Military and Strategic Affairs

Volume 3 | No. 1 | May 2011

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY
אוניברסיטת תל-אביב

Military and Strategic Affairs

Volume 3 | No. 1 | **May 2011**

CONTENTS

Military and
Strategic Affairs

The purpose of *Military and Strategic Affairs* is to stimulate and enrich the public debate on military issues relating to Israel's national security.

Military and Strategic Affairs is published three times a year within the framework of the Military and Strategic Affairs Program at the Institute for National Security Studies. Articles are written by INSS researchers and guest contributors. The views presented here are those of the authors alone.

Graphic Design: Michal Semo-Kovetz, Yael Bieber
Tel Aviv University Graphic Design Studio

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 61398 • Israel
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: info@inss.org.il

Military and Strategic Affairs is published in English and Hebrew.
The full text is available on the Institute's website: www.inss.org.il

Iranian Involvement in Lebanon

Eyal Zisser

Israel's military engagement with Hizbollah in the summer of 2006 has been called by many different names and monikers, including, of course, the Second Lebanon War, which was adopted by Israel as the official name of the war. Some commentators on Arab television stations called it the sixth Arab-Israeli round. In truth, however, most of the Arab world, at least its leaders and important segments of its ruling elites, supported Israel, and more precisely, stood aside with the expectation, which ultimately was not met, that Israel would defeat Hizbollah. Hence this was not another round in the battles between Israel and the Arabs, a direct continuation of the bloody conflict of over one hundred years between the Zionist movement and the Arab national movement, and between Israel and the Arab states and the Palestinians. Rather, it seems more accurate to call this war – as in fact, several commentators proposed during the course of the fighting – the First Israel-Iran War.[1] Latent in this term was the sense that Iran had succeeded in establishing its presence on the Mediterranean coast, and that for the first time this presence sparked an all-out war in which an organization, inspired by Iran and armed with Iranian weapons, fought against Israel.

The Iranian presence in Lebanon, Iran's major influence and perhaps even control over Hizbollah, and its ability to motivate the organization to act in its name and under its auspices are a known reality, including in Israel. Nevertheless, the question that remains is whether the Iranian presence in Lebanon and Iran's control over Hizbollah will turn all of

Professor Eyal Zisser is the Dean of the Faculty of Humanities and holds the Yona and Dina Ettinger Chair of Contemporary Middle Eastern History at Tel Aviv University, and is a senior research fellow at the Moshe Dayan Center for Middle Eastern and African Studies.

Lebanon into an Iranian vassal or satellite, giving Tehran complete freedom of action in Lebanon and against all the forces operating there.

Surprisingly, it was actually Bashar al-Asad who addressed this question from a singular angle. In an interview in late 2010 with the Arab newspaper *al-Hayat*, the Syrian president was asked to compare Tehran's influence in Iraq with its influence in Lebanon. After all, Syria preceded Iran as kingmaker in the Lebanese arena, and to a large extent Tehran exploited the weakness of Damascus and its having been pushed out of Lebanon to take its place. Although Bashar did not provide an entirely expected answer, the response is understandable to anyone deeply familiar with the Syrian-Iranian relationship, as well as Syrian ambitions in Lebanon. In his response, Bashar was unable to avoid taking a stab at Tehran as he attempted to draw Syria's red lines vis-à-vis Iran:

> It is not possible to compare what is happening in Iraq with what is taking place in Lebanon. It is therefore impossible to compare the role played by Iran in Iraq with the role it is seeking to play in Lebanon. Furthermore, Syria's geographic tie to Lebanon is completely different from the tie between Iran and Iraq. Therefore, it can be said that Iran does not get into fine details in the Lebanese context, but takes a detached panoramic view and deals only with major issues. What is important to Iran is to maintain the resistance [Hizbollah]. Syria, on the other hand, familiar with the fine details of the Lebanese arena, knows these minute details much better than Iran and deals with them, since after all, it has decades of experience with the Lebanese issue.[2]

It is quite possible that Bashar, and with him Syria, missed the train that has already left the station, and that Damascus will find it difficult if at all possible to regain its longstanding influence in Lebanon and undermine Tehran's presence. But it is also possible that the battle for Lebanon is not yet over, and that what appears to be Iranian domination in Lebanon is neither the complete nor the completed picture. This may be seen, for example, in the historic − if somewhat comical − visit of Mahmoud Ahmadinejad to Lebanon in October 2010. Hizbollah gave the Iranian president a welcome fit for a king. Posters with "*khosh amadid*" (welcome, in Persian) lined the roads to the Shiite areas of Beirut and the Bekaa Valley and to the south. However, the visit also exposed the dispute within Lebanon regarding Iran's influence in the country. Many Lebanese in the Sunni and the Christian camps did not hesitate

to declare that Ahmadinejad was not their guest and was not welcome, and therefore Ahmadinejad's visit was limited to Shiite areas. This phenomenon was mirrored one month later, in November 2010, with the visit to Lebanon, this time mainly to Sunni areas, by the prime minister of Turkey – an Iranian ally, who is actually competing for influence in the region. Here too posters adorned the streets, but this time they were in Turkish: "*hogeldin*" (welcome, in Turkish).[3]

Events in Lebanon took a dramatic turn in early 2011 with the collapse of the Saad al-Hariri government, following the resignation of Hizbollah representatives and their allies in the government. The background to the dismantling of the government was Hizbollah's demand that the Lebanese government disavow the international tribunal investigating the assassination of former prime minister Rafiq al-Hariri. Lebanese Druze leader Walid Jumblatt subsequently announced his defection to the opposition from Hariri's March 14 camp. Following this move Najib al-Miqati was delegated the task of forming a new government, which under the circumstances will function under the auspices and control of Hizbollah. Miqati is known for his close ties with Syria, and Walid Jumblatt's moves came in the wake of orders he received from Damascus. For this reason, Lebanon's future does not necessarily entail a takeover by Hizbollah and Iran, and perhaps heightened tension between Iran and Syria over control of Lebanon is the more likely scenario. Not only has the struggle for Lebanon not ended, but in a sense it is just beginning with new-old players.

The Roots of Iranian Involvement in Lebanon

The Islamic Republic of Iran should be seen as the successor of the Iranian state entity that existed throughout history in the space occupied today by Iran, and accordingly, this is an entity that has more than two thousand years of history behind it. From the dawn of history the state entity that stretched over the Iranian highlands – today's Iran – eyed the expanses to its west as a possible region of influence and a security zone. The Persian Gulf area was a potential Iranian zone of influence; Iraq was a frontier and border region and from many points of view the gateway to the heart of Iran; and the Mediterranean coast was a likely security zone against future provocation.[4]

Nevertheless, it was only in the mid 1950s that Iran once again set its sights on the Mediterranean coastal area. This was a direct result of

the stabilization of the shah's rule in Iran and the establishment of the Iranian nation state, two developments that helped consolidate a new Iranian interest on the eastern coasts of the Mediterranean, and in this context, an interest in influence in Lebanon as well. In addition to a longstanding geopolitical interest, the Iranians were troubled by the threat of Arab nationalism and sought to turn Lebanon – and not only Lebanon – into a frontline base in the struggle against the Nasserist advance, which Iran perceived as a real threat. As was explained in the late 1950s by a senior official of the SAVAK (the National Intelligence and Security Organization under the shah), Iran must stop Nasser's threat on the Mediterranean coastal states; otherwise Iran will have to shed its own blood on Iranian soil in order to repulse it.[5] In Lebanon, it was actually powerful Christian elements that shared the Iranian view and not the Shiite community, which was basically backward and lacking in sophistication, and more importantly, not well organized and even too religious for the shah. Nevertheless, as part of the efforts to strengthen their standing in Lebanon, the Iranians invested significant resources in Shiite religious institutions.[6]

Since the late 1950s, Shiite history in Lebanon has been shaped by the religious sage Musa al-Sadr, who was born in Iran to a Lebanese father and returned to Lebanon in 1959. Presumably the shah's regime sought to make use of Sadr for its purposes, and even assisted him from time to time. Thus, for example, Sadr had an Iranian diplomatic passport and maintained a close connection with the Iranian embassy in Beirut, although this did not make Sadr into a lackey working in the service of the shah. In the early 1970s, Musa al-Sadar reached the height of success and established a leading status for himself among members of the Shiite community, and it appeared that he would be able to lead the community to play a more significant role in Lebanon. Yet once the civil war broke out in Lebanon on April 13, 1975, most if not all of his achievements during the preceding years were obliterated. In 1978, Musa al-Sadr visited Libya at the invitation of Libyan leader Muammar Qaddafi and disappeared without a trace. Libyan authorities apparently brought about Sadr's liquidation because of his refusal to cooperate with Qaddafi's attempts to establish a foothold in Lebanon during those years.[7]

Iran and Hizbollah

The collapse of the shah's regime took place against the backdrop of Lebanon's civil war and its deterioration into bloody hostilities. Iran's own turmoil prevented it from playing a significant role in events in Lebanon precisely when there was a window of opportunity to do so. However, following the fall of the shah, an opportunity for Iran in Lebanon presented itself again in the form of Hizbollah. More than any other element, Iran contributed to the organization's founding and consolidation in Lebanon. It was Iran that acted to establish Hizbollah among Lebanese Shiite forces that it assembled under its auspices. It was Iran that acted as middleman and unified these forces, and it also provided them with a common shelter and aid at the start of their journey. It is no wonder that Hizbollah made *wilayat al-faqih* (rule of the cleric) a main ideological principle. This principle, which was cultivated by Ayatollah Khomeni, states that the community of Islam is obligated to subjugate itself to the authority of the most senior cleric in its midst and to obey his will.[8] On this subject, Hizbollah Secretary General Hassan Nasrallah stated:

> From the first moment, we saw ourselves as committed to the principle of the rule of the cleric (*wilayat al-faqih*), and we saw Imam Khomeini, may God have mercy on him, as the leader and the ruler *wali al-imam*; after Khomeni's death, we see Imam Khamenei as such a leader. For twenty-three years we have been committed to this principle of *wilayat al-faqih*, and we also implement it.[9]

Hizbollah burst onto the Lebanese stage with great fanfare in late 1983. A string of painful attacks by Hizbollah against Israeli and Western targets in Lebanon left hundreds of dead and wounded, and eventually brought American and French involvement in Lebanon, and then Israeli involvement, to an end. Hizbollah slowly assumed leadership of the military struggle against Israel in the security zone along the Israeli-Lebanese border, until it became the IDF's main adversary on this front, eclipsing the Palestinian organizations that previously were Israel's bitter adversaries there.[10]

Hizbollah's arrival on the scene in Lebanon as a radical militant organization waging a violent struggle against the West – and Israel in particular – and against the organization's domestic enemies reflected the formative influence of two significant regional events on the organization.

The first event was the 1979 Islamic Revolution in Iran, which for the Shiite community in Lebanon was a source of inspiration and a model for emulation. The second was the Israeli invasion of Lebanon in June 1982, which made Israel an easy target and a ready object of radical Lebanese Shiite fervor, and in particular, Hizbollah. These two events, however, were overshadowed by the Lebanese civil war between 1975 and 1989, when the Shiite community burst onto the Lebanese scene with new weight and became a major player in Lebanon.

After the Islamic revolutionaries established themselves in power in Iran, they began to exhibit increasing interest and involvement among the greater Shiite community, with the goal of harnessing more support for Iranian interests. It was the Islamic regime in Iran that led to the establishment of Hizbollah as a new organizational framework that was to serve, at least in Tehran's view, as a tool for promoting Iranian interests in Lebanon. It was also Iran that was behind the decision by prominent Shiite leaders to abandon the ranks of Amal, which until then was the main framework for the Shiite community in Lebanon, and to join the ranks of Hizbollah, and it encouraged or even compelled other Shiite forces, and sometimes competitors or adversaries, to unite under this new organizational umbrella. Iran subsequently became Hizbollah's main source of economic, military, and political support. Iranian aid to the organization included the dispatch of Iranian volunteers, some 2,500 members of the Revolutionary Guards, who arrived in Lebanon in 1982. Nearly 1,500 of them remained in Lebanon in the following years and helped establish Hizbollah's military power. Since then, the Revolutionary Guards have been the principal channel connecting the Islamic revolutionary regime with Hizbollah.[11]

In the late 1980s, Hizbollah became the leading force in the Shiite community, and it appeared that it was within its power to take over Lebanon, or at least to impose its authority over Shiite areas and establish an Iranian-style Islamic order. In October 1989, the Taif agreement, which concluded the Lebanese civil war, was signed in Saudi Arabia. The civil war had provided a fertile background for Hizbollah activity, but upon its resolution Hizbollah proved itself a pragmatic organization that ostensibly aspires to productive activity and is prepared to abandon its commitment to ideological concepts, or at the very least to postpone their realization to the distant future. When Hizbollah evolved from a militia to

a political movement, the scope of its activity among the Shiite population throughout the country increased substantially. Already in the mid 1980s, with generous Iranian aid estimated at tens if not hundreds of millions of dollars a year, the organization launched a welfare and social services system, which was intended to gain the support of members of the Shiite community and at the same time provide an alternative framework to the services offered – or that were supposed to be offered – by the Lebanese state. This system was significantly expanded as the organization consolidated its hold on the Shiite community over the years.[12]

Today the Hizbollah educational system includes hundreds of educational institutions in the Shiite areas of Lebanon with hundreds of thousands of students. The organization has also established an Islamic health care system that treats nearly half a million patients every year. It runs an organization that builds and rehabilitates houses, mosques, schools, and hospitals, paves roads, and even supplies water to Shiite villages. In addition, Hizbollah runs financial institutions that provide financial aid and loans to the needy. The organization has a fund for the fallen and has provided assistance to thousands of families of Shiite dead, wounded, and imprisoned. It established a judicial and arbitration system in the Shiite areas of Lebanon, and it is represented in workers unions in Lebanon. Hizbollah likewise has an extensive public relations operation: four radio stations and a television station, al-Manar. Under Iranian sponsorship, Hizbollah has also become an economic empire that includes industrial factories, small and medium sized businesses, and real estate. According to various estimates, Hizbollah has nearly 100,000 activists and members, including those employed in its institutions.[13]

Thus since the mid 1980s Hizbollah has built itself up as a viable, powerful organization. On the one hand, it is an organization in possession of a powerful militia focusing on the struggle with Israel, but at the same time, it is an organization that is a political and social movement whose goal is to promote Shiite interests in Lebanon.

