different systems and sectors developed separately and eventually converged to form a cyber-network that typically was not security oriented. As it became clear that it would be necessary to deal with the security aspects of cyber life, Israeli leaders were compelled to imagine what a future cyber battlefield might look like and the requirements needed to be victorious in it.

Developing strategies to engage in and defend against cyber warfare also jibe with other aspects of the Israeli situation. Cyber warfare allows Israel to initiate operations against remote targets without risking the lives of its citizens and soldiers, a cardinal goal of such a small country with limited human resources. Operations of this kind also gain Israel worldwide prestige, which can contribute both economically to the country's bottom-line—as other nations look to the Jewish state for expertise and advanced technologies and application—and reinforce deterrence. For example, at the January 2014 launch of CyberSpark—the Israeli Cyber Innovation Arena in Beersheba—Netanyahu said, "Beersheba will not only be the cyber capital of Israel, but one of the most important places in the cyber security field in the world."[39] Building on the success of Deutsche Telekom working in the city in collaboration with Ben-Gurion University, a number of multinational giants have opened centers of excellence in Beersheba, including EMC2-RSA, Lockheed Martin, Oracle, and IBM. In addition, JVP Cyber Labs is the first incubator for fledgling cyber companies investing in technologies that are set to revolutionize the future of cyber security.[40]

While Israel appears to be dealing with the cyber threat in advanced ways consistent with its general national security concept, additional measures will likely have to be taken as time goes on. One of this measures may be creating cooperation between the different security agencies in charge of cyber defense so as to establish the optimal policy for cyber defense and determine what national preparations must be made to this end.

Gil Baram is a Ph.D. candidate at the School of Political Science and International Relations at Tel-Aviv University, and a research fellow at the Blavatnic Interdisciplinary Cyber Center (ICRC).

37 *Calcalist* (Tel Aviv), Aug. 18, 2014.

38 *The Jerusalem Post*, Sept. 14, 2014; *Globes* (Rishon Le-Zion), Sept. 15, 2014.

39 "CyberSpark—The Israeli Cyber Innovation Arena," Ben-Gurion University of the Negev, accessed Oct. 31, 2016.

40 Hunter Stuart, "The Future of Cybersecurity Is Being Written in the Israeli Desert," *MotherBoard*, Feb. 1, 2016; "CyberSpark."