The al-Quds Force

Iran-Hizbollah communication, including Iran's aid to the organization, is conducted through the al-Quds Force, an elite unit that is part of the Revolutionary Guards and whose purpose is "exporting the Islamic revolution" beyond Iran. This is a secret branch with a wide range of

clandestine activities beyond Iran's borders, including establishment of an educational system and indoctrination, aid to organizations such as Hizbollah and Hamas, terror and espionage, and much more.

Testimony from Hizbollah members and material captured by Israel during the Second Lebanon War reveal that members of the al-Quds Force have established and operated a training network for Hizbollah members to prepare them to use the advanced weapons supplied to Hizbollah by Iran. Some of this training has been carried out in Iran itself.[14] In a speech on October 20, 2006, not long after the Second Lebanon War and on the occasion of Jerusalem Day, the al-Quds Force commander Qasim Suleimani declared:

> In the wake of Hizbollah's victory in Lebanon, a new Middle East is being formed, not an American [Middle East], but an Islamic one . . . The Shiite Hizbollah has succeeded in exporting and marketing to Palestine its model of a way of life of faith in God. The organization is also helping change the Palestinians' stones into missiles.[15]

At the same time, involvement by the al-Quds Force has not been limited to training. In practice, members of the al-Quds Force, headed by their commander, have become Hizbollah's supervising commanders, and they are involved in the organization's operational activity as advisors, supervisors, and even as the "go to" people, that is, as adjudicators with respect to decisions about the organization's operational activity against Israel and against its adversaries in Lebanon.[16]

Iran and Hizbollah: The Iranian Interests

Iran's interest in Lebanon stems from strategic considerations and possibly identification with and commitment to members of the Shiite community, as well as from the desire to strengthen the image of the Islamic revolutionary regime in Tehran as a promoter of Islam. Yet the sole destination where Iran has been able to export the idea of an Islamic revolution and play an active role, adopting a local client that expressed interest in the merchandise Iran had to offer, is Lebanon. Thus, not only was the idea of an Islamic revolution in Lebanon not contrary or threatening to Iranian interests; it actually advanced these interests, especially regarding the regime's image.

And indeed, the Levant's coasts were far from Iran, and it appeared that the Iranians felt and still feel even today that they can afford to

promote a foreign policy that provides an outlet for Islamic sentiments and thereby mitigate domestic pressures from conservative circles calling for the adoption of a more Islamic policy, without paying an immediate price for it. This is a reason for Iran's involvement in the Israeli-Palestinian conflict, and this increasing involvement has turned Iran in Israel's eyes into an enemy, and vice versa.

Iran's decision to establish Hizbollah as an Iranian frontline against Israel first of all transformed the organization into a well oiled, high powered military machine by supplying thousands of advanced missiles to Hizbollah, which today reach most of the territory of Israel and can hit their targets with a high degree of accuracy. The logic behind Tehran's decision to supply Hizbollah with close to 50,000 such advanced missiles, thereby turning it into a powerful force even in relation to the region's conventional armies, was of course Iran's desire to make use of the organization in order to deter Israel. Indeed, other than Hizbollah Iran has no real answer against Israel, and without Hizbollah, its ability to deter Israel from operating against Iran and against its nuclear facilities – or alternatively, Tehran's ability to respond and exact a price from Israel in the event of an Israeli or American attack against Iran – is highly limited. This is why Hizbollah is so important to Tehran. Syria has played an important part in allowing Iranian missiles to be moved through its territory to Hizbollah, and has also supplied thousands of its own missiles, especially, advanced missiles such as the rockets that Hizbollah fired at Haifa during the Second Lebanon War and Scud missiles, which are the crowning glory of the Syrian missile arsenal.[17]

In this context, it is clear why Iran did not hide its dissatisfaction with the outbreak of the Second Lebanon War, when the missile arsenal it had supplied to Hizbollah was exposed unnecessarily and then used for a different purpose than for what it was intended. After the war, Iran tightened its grip on Hizbollah, a trend that was strengthened with the liquidation of Imad Mugniyeh, the commander of Hizbollah's military wing, in the heart of Damascus in 2008.[18]

Interestingly, Iran has an important ally in Damascus in the form of the Syrian Alawite regime. It was by no means self-evident that there would be any congeniality between Iran and Syria, considering that the Syrian Ba'ath regime is secular and Arab nationalist, not to mention that it is an infidel regime, as there are serious doubts in the Islamic world concerning

the Alawite commitment to Islam, and more precisely, the commitment of its leaders. (The first person to issue a religious ruling allowing the Alawite community to be considered Shiite was Musa al-Sadr.) Still, this is an alliance of interests, and these dictate the moves of both states. The basis of these interests is fear, or in any case, the need for mutual assistance in light of the threats from the United States and from Israel, which appear to be acute and urgent in the eyes of Tehran and Damascus. However, it is actually Lebanon that may change from being a basis for cooperation between Syria and Iran and become a focus of dispute. This will occur if Syria concludes that Hizbollah's strengthening in Lebanon through Iranian backing endangers essential Syrian interests.[19]

Joining the political upheavals in Beirut in early 2011, that is, Hizbollah's overthrow of the Saad al-Hariri government and the establishment of a new government controlled by Hizbollah and Syria, are the shockwaves reverberating throughout the entire Middle East following the fall of the Husni Mubarak regime in Egypt in early February 2011. These events have created a new situation in which Lebanon is slowly distancing itself from the circle of American influence (to which Saad al-Hariri and his associates were inclined), and is linking itself with the opposing camp. This camp is united with respect to the struggle against Israel and the United States, but it has a different view concerning the future of Lebanon. Bashar al-Asad spoke to this issue that when he explained why it is appropriate for Syria and not Iran to become a stakeholder in Lebanon, and perhaps even the boss.

The Future of Iranian Influence in Lebanon

The Iranian presence in Lebanon appears more stable than ever, as does Tehran's hold on Hizbollah, which now depends on Iran's financial and military aid more than at any time in the past. At the same time, Hizbollah is growing stronger within the political system in Lebanon, a result of its efforts to become a legitimate and almost exclusive representative of the country's Shiite community. Not surprisingly, there are those inside and outside of Lebanon who warn of a future Hizbollah takeover of the country, through physical or demographic strength of the Shiite community, which over the years has become the largest community in Lebanon.

However, Hizbollah does not in fact represent and is not automatically supported by most of the Shiites in Lebanon, and even those who do support it are not keen to adopt its ideological concepts, especially its religious and ideological links with Iran. Just as in Iraq, in Lebanon too there are many who believe that the Shiism of the Khomeini school does not represent their authentic faith or the religion they grew up with. Amal, the competing Shiite organization, is still active in Lebanon, and it has not insignificant support, even though the weakness of its leaders, headed by Nabih Berri, leaves the Shiite field open to Hizbollah activity and control. Furthermore, it is actually the Iranian Shiite challenge felt today throughout the Middle East, and not just in Lebanon, that is stirring reactionary sentiments. Members of the Sunni community in Lebanon and other Arab states are determined to try to stop Iran. Turkey has joined them from a Sunni starting point, not an Arab one.

Iran has become a key player in Lebanon; of this there is no doubt. But the battle for Lebanon is far from over, and there are other forces in the race for control of Lebanon besides Iran. One of these forces is of course Syria, today a close ally of Iran, but perhaps in the future Iran's rival in the battle for Lebanon.

The foothold and the dominance Iran has achieved in Lebanon over the years undoubtedly stemmed from a convergence of factors, among them the collapse of the Lebanese system; the rise of the Shiites in Lebanon, at least numerically, and their failure to assume a leading role in society, the economy, and government; the Israeli challenge, which pushed Hizbollah into the arms of Iran and made it dependent on Iran; elements that brought a group of Iran-associated Shiite clerics and activists to the leadership of Hizbollah; and the weakness of Syria.

Iran's presence in Lebanon was built on the disorder, chaos, and anarchy prevailing in Lebanon over the years, and the ongoing tension and outbreaks of violence within Lebanon and with its immediate neighbors – Israel, Syria, and the Palestinian Authority. Hence, resolution of the internal Lebanese tension and diminished regional tension through promotion of a political settlement are enough to harm and erode Iran's status in Lebanon. Iran has little of value to offer Lebanon, especially to members of the country's Shiite community, other than an open ended supply of missiles.

Even without these factors, Iranian involvement in Lebanon is likely to encounter not insignificant difficulties. Syria has slowly returned to assume a key role in Lebanon, despite the domestic challenges the Syrian regime is facing following the storm of regional change that has reached Damascus, and this will undoubtedly occur at the expense of Iran and with ongoing friction between the two countries. Other Arab states as well, such as Saudi Arabia, are active in the Lebanese arena, and even Turkey has once again joined the fray. In the short term, this regional and inter-Arab energy will be concentrated against Israel, in a false display of demonstrations of solidarity against the challenge Israel presents to Lebanon. But in the long term, Iran will encounter increasing difficulty in imposing its will and the will of its Lebanese protégé, Hizbollah, on Lebanon.

The various sides in Lebanon are likely to reach the moment of truth following the outbreak of an Israeli-Iranian or an American-Iranian confrontation due to the Iranian nuclear project. In the event of such a confrontation, the question is whether Hizbollah will join the battle or even serve as the long arm of the Iranians, whereby, and especially with the missile arsenal in Hizbollah's possession, Iran will seek to respond to a possible Israeli or American attack on its nuclear facilities. Hizbollah's decision to respond to the Iranian diktat and open a front in the north of Israel is no trivial matter, since this would likely doom or at least seriously damage its standing in Lebanon even among members of the Shiite community if it becomes clear that Hizbollah has brought destruction to Lebanon, such as what it suffered in the Second Lebanon War, all in the service of Iranian interests. On the other hand, Iran has not supplied tens of thousands of missiles to Hizbollah, well beyond what the local arena requires, for naught. These missiles were supplied with the assumption that they would be used when Iran needed.

Therefore, an Israeli-Iranian confrontation will create difficult dilemmas, and perhaps even disputes on the Beirut-Tehran axis. In the past, Hizbollah leaders in Beirut and their superiors in Tehran knew how to walk the fine line between Iranian needs and the organization's local Lebanese interests. After all, Iran is conducting a rational foreign policy that recognizes the limitations of its power, and it will not want to endanger its investment in Lebanon. On the other hand, at the moment of truth, it appears that it is Iran that will be the player of influence through

the mechanisms of control – direct and indirect – that it has imposed over Hizbollah, and it will have the last word.

Thus, Iran's entrance onto center stage in Lebanon via Hizbollah is a fascinating chapter in history, but is not necessarily the end of the Lebanese story, which is still far from over.

Notes

1 Al-Jazeera, July 15 and 16, 2010; *Yediot Ahronot*, July 21, 2010; *Haaretz*, July 21 and 28, 2010.
2 *Al-Hayat*, October 26, 2010.
3 See al-Jazeera, October 26 and November 21, 2010. See also *al-Mustaqbal*, October 25 and 26, 2010.
4 For more on Iran's relations with Lebanon, see H. E. Chehabi, ed., *Distant Relations: Iran and Lebanon in the Last 500 Years* (London: I. B. Tauris, 2006).
5 See Shimon Shapiro, *Hizbullah: Between Iran and Lebanon* (Tel Aviv: Kibbutz Meuhad, 2000), p. 26.
6 Concerning the connections of Iran under the shah with Lebanon, see Abbas William Samii, "The Shah's Lebanon Policy," *Middle East Studies* 33, no. 1 (1997); Abbas William Samii, "The Security Relationship between Lebanon and Pre-Revolutionary Iran," in *Distant Relations*, pp. 162-79. See also Shapiro, *Hizbullah: Between Iran and Lebanon*, pp. 28-54.
7 On Musa al-Sadr see Fouad Ajami, *The Vanished Imam: Musa al Sadr and the Shia of Lebanon* (Ithaca, NY: Cornell University, 1986).
8 Ahmad Nizar Hamzeh, *In the Path of Hizballah* (Syracuse: Syracuse University Press, 2004), pp. 27-43.
9 See Nasrallah's interview with the Kuwaiti newspaper *al-Ray al-A'am*, August 27, 2005.
10 On Hizbollah's early days, see Hala Jaber, *Hizbullah: Born with a Vengeance* (New York: Columbia University Press, 1997).
11 For more on Iranian aid to Hizbollah in the organization's early days, see Shapira, *Hizbullah: Between Iran and Lebanon*.
12 See Judith Palmer Harik, *Hezbollah: The Changing Face of Terrorism* (London: I. B. Tauris, 2004); and Eyal Zisser, "The Return of the Hizballah," *Middle East Quarterly* 9, no. 4 (2002): 3-12. See also Amal Saad-Ghorayeb, *Hizbullah: Politics and Religion* (London: Pluto Press, 2002); Wadah Sharara, *Dawlat al-Hizbullah, Lubnan-Mujtama'a Islami* (*The Hizbullah State, Lebanon: Lebanese Society*) (Beirut, 1996); and Eitan Azani, *Hizbullah: From Revolutionaries and Pan-Islamists to Pragmatists and Lebanese*, doctoral dissertation, Hebrew University, 2005.
13 See Eyal Zisser, *The Bleeding Cedars: Lebanon – From Civil War to the Second Lebanon War* (Tel Aviv: HaKibbutz Meuhad, 2009), pp. 241-73.
14 Meir Amit Intelligence and Terrorism Information Center, http://www.terrorism-info.org.il.

15 See al-Manar television station, October 20, 2006.
16 *Haaretz*, February 23, 2008.
17 See *Haaretz*, December 17 and 24, 2010.
18 See Meir Elran and Shlomo Brom, eds., *The Second Lebanon War: Strategic Perspectives* (Tel Aviv: Institute for National Security Studies, 2007). See also *a-sharq al-Awsat*, September 9, 2008.
19 See Ahmad S. Khalidi, *Syria and Iran* (London: The Royal Institute of International Affairs, 1995); Anoushiravan Esteshami and Raymond A. Hinnebusch, *Syria and Iran: Middle Powers in a Penetrated Regional System* (New York: Routledge, 1997); and Jubin M. Goodazri, *Syria and Iran: Diplomatic Alliance and Power Politics in the Middle East* (London: I. B. Tauris, 2006).

The Unique Features of the Second Intifada

Zaki Shalom and Yoaz Hendel

Introduction

Over a decade has passed since the eruption of the second intifada, a grueling period for Israel with the long, sustained, and intensive series of terrorist attacks launched by terrorist organizations against civilians and soldiers of the State of Israel. Most difficult were the suicide attacks, generally carried out in urban centers and causing large numbers of casualties − dead and wounded − among the civilian population. Predictably, therefore, the terrorism phenomenon became a dominant issue on Israel's national and popular agenda. It reshaped the walk of Israeli civilian life, affected politics, and to a significant extent damaged the country's economy. In addition, for many years the intifada was accompanied by the Israeli public's sense that the defense establishment had no response that would put an end to terrorism, or at least drastically reduce it. Those times have not receded from the nation's collective memory and still affect how Israeli society formulates its positions on current political and security issues.

Since its establishment, the State of Israel has known difficult periods of war, bereavement, and casualty. The severity of each conflict may be evaluated through various criteria such as the balance of forces between the sides, the perception of the dangers to Israel, risk assessments, the numbers of dead and wounded, the ratio of civilian to solider casualties,

Professor Zaki Shalom is a senior research associate at INSS, a researcher at the Ben-Gurion Research Institute for the Study of Israel and Zionism, and a lecturer at Ben-Gurion University. Dr. Yoaz Hendel is a researcher at the Begin-Sadat Center at Bar Ilan University. The article is based on their comprehensive study *Let the IDF Win: The Self-Fulfilling Slogan* (Tel Aviv: Yediot Ahronot, 2010).

motivation during the campaign, the level of political support for or against the campaign, civil-military relations during the fighting (agreements versus disagreements), and others. It is difficult to draft an agreed-upon scale of criteria to rank the severity of the campaigns Israel has fought, and sets of criteria for assessing the severity of a war are largely subjective.

That said, when examining the public discourse about the military's confrontation with suicide terrorism in the first years of the second intifada, one encounters a unique phenomenon − the question of capability. Against the background of explosions and the stream of suicide bombings, the dominant argument within Israel touched on whether the IDF was capable of defeating suicide terrorism, and more generally, whether a regular army was at all capable of defeating a guerilla or terrorist organization. This question is an underlying element in the essay that follows, which argues that the intifada was one of the most severe military campaigns Israel fought since attaining its independence.

The Strategic Dimension of the Terrorism Threat

Over many years, in essence since the War of Independence, a fixed feature of Israel's security doctrine was the distinction between two categories of threat against Israel: threats at the strategic level versus threats at the tactical level. Threats at the strategic level were attributed to neighboring Arab countries, especially Egypt. The starting assumption was that the armed forces of neighboring Arab states could threaten the very existence of the State of Israel by territorial conquest and eradication of Jewish settlement. Threats at the tactical level referred primarily to the activities of the various terrorist organizations. According to this school of thought, the activities of terrorist organizations represented a bothersome nuisance but lacked the features that would define them as strategic threats.

This distinction was blurred in recent years, especially during the second intifada, which assumed the nature of a strategic threat in the public consciousness. Intensive activity by terrorist organizations, particularly suicide terrorism, changed the essence of the country's civilian routine. It had a severely negative impact on economic development in Israel, and on the scope of immigration and tourism. In addition, terrorism also affected the structure of the political system in Israel. Indeed, in virtually

every election campaign in the last two decades, terrorism and how to cope with it politically and militarily became hot issues in the contest for the public's vote. Most prominent in this regard were the May 1996 Knesset elections, held six months after the assassination of Prime Minister Yitzhak Rabin. Although polls predicted a devastating defeat of the right wing parties, Likud leader Binyamin Netanyahu was elected prime minister (albeit by a small margin). The Israeli media, with much justification, attributed his surprising election to devastating terrorist attacks, two of them in the heart of Tel Aviv, in the months leading up to the elections.[1] During the second intifada, however, the impact of terrorism was sharper, more sustained, and more acute.

The second intifada began while the Labor Party, headed by Ehud Barak, held the reins of government, the peace process seemed promising, and there was public support for compromise. It was succeeded by a government led by the right, which in turn spawned a new leadership based on a new centrist party supportive of peace, but using means of combat at a time when public support for the Oslo approach to compromise had declined. At the same time, the intifada sparked changes within the right wing camp regarding Israel's interests, which led to territorial withdrawals and as such, changes in borders and lines of control. These changes among the right were of major significance.

Likewise on the strategic level, the intifada served as a platform for the genesis of a new type of struggle − the delegitimization of the State of Israel and an influential anti-Israel campaign. This campaign brought together Palestinian organizations, leftist groups, and far right movements from across Europe as well as anti-Semitic circles, all taking advantage of the new momentum to advance their interests. Thus it is clear that terrorist activity during the second intifada had a strategic impact on Israel in a wide range of areas at least as much as have the wars waged by regular armies.

Defining the Enemy

Of Israel's campaigns, the second intifada was singular in that during most of its stages there was no clear, agreed-upon definition of the enemy Israel was fighting and who was responsible for the terrorist attacks against the state.

At the leadership level, the dilemma started with Arafat. Suspected by some decision makers as the dispatcher of a significant number of the suicide terrorists into the heart of Israel's urban centers, the leader of the Palestinian Authority had previously been portrayed as an ally of Israel. The Oslo Accords were seen by a part of the Israeli public as proof of his willingness to end the long conflict between two national movements − the Zionist movement and the Palestinian movement. Despite information gathered about his involvement in terrorism, there were people who believed that the man who spoke from every dais and into every microphone about his desire to implement "the peace of the brave" together with Israel and its leadership, the man who had no qualms about denouncing terrorist acts against Israel and the killing of innocents, had sincere intentions.[2] However, the growing intelligence file and the many attacks raised the question whether he was engaged in duping the whole world. As a result, Israel's leadership found itself between a rock and a hard place, between the desire to preserve its new-found friend on the one hand and the data that indicated that the friend was actually an enemy, on the other.

Within Israel, Arafat's intentions were examined time and time again. Was he worried about jeopardizing his achievements by closing his eyes to terrorism or being involved in terrorism? Was he prepared to jeopardize admiring public opinion, evident throughout the world and within large segments of Israeli society? Perhaps, said some, he too, like the moderate Israeli government, was caught in a difficult struggle against extremist groups trying to keep him from advancing towards true peace with Israel. Would Israel want to act against him in response to the attacks? Would Israel want to weaken him? And what would happen if, as a result, the extremists in the Palestinian camp were to gain the upper hand?

Israel had never faced such pointed questions about a leader for so long a period of uncertainty. Even when clear cut evidence of Arafat's personal involvement in terrorist activities accumulated, many felt that this was simply an element Israel had to accept. In any case, many Israelis opposed the idea of attacking the PA chairman in response to the terrorist attacks on Israel, its civilians, and soldiers, because of doubts regarding his personal involvement in terrorism and because Arafat was, in any case, the lesser of the evils.

The dilemma of identifying the enemy grew more acute when it came to activists on the ground. As the intifada continued, the IDF found it hard to decide on tactical moves such as instructing soldiers when to open fire. How was the IDF to relate to the PA police force, with which Israel supposedly had agreements and understandings? Was it allowed to act against a policeman in uniform by day if he was also carrying out terrorist activity by night? Should PA police be permitted to carry weapons? Where does one act against terrorists? Were PA regions to be considered cities of refuge with immunity or enemy territory where one must operate?

In practice, only the January 3, 2002 interception of the gun-running ship *Karine A* carrying major quantities of materiel from Iran to the PA put to rest any lingering doubts that the PA and Yasir Arafat were active participants in terrorist activity directed against Israel. This assessment gained a greater foothold in Israel once Arafat's credibility with the American administration evaporated as a result of the interception of the ship. Until then, the first task facing Israel's leadership was to identify, to itself and the Israeli people, the enemy before it.[3]

Can Terrorist Organizations be Defeated?

One of the critical questions of the intifada was if it was possible to defeat terrorist organizations attacking Israel, just as it was possible to defeat regular armies of sovereign nations. Many claimed it was not, and reasoned as follows: The circles Israel was calling "terrorist organizations" were just various factions of the Palestinian national movement. All Palestinians wanted to realize their right to self-determination. Among them, naturally enough, were disagreements about how to achieve that goal. Some supported waging the struggle through diplomacy and political action, while others favored violent means. A national movement striving to realize independence in the face of a conquering state would not rest until the fulfillment of its ambition.

In an attempt to persuade others of the justness of their position, many of this school claimed that history "proved" that in the end, conquering states were forced to concede control of conquered territories and allow the local population to achieve their independence. Examples from the first Indochina war through Algeria and Vietnam to the Soviet war in Afghanistan proved − according to those who denied the possibility of

a military victory – that it was impossible to defeat a terrorist or guerilla organization militarily. Therefore, and because the final result of the struggle against Palestinian organizations is known ahead of time, the cost in victims that both sides were being forced to pay for the struggle had no justification. The only way to stop Palestinian violence was by means of a political settlement. No military action would be able to end the violence against Israel.

Many public figures, media personalities, academics, and various experts expressed these opinions through modes of discourse typical of democratic states. A similar process, though with different levels of intensity, had taken place in Israel in its previous struggles. However, what distinguished the intifada was that this time doubts crept into the very heart of the security-military establishment. The State of Israel had known public disagreements in previous wars, but the defense establishment had always been able to argue convincingly that victory would be achieved. This is what David Ben-Gurion declared in the War of Independence: Israel will pay a steep price, but in the end it will win. Similar statements were made by Chief of Staff Yitzhak Rabin on the eve of the Six Day War. Six years later, during the Yom Kippur War, the determined voice of Chief of Staff David Elazar thundered that Israel knew how to overcome the circumstances and win the war that was forced on it.

During the intifada the situation was very different. Senior officials within the security establishment and the IDF, including commanders commended for their bravery and excellence whose integrity and professional abilities were deemed impeccable, called on the country not to indulge in fantasies of victory. It was imperative, they said, to aim for a political settlement, as only that could put an end to Palestinian violence. The most prominent among these figures was Major General Amram Mitzna, GOC Central Command at the outbreak of the first intifada. On many occasions, he gave prominent expression to his clear cut stance that it was impossible to arrive at a military decision in a confrontation with "terrorist organizations" and that only a political settlement would result in calm being restored to Israel:

> The Palestinian conflict, which today is actually the heart of the military-terrorist confrontation we are facing, has over recent years been demanding all our energies. Not only our financial resources, but actually all our energies...It seems to me that today most residents of the State of Israel under-

> stand, maybe better than they did two years ago...that there is no military solution to our conflict with the Palestinians. It's important that we understand this. Slogans such as "let the IDF win," which are primarily political, though they purport of course to have some kind of professional, to-the-point significance, are empty. There is no military solution. Similarly, terrorism will not succeed in bending the State of Israel or in forcing on it and its citizens certain settlements, agreements, or solutions detrimental to Israel's security and its critical interest. The army and military force have a great deal of meaning and a great deal of importance also in this struggle against Palestinian terrorism, as well as in many other issues connected to the security of the State of Israel. However, it is also important that we understand that there is no military solution. There is no solution of pure aggression.[4]

Mitzna was not the first to speak in this way. During the terrorist attacks of the 1990s Prime Minister Yitzhak Rabin said that "there is no real deterrence against terrorism," and according to Amnon Strashnov, the Chief Military Prosecutor during the first intifada, "Shomron quickly understood that a military solution to the intifada was nowhere to be found."[5] And subsequently, throughout the intifada, Israel was faced with an unprecedented phenomenon: the fact that even prominent members of the military establishment had doubts with regard to Israel's ability to defeat the challenge confronting it, i.e., terror. This had not occurred in Israel's prior confrontations.

Doubting the Justness of the Cause

In addition to these challenges, Israeli society was beset by doubts about the justness of the cause. Many asked: were we, the descendants of a nation that had fought for its freedom and independence for thousands of years, conducting a moral war against the Palestinians? Was it fair of us to deny them the right of self-determination? Many Palestinians had been living as refugees for decades after having been expelled from their homes during the War of Independence. Could Israel, the descendant of a nation that had lived in the Diaspora as often-persecuted refugees, afford to ignore the Palestinians' plight? These questions created deep fissures in Israeli society about the justness of the struggle against terrorist organizations during the intifada.

Similar types of public protest were not unknown to Israel during other military confrontations. The first significant instance of public protest about the justness of war occurred during the War of Attrition in 1968-70. The static presence on the Suez Canal and daily exposure of IDF soldiers to heavy fire and ambushes from the Egyptian side combined with the sense that the Israeli government, headed by Golda Meir, was not demonstrating enough flexibility in the attempt to arrive at an Israeli-Egyptian settlement generated a wave of protests that continued until the August 1970 Suez Canal ceasefire agreement. Among the prominent expressions of this protest wave were "Shir Lashalom" ("A Song for Peace") performed by the IDF Nahal Entertainment Troupe and the play *The Queen of the Bathtub*. The central motif in both was the real possibility of attaining peace with the neighboring Arab states, especially Egypt, even while the Meir-led government undermined this possibility because it wanted to continue controlling the territories captured in the Six Day War.[6]

Similarly, during the First Lebanon War and during the extended fighting in southern Lebanon that followed, public protest swelled the longer the combat continued. The protest was expressed mainly with songs directed especially at Ariel Sharon and, starting in 1997, with the establishment of the Four Mothers movement. This protest movement had a decisive impact on the growing popular support for withdrawing from southern Lebanon even without an agreement with the Lebanese government. Ehud Barak, then head of the Labor Party, was the first to understand the electoral appeal of this movement and its demand for withdrawal and leveraged it in his May 1999 election campaign. Indeed, his commitment to withdraw from Lebanon was one of the decisive elements in his victory over Binyamin Netanyahu. A year later, in May 2000, he made good on his promise to withdraw the IDF from Lebanon within one year of his election.

By contrast, the protest that swelled in Israel during the second intifada was of a different kind, far more intensive and extended than previous protest movements. The claims that it was impossible to attain a victory and that therefore harsh military moves against the Palestinians were useless became major issues in the debate on the legitimacy of the fighting.

For example, Palestinian terrorist organizations to a large extent conducted their war from within the Palestinian population. This required the security services in Israel to conduct their campaign with the awareness that Palestinians who were not necessarily directly involved in violence against Israel might easily be harmed. Targeted assassinations, which on more than one occasion cost the lives of innocent civilians, provided a major example of this phenomenon, and they often generated widespread public criticism within Israel, in addition to international condemnation. The so-called "dissenting pilots' letter" was especially prominent in this context: twenty-seven Israel Air Force fighter pilots, headed by renowned IAF pilot Brig. Gen. Yiftah Spector, signed a letter in which they stated their refusal to continue harming innocent civilians. The letter was published on September 24, 2003.

In the letter, the pilots protested IAF activity against wanted terrorists that involved the killing of innocents:

> We, Air Force pilots who were raised on the values of Zionism, sacrifice, and contributing to the State of Israel, have always served on the front lines, and were always willing to carry out any mission to defend and strengthen the State of Israel.
>
> We, veteran and active pilots alike, who have served and still serve the State of Israel for long weeks every year, are opposed to carrying out attack orders that are illegal and immoral of the type the State of Israel has been conducting in the territories.
>
> We, who were raised to love the State of Israel and contribute to the Zionist enterprise, refuse to take part in Air Force attacks on civilian population centers. We, for whom the Israel Defense Forces and the Air Force are an inalienable part of ourselves, refuse to continue to harm innocent civilians.
>
> These actions are illegal and immoral, and are a direct result of the ongoing occupation which is corrupting the Israeli society. Perpetuation of the occupation is fatally harming the security of the State of Israel and its moral strength.
>
> We who serve as active pilots − fighters, leaders, and instructors of the next generation of pilots − hereby declare that we shall continue to serve in the Israel Defense Forces and the Air Force on every mission in defense of the State of Israel.[7]

The letter did not express outright opposition to targeted killings; rather, it rejected the outcome whereby innocent bystanders would be harmed in the course of such actions. However, it is in fact impossible to ensure that any targeted assassination will not harm bystanders. Sincere attempts can – and are – made by the IDF to avoid harming civilians, but there is no guarantee that this will not happen in practice. If the demand to avoid killing civilians is absolute, it would necessarily abolish the practice of targeted assassinations, viewed by the IDF as very effective in the war against terrorist organizations.[8]

IAF pilot Yigal Shohat was more explicit in his criticism of the IAF in the war against terrorist organizations:

> Pilots have to decide, every day anew, and sometimes from hour to hour, what they are morally and legally allowed to do...In my opinion, pilots have to look very closely at the commands they're given, ask a lot of questions about the target, and refuse to obey commands that are legally problematic in their opinion...I think that F-16 pilots should refuse to bomb Palestinian towns. They have to think about what such a bombing would look like where they themselves live...I'm talking about eliminating entire main streets... When a jet bombs an inhabited city you take into account the killing of civilians even if you're talking about precision armaments. In my opinion, this is intentional killing of civilians. That's a war crime.[9]

Alongside these pilots and organizations such as "Breaking the Silence," civilian movements were also established that viewed the IDF's campaign against Palestinian terrorism as crossing permissible lines. Their claims changed as the campaign developed. If at the outset they explained that there was no point in fighting because in any case there would be no victory, from the moment the terrorism abated thanks to IDF activity the claims became based on morality. While in their view the goal was rational, the manner was not justifiable.

Conclusion

Typical of warfare against a guerilla or terrorist organization, the second intifada started with uncertainty and with no clear front or rear. Unlike smaller wars throughout the world, during the intifada Israel was at the mercy of a host of suicide terrorists and the problem of defining and identifying the enemy. These difficult starting conditions were

compounded by widespread skepticism regarding the ability to score a victory against terror and guerilla organizations, and ultimately by questions undermining the legitimacy of Israel's fight against the terrorist organizations, i.e., the loss of belief in the justness of the cause. This convergence of elements made the second intifada one of the most complex campaigns Israel has had to undertake, both militarily and civilly. Nonetheless, Palestinian terrorism in general, and suicide terrorism in particular, was defeated militarily and the IDF earned its victory. This is a significant achievement not only for Israel, but also for many other democratic states that have to cope with terrorism over a long period of time.

Notes

1 Mazal Muallem, "The Voices of War," *Haaretz*, January 4, 2009.

2 The term "peace of the brave" was coined by Yasir Arafat. It is usually associated with Yitzhak Rabin with whom, according to Arafat, he signed, "the peace of the brave." See Zvi Barel, "Neighbors," *Haaretz*, November 3, 2005.

3 Zaki Shalom, "Defining the Enemy in an Asymmetrical Confrontation: The Case of the Second Lebanon War," *Strategic Assessment*. 12, no. 3 (2009): 7-18, http://www.inss.org.il/upload/(FILE)1259664194.pdf.

4 Address at the Third Herzliya Conference, December 4, 2002, http://www.herzliyaconference.org/_Articles/Article.asp?CategoryID=87&ArticleID=2247.

5 Amnon Strashnov, "Between Two Chiefs of Staff, Dan Shomron and Moshe Levy, Israelis of a Different Species," *Haaretz*, February 28, 2008.

6 The lyrics of "A Song of Peace" were written by Yaakov Rotblit and set to music by Yair Rosenblum. It was first sung in 1969 during the War of Attrition by the IDF Nahal Entertainment Troupe in its routine called "A Nahal Settlement in the Sinai." The satire *Queen of the Bathtub* ran in early 1970. It was meant to serve as a platform for satirizing the euphoria and nationalistic fervor that characterized Israeli society after the Six Day War. Source: Wikipedia.

7 "Courage to Refuse," http://www.seruv.org.il/english/article.asp?msgid=55&type=news.

8 Neri Livneh, "If the IDF Does Not Change, the Deterioration Will Continue," *Haaretz*, December 8, 2007.

9 Yigal Shohat, "Israel En Route to The Hague: War Crimes and Israel's Security," *Gush Shalom Conference*, Tzavta Hall, Tel Aviv, January 9, 2002, at http://gush-shalom.org/archives/forum.html.

Israeli Naval Power: An Essential Factor in the Operational Battlefield

Zeev Almog

Although the State of Israel has always been threatened from the sea, preparing for the threat was not an important priority for the state's leaders, as reflected by the resources that were allocated to the navy. However, once long range missiles appeared in the naval arena (in the 1960s), it became clear that the navy's vessels and the air force's planes were not capable of coping with this challenge.

Another change occurred following the Yom Kippur War and in no small measure as a product of the war, when the threat to Israel from the sea developed and assumed unprecedented proportions. As a result of their defeat in the naval theater in the Yom Kippur War, Arab fleets (with Western support) significantly increased their strength, mainly by acquiring high quality missile boats, submarines, and naval helicopters, and by fortifying their coasts and turning them into independent command centers. At the same time, technologies and naval arms were upgraded. The result was a changed naval theater, and an increased threat to Israel from the sea. Salvos of long range missiles (300 miles and more) with warheads with great explosive strength and pinpoint precision strike capability could henceforth be launched from surface vessels and submarines deep into Israeli territory.

Ninety-eight percent of Israel's cargo passes through the state's maritime space, which adds a level of vulnerability from this theater. In addition, in the 1970s maritime terror attacks began to increase. They occurred at sea[1] and/or on Israel's coasts (some of these attacks to the country's soft underbelly were among the worst that the State of Israel has experienced to this day), particularly because most of the state's

Rear Admiral (ret.) Zeev Almog , former Commander in Chief of the Israeli Navy

population and a major portion of its infrastructure are spread along the coasts. Following the coastal road massacre (March 11, 1978), the Israel Defense Forces operated in Lebanon and continued to do so for the next eighteen years.

The peace treaty signed with Egypt in 1979 removed Egypt from the cycle of war and violence against Israel (for the first time in its history, Israel was able to navigate from the Mediterranean to the Red Sea through the Suez Canal). At the same time, Israel's territorial depth was reduced, and given the political upheavals common in the Middle East, there was no guarantee that the signed crossing agreements would exist in every future situation. Indeed, in light of the current upheaval in the Arab world, these fears are far from illusory. Even countries belonging to the "third circle" such as Tunisia, Algeria, Libya, Iran, and Yemen could attack Israeli shipping, since they have the capability to reach the maritime area off of Israel's coasts[2] without great difficulty and to fire weapons from afar. Under the cover of large distances from Israel, they can support maritime terrorist cells operating against Israel and send weapons shipments, as some, including Syria, Lebanon, Libya, Tunisia, Algeria, and Iran, have indeed done. It was not possible, and this is still true today, to act effectively against this entire range of threats through the IDF's ground and air forces, and therefore, the navy, which underwent a major buildup beginning in the late 1970s, was required to provide a suitable professional and operational answer to these significant new threats.

The Strategic Nature of the Naval Arena

The maritime space is Israel's only strategic depth under or over the surface (other than depth in space). The military moves and the technological innovations in the 1991 Gulf War, as well as the political and strategic changes that came in its wake and that are now taking place, have emphasized anew the maritime arena's decisive influential capability, different from that known in the past, both in terms of coping with the threat from the sea and the potential contribution to the naval and land operational battlefields. This has made it necessary to update the priorities and the scope of the defense allocations for the navy in the IDF's multi-year plan.

In early 1979, in the wake of the lessons of the Yom Kippur War and the changes underway in the geopolitical arena, and in light of an analysis of technological developments and the balance of power in the naval theater, the Israeli Navy began to formulate an appropriate response to the new threats in the naval realm that were capable of striking both Israel proper and its essential shipping lanes, a response that would pave the way for the navy to enter the gates of the future battlefield. Following the analysis, a plan to provide the desired operational response was drafted, composed of Sa'ar 5 missile boats and Dolphin submarines, which both match and complement each other.

In September 1979, in the wake of the signing of the peace agreement with Egypt, the General Staff recognized the IDF's naval requirements and decided to build twenty-four missile boats and six submarines. Thus in the same year, there was a paradigm shift in the navy's concept of warfare, and subsequently in that of the chief of staff and the minister of defense.[3] However, the new procurement plans that were approved were not implemented on the proper scale and at the proper pace, and with respect to the building and operation of the force in the framework of the independent naval battle and/or a system-wide battle, the concept was only partly translated into practice. The hesitations and foot dragging among the decision makers in Israel's defense leadership, which stemmed mainly from bureaucratic procedures and from resistance by former naval officers who did not understand the substance of the change, coincided with a rise in prices of the vessels and the systems, and as a result, the order of battle that the leadership itself had approved was reduced in scope.

The new naval order of battle (the modern surface ships and submarines) that was planned and began buildup in 1979 was suited to several aspects, including:

a. To be located outside of the port, which is necessarily a vulnerable location.
b. To allow rapid movement and a stay of a number of weeks in the tactical, operational, and strategic maritime space.
c. To work flexibly and at short to immediate time constants, and to strike targets in all circles of the space that directly threatens Israel.
d. To procure stealth technologies, such as a geometric structure and special building materials for the body of the ship, which provide the

ship with low images in all parameters (radar, acoustic, and thermal), and with protection and warning methods that are among the most advanced, which increase the ships' survivability and their ability to locate and strike targets.

e. To take advantage of the multiplicity of neutral targets in their operational arena that are difficult to identify (especially from the air) and exploit the conditions for concealment, darkness/fog, time spent underwater, and bad weather.

f. To create an arms infrastructure that makes it possible to carry a significant quantity and large variety of weapons and ammunition that are capable of attacking all types of targets at sea, in the air, and deep inland with massive precise force, and capable of being used as firepower that aids in the effort to maneuver and destroy at sea and on land.

g. To destroy enemy submarines, which can launch missiles at Israel proper from the depths of the sea and from a great distance, and which are capable of mining the entrances to the only two ports located in Israel's existential supply route (on the Mediterranean) and neutralizing them for a significant period of time.

h. To assist Israel's ground forces by destroying the enemy's expeditionary forces on their way to aid and reinforce the theater of battle or the other forces on the ground.[4]

i. These advanced tools – provided that their number grows to form an appropriate quantity – can aim massive fire at essential strategic enemy targets deep inland as well. It will also be in their power to protect landing and invasion forces in places and in ranges where the air force is limited.

j. To cope with various attack scenarios, including: missile salvos fired from the sea to strike at infrastructures or the civilian home front and disrupt troop mobilization; an attack by submarines to mine entrances to ports and attack (by means of missiles and bands of commandos) infrastructures; and a landing by commando forces from the sea that is intended to disrupt the movement of Israel's mobilized troops to the fronts and demoralize the civilian home front.

The weight and volume of the combat systems planned as a function of these properties dictated the optimal size of the ships. This would

allow them to operate even beyond the second and third circles (up to and beyond one thousand kilometers) with munitions that are no less small and accurate than what Israel's planes are capable of carrying, but without anti-aircraft and weather interference.

There have been four wars since the 1991 Gulf War in which the mobile naval fire base (surface ships and submarines) was one of the main factors in the modern operational battlefield. This protected firepower base fired long range missiles for pinpoint strikes on land with large warheads, and was also a base for launching attack planes, helicopters, and ground forces. In the circumstances in which Israel operates, the Israeli Navy has repeatedly proven in four of its last wars – the War of Attrition, the Yom Kippur War, the war to eradicate terrorist infiltrations from the sea (which continues until this day), and Operation Peace for the Galilee – that it is able to carry out its missions with great success with little force, almost without losses, and while being integrated into and contributing to the ground war.

In light of the threats to the State of Israel from the sea and in the wake of the experience from Israel's wars and the wars of other navies, it has become clear that in most instances, the aerial assistance given at sea in tactical (near) and strategic (far) fighting circles is not possible or effective or necessary. The operational naval/coastal fighting circle is the space in which the aerial force maintains regional aerial superiority and prevents the enemy aerial force from striking or from denying the naval force freedom of action. In this space, it is appropriate to plan receipt of aerial assistance that is intended to achieve regional aerial superiority, but not direct pinpoint tactical aid, which is also liable to endanger the forces.

In October 1979, six years after the Yom Kippur War, the navy staged an attack on Israel's coast (a "routine" exercise). Its offensive order of battle included twelve missile boats, two submarines, and nine squads from Shayetet 13 (the elite naval commando unit). Against it was the IDF's aerial force. Although the air force knew the time of the attack and was not busy with other tasks, and in spite of the fact that there was an expensive, cumbersome detection system along the coast that included fifty-eight permanent infantry observation posts (which were placed there in the wake of the coastal road massacre), the air force and the defensive forces that joined it did not succeed in preventing the attack from the sea, which was carried out to conclusion.

In the 1991 Gulf War Scud missiles landed in Haifa Bay, and in the Second Lebanon War (2006) rockets landed in the Haifa port, and the air force was not able to prevent this. As a result, in 2006 the navy was forced to evacuate its ships from the Haifa port, exactly as it foresaw back in 1979, when it planned for the Sa'ar 5 boats and the Dolphin submarines, which are capable of spending significant periods of time in the open sea outside the vulnerable ports. Indeed, the idea that arose among certain non-professional circles of making use of merchant ships for massive missiles attacks deep in enemy territory was examined in the past and found baseless. This is because of the vulnerability of the ships while the missiles are being loaded in the port (from this point of view, the advantage of the ships over air force bases is eliminated), and because at sea, they are not able to defend themselves. The attempt to "secure" them using other military hardware (especially in an arena saturated with missiles) will not succeed, and the techno-logistical process to maintain and operate them is complex and expensive. In the course of the Battle of the Atlantic during World War II, hundreds of "secured" merchant ships were damaged, as were dozens of Allied war ships that secured them on their way from the United States and Canada to Europe. This battle was decided by a thread, and Israel is not a superpower that can withstand this.

Israeli Naval Achievements

The Israeli Navy must be increased in size, improved, and adapted to the circumstances that have changed in the naval theater in particular and in the geopolitical arena in general, but without going to "superpower dimensions." This assertion is substantiated by a brief review of events that illustrate how the small, professional, sophisticated, and cunning navy gained its achievements in fighting, and what its contributions were to the overall battles. Without these contributions, these events would almost certainly have ended differently, and for the worse.

For nineteen years from the War of Independence until the Six Day War, the navy did not fight beyond Israel's borders. The first test given to the navy in the Six Day War, to attack five major naval targets in Egypt and Syria, ended with no results. To this failure were added three major disasters − the attack on the *Liberty*, the sinking of the *Eilat*, and the disappearance of the *Dakar* − which strengthened the disappointment with the navy and heightened doubts about its ability to integrate and

assist the general campaign of the IDF. By the end of the Six Day War, 800 kilometers of coastline were added to Israel's control, and in fact, the vast majority of the territory under its control was now bordered by water.

A sequence of three special raids by the IDF of unprecedented type and quality − the June 1969 ground raid on the Adabiya Peninsula, the July 1969 ground raid on Green Island, and the sinking of two Egyptian torpedo boats in September 1969 − placed the navy on the operational map of the IDF. The Egyptian torpedo boats were an obstacle to a raid by an armored IDF force that could operate with great success in broad daylight along fifty kilometers of the west bank of the Suez Canal, which was under Egyptian control (Operation Raviv). The sinking of the torpedo boats (Operation Escort), a sophisticated and difficult operation itself, was carried out by a handful of fighters from Shayetet 13. Shayetet 13 earned the operation at the initiative of Chief of Staff Bar-Lev, who made Raviv conditional on the successful execution of Escort. The armored force was transported and made a surprise landing by means of the navy's landing craft. For the first time in its history, the navy was used on the main front of the fighting, and its contribution was essential in reaching a ground target defined by the chief of staff. Escort and Raviv resulted in heavy losses and humiliation for Egypt. In their wake, the Egyptian chief of staff and the commander of the navy were dismissed. President Nasser suffered a heart attack, and died within a year. Following the raid on Green Island, historian Dr. Mustafa Kabha wrote in his book: "This action was a turning point in the War of Attrition. It symbolized the beginning of a new stage in the war...in which the military initiative moved from Egypt to Israel."[5]

Thus with a unit of only thirty-two fighters, Shayetet 13 brought about these results in the course of one year. As such, it paved the navy's way for the chief of staff's recognition that allowed it, during the Yom Kippur War four years later, to operate at full strength and with all its skills.

During the Yom Kippur War, only one naval target was destroyed from the air, versus forty-four vessels that were destroyed and captured by the navy. The navy did not lose any vessels, and over the entire course of the war suffered three losses, even though sixty sea missiles were fired at it in the two naval battle theaters, and it was forced to infiltrate five times (once in Port Said in the Mediterranean, and the other times in Hurghada in the northern Red Sea) with small Shayetet 13 forces, which

penetrated the enemy's harbors in missile-protected areas without any aerial assistance and pulled Egyptian naval forces from the open sea for their own protection. The Israeli missile boat force in this war comprised fourteen vessels, versus the twenty-four that were operated by the Egyptians and the Syrians. It achieved an historic crushing victory, and this became the first missile battle in the history of war at sea. No Israeli submarines operated during this war, though there were twelve Egyptian submarines operating in the Mediterranean and the Red Sea. Thanks to this offensive action by the navy, freedom of shipping was established for some 200 merchant ships going to and from Israel, almost as in routine times. The Syrian and Egyptian fleets were forced to remain in their ports, although even in Port Said they were under attack. With one exception, all of the navy's attacks in this war were carried out without assistance and with minimal participation by the air force. During the war, the Israeli home front spread along the coast was not attacked, and the mobilization of forces to the decision theaters was not disturbed.

Shayetet 13 attacked the main Egyptian harbor in Hurghada four times, and destroyed two Egyptian missile boats and blew up the main docking pier. A group of some twenty commandos accomplished this in thirteen days of fighting, while the air force avoided attacking Hurghada since it was surrounded by heavy missile protected areas (six batteries of surface to air missiles). Although the navy did not receive any direct aerial assistance in this theater on a tactical or strategic level, and in spite of its small force (with no missile boat, and even though all the vessels in its possession were defensive in their nature), it destroyed and captured twenty-three vessels that were in Egyptian active service; caused the Egyptians to withdraw from their main base, Hurghada; took 1,500 Egyptian POWs from the port of Adabiya in the northern gulf (which was conquered by the IDF with the help of the navy) to Israeli territory; and tightened the siege on the Third Egyptian Army from the sea. At the end of the war, this last step became a political bargaining chip for lifting the Egyptian siege in the Red Sea, through which the Egyptians attempted to foil the transfer of oil to Israel. With the same minimal forces at its disposal in the Red Sea theater, the navy ensured the flow of oil from the Gulf of Suez to Israel throughout and after the war.

On October 15, 1973, the navy achieved control over the Gulf of Suez, and thus paved the way for a well prepared landing of an armored division in the southwest of the Gulf (Operation Green Light), which was

a planned alternative to crossing the Suez Canal. The landing, which was proposed three times in the course of the war, was canceled "at the last minute," likely (in the estimation of the author and the late Maj. Gen. Israel Tal, who devised the idea) due to a lack of understanding and strategic daring.

During the Yom Kippur War, the Egyptian naval blockade in the Red Sea extended beyond the range of the vessels and the weapons available in that theater to the navy; the first six Sa'ar 4 missile boats that were built in Israel and were intended to circle Africa and report to the Red Sea theater reached it only about half a year after the war. The air force did nothing (and apparently could not do anything) in order to prevent or foil this blockade. This will likely not change in the future. Furthermore, it is only by virtue of the navy's offensive action in the Gulf of Suez while escorting the oil tankers from the Gulf to Eilat, on the one hand, and on the other hand, the attack on Syria and Egypt in the Mediterranean theater, which caused the latter to remain in their ports, and the directing of the Israeli oil tankers that sailed from Iran to bypass the Red Sea, that freedom of movement was achieved for all merchant ships. This made the flow of oil and the transport of grain and weapons to Israel's ports possible nearly throughout the war. A survey conducted after the war proved that during the entire period, the State of Israel did not lack for one drop of oil. In fact, Israel even sold oil to third parties that were suffering from the Arab oil boycott in this period.

Terrorist attacks from the sea posed a challenge that continued for about ten years (1970-79) that the IDF, with all of it resources, including the navy, was not able to overcome. The most serious attacks to this day (the coastal road massacre, the Savoy Hotel in Tel Aviv, and Nahariya) caused heavy losses in the heart of the country and seriously harmed civilian morale. In 1979, the navy adopted a new plan of action. In a proactive rather than reactive approach, it took the initiative and attacked every coast on which a force of terrorists was organizing, and interfered with their ability to sail or to move in the deep sea. This approach reflected the view that rapid, flexible special forces (Shayetet 13) should be used against terrorist forces, assisted, as ncessary, by "heavier forces" (missile boats, submarines, and the like), and that they should always have the advantage of surprise. All of this would be carried out with meticulous care (including taking risks) to avoid innocent casualties. All of the navy's

actions during the six years of "obstruction" against the terrorists ended without any casualties, and with the use of air force planes or ground forces outside the navy in a limited manner. They were carried out with careful attention to the rules of international law, and while avoiding publicity and media announcements. Eighty varied operations against terrorists were carried out between 1979 and 1984, with the result that twenty-three "contaminated" ships were caught and brought to justice in Israel, and seven ships were sunk in the harbors of Lebanon. All this brought about the complete eradication of deadly terrorist infiltrations from the sea. In fact, even in 1979, the change wrought by this campaign – which has continued to this day, for thirty-two years – was apparent. This is the sole sector along the country's borders that can boast of such a result.

Operation Peace for the Galilee opened after terrorist infiltrations from the sea had already been stopped for three years. In fact, all the methods and techniques for fighting the terrorists were tapped and practiced along the coasts of Lebanon during these three years, and they were the most effective and thorough preparations in the potential combat sector. Many operational patrols, which included all components of the fighting force (missile boats, submarines, and Shayetet 13), were carried out in the same period in other naval theaters as well, and were run secretly according to the "joint naval battle" format. These patrols were intended for the purposes of gathering intelligence and/or practicing the approach and the method. Indeed, the navy never distinguished between ongoing security activity and preparations for war, and therefore, the transition to Operation Peace for the Galilee, in spite of the complexity of landing and providing gunfire assistance to ground forces, was simple and smooth.

In the three years from 1979 to 1982, the navy evacuated its bases and its forces from the Red Sea theater, and during this time, the components of the landing, transport, and beaching forces were assembled at the Ashdod base and placed under one commander, who would ultimately serve in Operation Peace for the Galilee as the commander of the sea landing operation. He relied on the combat doctrine that was formulated and practiced in the Red Sea theater prior to Operation Green Light (which was prepared for the Yom Kippur War), and he trained his troops on this basis. His presence on the coasts of southern Israel and near armored corps and paratrooper bases facilitated the practice of

landing exercises and made the exercises and joint preparations more effective. During those years, many landing beaches along the coasts of Lebanon and other coasts were searched secretly by Shayetet 13 and the underwater mission unit (defensive divers). These were sorted, mapped, and marked as possible points for landing ground troops of all types.

Operation Peace for the Galilee was the largest direct naval aid given to ground troops in the history of the IDF. Some fifty-four vessels took part in the operation itself: twenty-two missile boats; two submarines; fifteen Dabur boats; three landing craft (outdated); an auxiliary boat with thirty-four rubber boats for transporting the paratroopers to the landing beach; a tow tug for rescuing vessels; and a group of Sa'ar and rubber boats for transporting beachhead and ambush troops operated by Shayetet 13 forces to seize and protect the landing beach.

In the first ten days of the operation, the navy landed 388 armored fighting vehicles of various types, including tanks, cannons, and transport and rescue vehicles, 604 paratroopers from Division 96, and armored corps soldiers, without any real mishaps. The navy refused aerial fire assistance (for fear that its forces would be hit), and the navy also refused troops of another division, who were stuck south of the city of Sidon and transferred northward. In the course of the paratroopers' advance along the coast northward in the direction of Beirut, the navy, using missile boats, landed 128 artillery shellings (about two thirds of them based on requests from the paratroopers).

For three months more, the navy undertook a naval blockade of the Beirut-Tripoli sector, and during that time additional troops and armored fighting vehicles were landed and many attacks were carried out, especially in the Tripoli sector. In all, 4,469 people and 1,087 vehicles of various kinds (tanks, armored personnel carriers, cannons, and trucks) were landed and transported during this time. Following the navy's offensive action in the Tripoli area, IDF POWs in the hands of the terrorists were returned (by sea) on November 24, 1983, and Arafat and the terrorists under him were removed from this region on December 20, 1983. In the period preceding Operation Peace for the Galilee, most of the members of the General Staff were apprehensive regarding the landing operation, with the exception of the chief of staff, Rafael Eitan, who unwaveringly supported and encouraged the navy, which believed that the operation was possible. Throughout Operation Peace for the Galilee,

as well as in the preceding and succeeding periods, the navy suffered no casualties and no naval vessels were damaged.

Conclusion

Combat experience, taken with an assessment of the elements operating in the naval theater, leads to several conclusions. First, a naval force alone that is built correctly and equipped with enough of the right tools will in the foreseeable future be able to halt or prevent a massive attack from the depth of the sea against Israeli territory. It would be difficult if not impossible for an aerial or ground force to prevent or thwart such an attack.

Over more than thirty years, from 1979 – when planning began for the navy's order of battle – until today, the approved order of battle has been whittled away and has shrunk to three Lahav Sa'ar 5 missile boats, eight Nirit Sa'ar 4.5 missile boats,[6] and five Dolphin submarines; the latter have not yet been built. (This minimal order of battle was built thanks to the examination and recommendation of Maj. Gen. Tal, who headed a defense establishment committee appointed by then-Defense Minister Yitzhak Rabin and Chief of Staff Dan Shomron.) A development space was planned that will be capable of integrating other advanced systems into the infrastructure, which was built to carry a significant amount of varied armaments, including missiles, and therefore, an effort should be made to allocate resources in order to exploit and complete these systems.

The Sa'ar 5 boats, where "suitable armaments" will be installed on the decks (this may require that they be enlarged), can in the future also participate in defending the country's skies, by acting as mobile fire bases that are difficult to locate. This is in sharp contrast to airports and sea ports in Israel, which are stationary and publicly identified, and a target for enemy attack. The addition of "suitable armaments" will also help to assist in carrying out long range naval raids.

Experience has shown that to execute landings and beachings from the sea to the coast and to undertake raids against both near and remote targets (which are near the shipping lanes to Israel), decisive naval tools are needed such as missile boats, submarines, and Shayetet 13 forces that will protect and cover the landing troops, without necessarily requiring aerial forces. While naval task forces carry the full strength of weapons and means of protection and are equipped to conduct a battle

along the way against targets located at long ranges, under the best of circumstances aerial forces are built to reach the targets, strike at them, and return immediately to their base because of time constraints and because other troops require coverage and protection, without which they have a curtailed ability to act and attack far targets.

Only a command and control system that is based mainly on naval components can prevent terrorist infiltrations from the sea to Israel's coasts, since only a naval force is built to identify (and usually also to detect and process a naval picture, and to prepare a pinpoint response immediately (before the terrorist target disappears/escapes) in the maritime space. This has been proven in the only sector in Israel in which in the past thirty-two years, fatal infiltrations from the sea have been completely stopped and there have been few casualties (the notable exception is the mishap in a Shayetet action in Lebanon in 1997).

Only a naval force can ensure the movement of essential cargo shipping during wartime and afterwards. With the same order of battle built for conflict and confrontation on the naval battlefield, it is in fact possible to realize this freedom of movement. For this purpose, a specific addition to the order of battle, beyond what was planned and decided on in the General Staff – i.e., eight Sa'ar 5 boats and six Dolphin submarines – is not necessary. An offensive action by the navy's advanced fighting force has the ability to confine enemy navies to their ports and create freedom of maritime movement, which will make it easier for the state to function in emergency situations and in war. Thus, not only will it become possible to transfer essential equipment to Israel's ports; it will also be possible to supply weapons and systems for IDF aerial and ground troops.

The new order of battle that was built has the potential for development and for a lifespan that is much beyond 10-20 years. Time cycles in the navy are necessarily planned to be much longer than the norm in the other branches of the IDF, but this is for purposes of operational exploitation that preempts the enemy and not as a delay in buildup. The first Sa'ar 5 boats did not arrive in 1986 as planned but in 1994, and the first Dolphin submarine arrived in 1999, fifteen and twenty years, respectively, from the start of the planning. This was notwithstanding that in the basic work plan, twenty-four missile boats, including eight Sa'ar 5 boats and six Dolphin submarines were planned, and in certain time segments were

even approved for building. It is true that the navy took advantage of the delays in building for more in-depth planning, but the vessels that arrived were too few and too late. The delays stemmed from failures of decision making and interference, and a lack of integrative and systemic vision, and not from budgetary reasons. In any case, with the delays, prices rose, which reduced the scope of the order of battle that was planned.

In the current and future battlefield, imperatives will apparently continue to exist that are relevant and unique to the naval branch. The potential inherent in the navy has not yet been tapped, both because of the delay in completing the systems for the excellent vessels that were built in the new order of battle, and because the building and completion of a quantity of the order of battle and its required systems is being delayed. The quality of these vessels, in the opinion of top experts (such as former US Secretary of the Navy John Lehman and the heads of the Dutch navy, who helped to build them), is way ahead of those of other navies in the world. They were specified, planned, and built by virtue of advanced operational and professional thinking by the commanders and engineers of the Israeli Navy, and they are operated today with great success by first rate officers and fighters.

In 2001, then-Chief of Staff Shaul Mofaz stated:

> When I say in the battlefield, I mean also on land, on sea, and in the air. Our vision today is a multi-branch vision. This is how we are building the IDF, this is how its strength is being built, and this is how the General Staff operates its forces in these three arenas − through optimal integration and with the goal of decision and victory.[7]

It is evident, however, that the integration and the multi-branch vision is still lacking, in terms of a realistic assessment of the far reaching threats in the naval theater that Israel must confront, the correct balance between the naval branch and the other components of power in the IDF, and the navy's contribution to IDF victories in the operational battlefield. Therefore, the time has come to close the investment gap in Israel's naval branch at a faster pace. The existence of the wide, deep expanse should be recognized, as should the possibilities latent in the medium and the technology that have been developed for it, in the rest of the world and in Israel. Today, more than at any other time, these suit Israel's current and future needs. It is worth rising above conventions and adopting what is called in naval combat slang "a view beyond the horizon and precise

fire on a desired target." An analysis of the modern battlefield necessarily urges reorganizing the system for more effective yield by the IDF force components.

In his book *National Security: The Few against the Many*, Israel Tal wrote: 'The concept of strategic depth usually refers to geographic land spaces, but the sea can also constitute strategic depth if there is a navy that exploits its spaces and depths. Israel's navy must turn the sea into part of its security depth. The navy's mission must change – it must no longer be an auxiliary branch, but a strategic deterrence branch. Even though Israel's naval power is relatively small in quantity, it must be large in quality."[8] This vision has not yet been completely realized.

Notes

1 On June 11, 1971, nine RPGs were fired from a small boat near the Strait of Bab el-Mandeb at an Israeli tanker on its way to Eilat. Through great luck and resourcefulness, the tanker did not explode.

2 On December 1, 1983, for example, against all assessments, a Libyan submarine reached the Syrian port of Tartus, and anchored there. It succeeded in secretly moving from one of the ports of Libya, which is in the center of the Mediterranean, without the Sixth Fleet noticing it, in spite of the fact that many of its vessels were then at sea across from Libya and Syria and operated frequently in the Lebanon sector.

3 In March 1983, four years after the signing of the peace agreement with Egypt, a committee appointed by the Defense Minister to examine the IDF's budgetary resources and headed by Zvi Tropp, the Ministry of Defense economic advisor, "recommended the development of Sa'ar 5 by 1989, and supported the procurement of eight ships, two of them during the period of the Shahar B plan (by 1992), while attempting to increase the resources with the goal of realizing even three ships during Shahar B," Ministry of Defense, March 16, 1983.

4 This was done in Operation Peace for Galilee on a smaller scale.

5 Mustafa Kabha, *Harb al-Istanzaf: The War of Attrition through the Prism of Egyptian Sources* (Tel Aviv University, Yad Tabenkin, the Galili Institute for Settlement, Defense, and Foreign Policy Studies), p. 86.

6 These missile boats were built by Israel shipyards at the initiative of this writer, and were intended for the intermediate stage only.

7 General Staff symposium on "Decision and Victory on the Future Battlefield" at the National Security College.

8 Israel Tal, *National Security: The Few against the Many* (Dvir, Zemora Bitan, 1996), chapter 42, "National Security in the Future," p. 223.

Naval Flanking in Ground Warfare

Gideon Raz

"The indirect [approach] is by far the most hopeful and economic form of strategy."
B. H. Liddell Hart[1]

Israel's Coastal Border

The Mediterranean Sea, Israel's only open border, also borders Israel's enemies to the north and the Gaza Strip to the south, thereby linking it to enemy states. Thus, Israel's control of this naval arena would enable it to project military strength from the sea, and afford it the capability to embark on landing operations of various types. "The shores of the State of Israel, the naval interface with each of our enemies, require us to expand our naval strength to the point of being able to land forces from the sea. David Ben-Gurion even said that we are bound to view the sea as Israel's extended western territory."[2] The naval arena is the Achilles' heel of Israel's enemies and therefore also an opportunity for the IDF.

The Operational Need

> Today the threat of high trajectory fire, based on the use of conventional weapons (missiles, rockets, mortar bombs) in massive quantities, tops the list of threats Israel confronts. It joins the classical, conventional threat that was based on the use of large military systems engaging in battles of ground maneuvers...The IDF must use the two major components of its capabilities, firepower and ground maneuver, in order to damage both the enemy's military capabilities and its political or organizational infrastructure...An enemy seeking to avoid severe blows operates purposefully and cynically within civilian population centers.[3]

Rear Admiral (ret.) Gideon Raz, former Deputy Commander of the Israeli Navy

Frontal assault has traditionally been the IDF's main maneuver. Activity deep in enemy territory was usually reserved for special operations, with a limited effect on the duration and results of the fighting. An exception to this rule was the landing of paratroopers from the sea during the First Lebanon War. Now, especially in light of the change in the threat, it behooves us to consider whether the IDF should continue to focus only on frontal maneuvering or whether it should also consider expanding the capability to carry out substantive maneuvers deep in enemy territory. Naturally, transferring a significant maneuvering force into the depth of enemy territory, operating there, and maintaining it would mean that the IDF would have to rely on naval capabilities as the primary platform, with the aerial storming forces playing a complementary supporting role.

Conducting substantive maneuvers deep in enemy territory has several advantages: dispersing the enemy's forces and upsetting its link between the front and the depth; surprising the enemy and upsetting its equilibrium; and finally, tackling the elements deep in enemy territory where there is a clear advantage to the use of ground maneuvers rather than firepower.

The need for flanking maneuvers[4] stems in part from the growing urbanization along the Syrian front, which appears to be the result of intentional Syrian policy designed to thwart IDF maneuvering and firepower. According to Liddell Hart, the flexibility provided by amphibious capabilities is the strategic resource at the disposal of a state with a coastline. The primary benefits of landing operations are mobility and flexibility, i.e., concentrating force and hitting the enemy whenever and wherever a state chooses. Such operations aim to take advantage of the surprise element and the enemy's weaknesses. The enemy, aware of Israel's ability to conduct landing operations on its shores, is stymied by its inability to guess when and whence the attack might come.

However, even if Israel enjoys superiority in the naval arena, it is clear that the battle cannot be decided at sea. In fact, the IDF has aerial and naval superiority, two essential components for the existence of a naval flanking option. In constructing a larger amphibious force, the IDF would be able to translate its naval superiority into a significant contribution for attaining decisions in ground battles. The essay below examines the components of the landing process and offers some recommendations on construction of this type of force.

Amphibious Operations: Historical Background

The history of naval power documents amphibious operations of various types and scopes.[5] These played a large and decisive role in World War II, from bombardments with naval gun fire and commando raids, through naval raids, to the landing of entire armies. An impressive range of amphibious operations – in terms of scope, operational conditions, and forces used – likewise took place following World War II. Among the most notable were the Anglo-French landing at Port Said (1956), the Turkish landing on Cyprus (1974), and the British landing on the Falkland Islands (1982), but the most striking landing in the post-World War II era was the Inchon landing in 1950.[6] While the American landing capabilities in the Korean War were but a faint shadow of what they had been in World War II, the United States was still capable of creating a quick maneuver from the sea and providing logistical support at shores that had not previously been prepared for landing.

The IDF's short naval history is studded with fairly impressive landing operations; especially given the relatively low priority the Israeli military has usually accorded this type of fighting. There were several operations representing milestones in this field, beginning with the Sinai Campaign, when Israeli Navy landing craft accompanied Brigade 9 troops along the shore in the move to capture Sharm el-Sheikh. The ships fired on Egyptian positions and assisted the provision of fuel to the force, which was isolated from every other supply route. In certain cases, even tanks were landed to strengthen the brigade. It is highly doubtful that these tanks would have reached their destination any other way or would have arrived in time to make a difference.

The Raviv Operation on the western shore of the Gulf of Suez in the War of Attrition was a joint operation of naval landing and armored vehicle activity, and may be considered one of the most successful of all IDF operations. Raviv had all the components of a classic joint landing, integrating tools and forces from all three branches of the military. The armored force did its job by attacking military camps, sentry posts, radar stations, military vehicles, and tent formations, causing heavy casualties to the enemy (some 150 dead) and heavy damage to installations, staying on the Egyptian shore some ten hours, and moving along an extended axis by daylight. More importantly, the operation achieved its strategic goal by demonstrating to the Egyptians that their rear was vulnerable,

thereby forcing them to mobilize forces there, which resulted in an easing of the military pressure on the canal sector for some time.

No naval landing was carried out in the Yom Kippur War,[7] despite long, exacting preparations in the Red Sea by the Israeli Navy in conjunction with armored formations that were designated to participate in the operation. According to one school of thought, this would have been the optimal use of the IDF's amphibious capabilities since the navy had the naval superiority that allowed the plan to be put into practice. However, the IDF found it difficult to allocate a sufficient number of forces at the beginning of the war and did not need the operation in order to reach a decision toward the end of it.

As part of the Peace for the Galilee war, the Israeli Navy undertook a large number of landings and raids from the sea. The most prominent was the landing of infantry and armored forces at the mouth of the Awali River, a naval flanking operation that led to successful flanking missions around terrorist forces that were concentrated in the Sidon area.

Many people within and outside the IDF claim that given the current geopolitical array, and especially the peace agreement with Egypt, the IDF no longer has the possibility to carry out naval flanking maneuvers that would help attain a decision on land. Yet according to Maj. Gen. (ret.) Amos Yaron,[8] who commanded the landing operation on the Awali shore in Operation Peace for the Galilee, the landing array was highly critical during the years Israel controlled the Sinai Peninsula and when Lebanon formed the background of every security discussion. The IDF retained the idea of naval flanking throughout; coordination and training were an integral part of IDF's state of preparedness.

The Future of IDF Amphibious Operations

As part of the formal definition of the objectives of the Israeli Navy, the mission of supporting the ground forces towards a decisive victory in the ground battles is accorded high priority. Assisting a decision on land encompasses a range of activities, including:[9]

a. Defending Israel and the areas in which the IDF is active from attacks from sea, thereby relieving the ground forces of the need to secure the sea sector.
b. Preventing the flow of reinforcements to the front through enemy ports.

c. Pinning down the enemy's forces in defensive missions to protect military and civilian infrastructures along its shore.
d. Bombarding targets along the shore.
e. Carrying out commando raids from the sea.
f. Gathering intelligence via the sea.

Nonetheless, the most significant support by the Israeli Navy in reaching a decisive result in a ground battle lies in outflanking naval maneuvers. In general the final objective of the navy's battle is in the land battle; the naval battle does not take place for its own sake. The primary goal of navies is to reach superiority at sea in order to support the ground forces, both using fire from the sea and by carrying out naval outflanking maneuvers. The direct effect of the naval force occurs (inter alia) by means of sea-to-land fire with various types of missiles, aerial attacks from aircraft carriers, naval artillery, and landing of forces of various scopes.

The assistance of naval forces to the primary ground effort requires several underlying conditions:[10]

a. Transport and landing capability of armored troops at least at the brigade level in one round (which means landing capabilities for a division in four to five rounds).
b. A total control of the transport and landing route with every type of warfare – in the air, at sea, underwater – so that the landing force is not exposed to attack during sailing or during beaching.
c. Systemic targets on land suitable to attack by the landing force coming from the sea based on the following criteria: the lack of easy land routes to these targets; the existence of an appropriate area for landing in terms of accessibility from the sea and suitable terrain conditions for organizing after beaching; the likelihood of operational surprise likely to destroy the defensive systems of the enemy; and the ability of the landing force to join up with other forces arriving by land or that have landed in other locations.

Except for the landing operation at the mouth of the Awali during the Second Lebanon War, no significant outflanking naval operations were carried out by the IDF, apparently for several reasons. One, there were concerns about the risks to IDF forces from the sea route of the landing forces. Two, the targets appropriate for attack were far from where primary efforts were underway and there was concern that dividing the

ground forces among remote targets would do more harm than good to the primary effort. Three, constructing a massive landing force of troops via the sea requires systematic investment in equipment, weapons, and training at sea, in the air, and on land.

Executing a Landing Operation

An operation of landing troops on enemy shores, in order to conduct an outflanking naval maneuver, is a joint naval-ground-air operation. Such an operation is likely to include the following:

a. Conquering the beachhead from which operations will be launched in the depth and rear of enemy territory.
b. Taking control of the area in order to join up with other ground troops or for use by naval and aerial forces as a base for further operations.
c. Taking control of the area in order to deny enemy access to it.
d. Destroying enemy installations.

Naval landings are considered the most complex of military operations. For this type of action, a great deal of training and rehearsal is necessary. In addition, coordination and control of the composition of forces – ground, naval, aerial, and firepower – are critical. There are a few main stages of an operation. The first involves concentrating and training the forces in an area that in terms of sea, shore, and adjacent ground conditions is similar to the enemy area planned for the landing. Rehearsals involve the staff of the designated unit and navy vessels and equipment. The second stage involves rehearsing loading of the troops and their equipment. The third stage is transport oversea from the loading point to the point of debarkation. The fourth stage is the landing itself, from the rendezvous point of the vessels to the landing, and the securing of the beachhead.

A number of considerations – many of which are common to ground offensive operations – affect the landing operations. The operation will usually enjoy the advantage of taking the initiative and the ability to choose among a number of targets. Until the execution of the landing, the landing area must be kept a tightly guarded secret. However, more time is needed to embark on an assault from a shore landing than what is usually assessed for attacks on the ground.

From the time of the landing, the ground troops are limited in terms of assault abilities but are highly exposed to enemy fire. Fire support

during the first stages of the operation is based entirely on support from the sea and the air, taking advantage of long range precision armaments capabilities. The navy must make sure[11] to neutralize shore-to-sea missiles aimed at the debarking forces. The importance of preparations and planning has been summed up as follows:

> In the operational plan, the organization and implementation of the loading shore will have been spelled out in detail…the manner of transporting the troops and the armored vehicles at sea, the method for taking control of the beachhead and securing it. The plan will also have listed in detail the actions required to prepare the landing zone, preparing the landing crafts for the landing, the order of the landing, and manner in which the troops and the armored vehicles are to be taken out of the ships and placed on the shore.[12]

Choosing the Landing Zone

The primary considerations for choosing a landing zone include the sea and land conditions required for establishing a beachhead with sufficient depth to defend the zone from enemy fire. The choice of landing zone is dictated by the specific mission, the strength of enemy outposts, the existence of installations such as piers and quays, the number of landing shores and their features, ground conditions for carrying out the mission at its later stages, timetables, and weather conditions.

a. The mission: The zone chosen must allow for landing by a force of the required size, from which point the force will be able to proceed with carrying out its missions.
b. Daytime versus nighttime is the primary consideration, in context of the relative effects on the element of surprise, the ability of the aerial force to operate, enemy troops on the ground, at sea, and in the sky, navigation difficulties, and the ability to operate after the landing. Nighttime is useful in gaining a level of surprise and makes it difficult for the enemy to attain the information necessary to organize its troops.
c. The beachhead is the sector where a navy unit (usually a naval commando unit) lands and defends the area, assisted by other units, until a ground force of sufficient size lands, deploys, and begins to advance towards the predetermined targets. There is an operational option to take control of the beachhead and control sites in the vicinity

by troops flown in by helicopter. At the first stage, a commando force determines the situation on the shore and the immediate area; later, it is possible to reinforce the area with troops flown in by helicopter or brought in from the sea, or both.

d. Rehearsal and training:[13] Preparations for landing operations require strict, individualized rehearsal and training to ensure close cooperation and full coordination between all operation participants. The planned forces must train together so that each part understands the jobs, capabilities, and limitations of every component in the combined force.

The Force Units and their Missions

It is essential that the force components operate according to clear command and control principles. Cooperation between the ground and naval forces may be ensured through the normal procedures of inter-branch cooperation or through training of the force with a joint command for the operation. The command groups of the ground and naval forces must be located together on the command ship, preferably with a multi-branch presence at all command and control levels. A breakdown of the force structure and its missions shows:[14]

a. A naval task force, whose missions are intelligence gathering, defense against the enemy's naval forces, landing the troops and their equipment on the shore, assistance with sea-to-shore fire, and management of the sea-to-shore communications system. The naval force is to be divided into secondary forces on the basis of the missions. These include a unit to examine the landing shore, which entails identifying enemy outposts in the beachhead zone and vicinity; determining the state and conditions of the sea and landing beach; and checking for obstacles in the water and on the landing shore. There must be a unit to gather information on the enemy's aerial presence, and a unit to assist with fire from the sea, which will provide gun and precision fire to support the landing troops. "Naval platforms, which are mobile, carry large numbers of missiles (and other precision arms), and supported by satellite navigation capabilities, can play a central role in offense missions. In terms of the capacity to carry weapons, the naval platform is equal to many fighter jets. While naval platforms too are vulnerable, the naval

battlefield has become sophisticated and endowed with technology in ways that strengthen Israel's superior capabilities."[15] In addition, there must be a control unit, i.e., one or more ships controlling or helping to control the movement of troops to the landing point, ensuring ongoing and intact communications with all landing vessels, and assisting in controlling fire from the sea and creating smoke screening, if required. After the first landing wave, the control unit will direct the vessels of the second wave, as well as the landing of the equipment and the armored and other vehicles as required by the operation.

b. The landing force, which is transported by landing craft operated by the navy. These forces take control of the shore immediately upon landing, lead the troops parachuted in or dropped by helicopters, and provide close fire assistance to the landing troops.
c. Air support, which will assist in intelligence gathering, prevent interference by enemy airpower, attack enemy targets, transport parachutists or forces by helicopter, and provide close air firepower for the landing forces.
d. The beach party: The beachhead link is a naval force, commanded by the beach master, in charge of activity along the waterline of the landing shore. The size of the party depends on the size of the landing beach and the number of the planned landing troops. It will generally contain signal communication, boat maintenance personnel, a medical team, representatives of the battalions that are landing, and liaisons with the air force and ground firebases.
e. The shore party is a group of landing troops responsible for organizing and directing the troops as they land, comprising representatives of all landing units, including medical, engineering, and communications. The commander of the party is in charge of communications with the navy's beach master.
f. Beach activity:[16] During the landing, it is necessary to maintain the organizational structure of the units, from the squad level up, in the sea and on the shore. The loading of the troops and their debarkation must be planned accordingly. Once it lands, every unit is relied on for the landing of the remaining units from its parent unit. This means that it is necessary to load the troops in such a way that organic units arrive sequentially on the landing shore. Success in the critical phase

of the fighting that takes place immediately upon landing is based on the fighting capabilities at the squad and platoon levels. Every small unit is built up with the landing of its parent unit.

g. Intelligence reconnaissance before and during the landing: Landing a patrol unit for the purpose of intelligence gathering is common near the time of the landing of the main force. The most important information includes: the location and strength of enemy positions; the location and type of enemy fire positions (shore-to-sea batteries, artillery, anti-tank); the location of obstacles on shore and in the water; data about waves on the shores, the type of shore, and ground conditions leaving the beachhead; the location of communications, command and control centers, and observations posts; identification of landing areas for aircraft in the landing shore area; and discovery of errors on the map of the region.

In addition to the force components, there are further aspects to the landing operations, including:

a. The size and structure of the beachhead. The beachhead should be deep enough to allow defense against mid-range artillery. Conquering a beachhead of this size requires a relatively large force without exposing the flanks of the troops. The shorefront is determined on the basis of the topography of the area and in response to threats in the immediate surroundings.

b. Establishing the beachhead: At the first stage, the naval commando unit must inspect the landing shore, undertake hydrographic examinations of the shoreline and the sea, and ascertain that there are no natural or other obstacles that might interfere with the landing. The unit must observe the area and identify enemy presence. At the next stage, it will direct infantry troops arriving by specialized navy vessels to the shore to take the beachhead before the landing of the first wave of the main force.

c. Advancing from the beachhead: In landing operations, ground units must evacuate the beach as quickly as possible, moving rapidly away from the shore into the rear or in whatever direction has been assigned. Despite the importance of creating a secure perimeter around the landing shore, the landing force commander must not act defensively. Offensive activity is the best way to secure the landing shore.

d. The action plan: The choice of the landing shore is a function of the goals of the operation, an assessment of the enemy in the surroundings, the topographical features of the possible shores, and the ground conditions beyond the landing zone, time, and target ranges. The time of the landing, day or night, depends on the nature of the operation. The scope of the landing force is a function of the size and composition of the landing troops, the ORBAT of the landing at the navy's disposal, the size of the landing shore, and the plan of action following the landing. The depth of the beachhead taken by the landing force is a factor influencing the action plan for the coming stages. In the initial landing stages, the ground force will rely on effective cover provided by the navy and air force. Fire from the sea, aerial cover, and guided precision fire must be concentrated in order to ensure the success of the landing. Usually there is only a single opportunity to carry out a successful landing. Should the attempt fail, it is very difficult to change the situation. Therefore, it is necessary to deepen the hold on the ground in conjunction with the fire support that may be provided to the attacking force.
e. Protected beaches: It is preferable to avoid landings across enemy positions, to land light forces on unprotected flanks (even if the geographical conditions are not optimal), and to neutralize enemy positions with fire from the flanks before attempting the primary landing.
f. Using existing infrastructures:[17] In the first stage the preferred mission of a landing operation is to take control of the pier/jetty to allow quick, efficient flow of the forces and their equipment, even before the surprised enemy has had a chance to organize its troops for a counterattack. A preemptive, in-tandem strike of the raiding party's forces against enemy defensive systems liable to act near the pier/jetty should be considered. Special forces should land from the sea or air near the jetty, take control of it or part of it, and allow the landing vessels to enter with the first wave followed by the vessels with the main force and its equipment.

Types of Landing Operations

There are several types of landing operations.[18] One is intended for deception: a naval force arrives in the area and carries out what looks like

a landing. The aim of the action is to force the enemy to dispatch large forces to the area at the expense of the true destination. In World War II and in the 1991 Gulf War the US Marines undertook many actions of this kind.

The second type of landing operation is a raid from the sea.[19] The naval raid is an operation of a limited scope – relative to the size of the force and the length of the operation – taken by a force with high mobility operated from the sea. The nature of the raid is a type of mini-warfare based on the naval force. It is designed to unsettle and wear down the enemy, suppress its assault initiatives, and force the enemy into a defensive posture. By its nature, a naval raid is not likely to change the fate of the war but often its utility is likely to be high, especially in terms of morale.

A third type involves landing for the sake of assuming control of an isolated target, such as a jetty or an airfield. In such an operation, there are no missions requiring further movement of the troops into the depth of enemy territory. In a similar vein, there is landing operation for the sake of conquest**.** This operation opens a beachhead or a jetty for the sake of the quick offloading of troops as part of a comprehensive assault. This type of operation is the most complex, and speed is critical. It must allow the flow of troops in order to capitalize on the success of the surprise element. Taking control of a pier/jetty is a preferred goal.

Finally, there is evacuation by sea. The operation plan will include the evacuation of the troops by sea or their joining up with ground forces. Evacuation will take place as the result of strategic considerations or as a retreat forced by developments in the battlefield. Retreat and evacuation by sea under enemy assault is a complex operation accompanied by many risks to the evacuating troops.

Command, Control, and Logistics

A naval flanking operation is considered the most complex among all military operations. It combines forces from all three branches of the military and troops from different corps that are not trained in the unique battle doctrine of amphibious operations. It also requires full coordination between all participants and is (usually) controlled by a unified command post. The database of all units of the force must be shared and up-to-date. A conceptual (as opposed to technical) summary based on the US Marine Corps Command and Control Doctrine deals with

understanding the system known as "mission command and control."[20] Accordingly, the command and control plan for a joint amphibious operation depends on the unique requirements of the specific conditions of the operation. In most cases, one should prefer the "mission command and control" approach as it more effectively deals with the unexpected and with changing timetables. Since uncertainty defies control, flexibility and speed are preferred. The approach allows flexibility in handling rapidly changing conditions and better use of windows of opportunity. The approach provides for the degree of cooperation necessary to an integrated effort yet gives commanders at all levels the latitude to act with initiative and daring.

As part of the landing forces, there will be a secondary force whose function is to establish an infrastructure for a logistical base (supplies, maintenance, and medical) as well as a helicopter landing pad. At a later stage, it will be necessary to maintain a continuous flow of supplies from the rear through the naval force to the beachhead. The supplies will arrive according to a timetable and contents determined by the commands of the operations and according to operational developments on the ground.[21] The US Marines have held deliberations on the value of maintaining the logistical base on ships outfitted to this end and located in the naval sector beyond the enemy's range of fire. Such a ship or ships would be secured by a navy task force. Should the landing force wrest control of the jetty or pier, this would become the logistical base. The operations plan should determine the logistics plan on the basis of the following considerations: the logistical contents on the beachhead relative to the scope of the force landing in order to complete its missions; the conditions and tools available to the force allowing them the opportunity to establish logistical support at sea; and the distance between the logistical base at sea and the fighting force on the beach (depending on the enemy's ability to threaten the ships at sea).

In the medical context, it is necessary to find the balance between the need for providing medical assistance on the beachhead and medical treatment on the ship outfitted for this purpose until evacuation to a hospital. The plan must solve the problem of providing first aid and stabilizing the injured near the fighting force and later evacuating to a medical base on a hospital ship or a hospital in the rear, depending on the type of injury and the decision of the doctors in the zone.

Conclusion

The very existence of an active amphibious force in the IDF order of battle[22] would lock enemy troops into defending targets on the shore at the expense of placing forces in the primary arena. Operations such as outflanking naval maneuvers are likely to upset the equilibrium of the enemy's political and military leadership. By landing troops from the sea, for example, it is possible to threaten Hizbollah leadership centers in southern Beirut. Large, tightly clustered orders of battle − armored corps, anti-missile systems, and rocket, missile, and artillery batteries − would present themselves on the main front line.[23] Some of the Syrian rocket launchers are located in the depth of the country, as a result of the missiles' extended ranges. Therefore, fire from the sea and forces arriving by a flanking maneuver to take action against these systems have important functions.

A common argument in the IDF against developing and maintaining naval flanking capabilities relates to the allocation of the necessary resources. Accordingly, in order for troop landings to be effective in wartime, it would be necessary to land a joint force at the division level in a very short period of time, requiring transport and landing capabilities of an armored force of brigade size at every landing round. Such a capability would require a major investment of resources, at a time when the IDF is in a tight budgetary position. Other claims touch on the high risk inherent in such operations (a factor that lessens leaders' motivation to approve them) and the inability to allocate a ground ORBAT formation for a flanking maneuver. There is also doubt about the presence of targets for which it is possible to execute a naval flanking move that would at the same time allow the flanking force to join up with the primary ground force and have a tangible effect on the main ground battle. This skepticism grew once Egypt left the circle of active warfare against Israel.

Despite these claims, it seems that naval landing operations are still fully relevant both for the world at large and for Israel. The peace treaty with Egypt and the withdrawal from the Sinai Peninsula may have taken the most natural target for sea-to-shore landing operations on the Gulf of Suez off the table, but there are still many contexts, both in terms of Israel's routine security measure and in terms of warfare, in which landing on the Lebanese or Syrian shore would effectively serve various

Israeli interests. In any situation they can contribute to pinning down enemy forces and keeping them away from the front lines.

The question of resources allocated by the IDF to amphibious goals requires clarification. First, the attainment of naval superiority, which is a requisite precondition to a significant naval landing on enemy shores, is already obligatory on the basis of the Israeli Navy's other missions, first and foremost securing the nation's shores. Therefore, the core of the required resources for creating the conditions necessary for naval flanking maneuvers is already invested. The additional marginal resources required to construct a flexible, effective amphibious force to carry out naval flanking maneuvers are not high (primarily landing craft). Yet the IDF's ability to translate naval superiority attained in the first days of fighting into a significant contribution to a victory on the ground is highly limited.

Staff work is underway in the IDF in order to budget and strengthen the IDF's landing capabilities. The Israeli Navy is undertaking a professional examination of the different options for the various types of landing vessels that could provide responses to the requirements of the ground forces. By using the navy and a designated formation of ground forces, the IDF must construct amphibious capabilities that will allow it to use the advantages of the sea and the indirect approach by landing troops on selected targets along the coastline in the enemy's rear.

The objective must be construction of a designated force that would be ready and prepared to carry out large scope flanking operations that would be carried out jointly from the sea and the air. In order to promote the subject of flanking maneuvers effectively, there seems to be room for establishing a designated command that would incorporate commanders from the naval and aerial branches. This command would bear overall responsibility for the subject, and command flanking operations in war.

Notes

1 B. H. Liddell Hart, *Strategy: The Indirect Approach* (New York: Frederick A. Praeger, 1954), p. 162.

2 Maj. Gen. Sami Turgeman, CO ground forces, in a lecture to students at the Command and Staff College, December 30, 2009.

3 Gabriel Siboni, "War and Victory," *Military and Strategic Affairs* 1, no. 3 (2009): 40-42, at http://www.inss.org.il/upload/(FILE)1269344811.pdf.

4 Author interview with Maj. Gen. Gadi Eisenkot, GOC Northern Command, November 15, 2010.

5 Gideon Raz and Ariel Levite, *Whither the Navy? Some Thoughts on Doctrine and the Construction of the Israeli Naval Force*, Memorandum No. 19, Center for Strategic Studies, July 1987.
6 Donald Boss, "Army and Security," The Second Latrun Conference on Ground Warfare, September 16-17, 2008.
7 Zeev Almog, "Israel's Naval Arena: Assessment and Lessons," *Maarachot* 299 (July-August, 1985).
8 Author's interview with Maj. Gen. (ret.) Amos Yaron, November 24, 2010.
9 Raz and Levite, *Whither the Navy*.
10 Ilan Amit, "Constructing a Naval Force for the 1990s," *Military Studies*, Rafael Advanced Defense Systems, December 1980, p. 72.
11 Author interview with Maj. Gen. (ret.) Amos Yaron, November 24, 2010.
12 Zeev Almog, "The Israeli Navy in Operation Peace for the Galilee," *Maarachot* 413 (July 2007).
13 *Landing Operations on Hostile Shores*, War Department, June 2, 1941.
14 Ibid.
15 Gideon Raz, "Naval Firepower and Its Role in Land Battles," *Military and Strategic Affairs* 2, no. 2 (2010): 22 at http://www.inss.org.il/upload/(FILE)1298302355.pdf.
16 *Landing Operations on Hostile Shores*, War Department, June 2, 1941.
17 Carlton Meyer, *The Spectrum of Future Warfare*, www.G2mil.com , 2010, Chapter 9.
18 Ibid.
19 Raz and Levite, *Whither the Navy*.
20 *Command and Control*, U.S. Marine Corps, October 4, 1996, p. 105.
21 *Naval Expeditionary Logistics: Enabling Operational Maneuver from the Sea*, National Academies Press, 1999.
22 Author interview with Brig. Gen. Shai Brosh, former commander of Shayetet 13, October 22, 2010.
23 Author interview with Maj. Gen. Gadi Eisenkot, GOC Northern Command, November 15, 2010.

Israel's Unilateral Withdrawals from Lebanon and the Gaza Strip: A Comparative Overview

Reuven Erlich

Introduction

In the last decade, Israel unilaterally withdrew from two areas: the security zone in southern Lebanon and the Gaza Strip. Israel had previously withdrawn unilaterally from occupied territories without political agreements, but these two withdrawals were more significant and traumatic, both socially and politically, than any prior withdrawal. The time that has passed since these unilateral withdrawals affords us some historical perspective and allows us to compare them in terms of their outcomes and the processes they generated, both positive and negative. This perspective allows us to study the larger picture and trace influences that in the heat of the dramatic events were difficult to discern and assess.

When looking at Lebanon and Israel's policies there, my approach is not purely academic or that of an historian who wrote a doctoral thesis on Israeli-Lebanese relations. I participated in some of the events in Lebanon, not as a decision maker but as a professional, whether in the course of my service in Israeli Military Intelligence, both in Tel Aviv and in the Northern Command, or in my position with the Ministry of Defense, as deputy to Uri Lubrani, Coordinator of Government Activities in Lebanon. My perspective today on Lebanon and the Gaza

Col. (ret.) Dr. Reuven Erlich is Head of the Meir Amit Intelligence and Terrorism Information Center at the Israel Intelligence Heritage and Commemoration Center (IICC). This essay is based on a lecture delivered at the conference "The Withdrawal from Lebanon: Ten Years Later," which took place at the Institute for National Security Studies on June 28, 2010.

Strip is shaped by my position as Head of the Meir Amit Intelligence and Terrorism Information Center at the Israel Intelligence Heritage and Commemoration Center (IICC), which studies the various arenas that are points of origin for terrorist activity against the State of Israel.

Background to the Unilateral Withdrawals

On May 24, 2000, the IDF withdrew from Lebanon; the disengagement from Gaza took place in August 2005. Both withdrawals were unilateral, that is, were carried out without any agreements with a state entity (Lebanon) or a semi-state entity (the Palestinian Authority). In both instances, the IDF withdrew to an international border rather than to one security line or another. Neither withdrawal provided a fundamental solution to the problems Israel faced and that it continues to face in these arenas.

The withdrawal from Lebanon in 2000 was preceded by other unilateral withdrawals undertaken without agreements or political arrangements (though it was the most significant of them). The IDF unilaterally withdrew to the Awali line during the IDF's presence in Lebanon after the First Lebanon War and also withdrew to the Israeli-Lebanese border and established the security zone (January 1985). During its prolonged presence in Lebanon from the outbreak of the war and the subsequent gradual disengagements (1982-2000), Israel experienced a peace agreement with Lebanon that collapsed (the May 17, 1983 agreement), military talks that failed (the Nakura talks, November 1984-January 1985), and Israeli-Lebanese negotiations in Washington as part of the Madrid process, which ultimately went nowhere (1991-93). In all three cases, Syria, which became the sponsor of the Lebanese government after the First Lebanon War, made sure that Lebanon would not arrive at any sort of separate agreement with Israel independent of an Israeli-Syrian settlement.

The eighteen years between the IDF's entrance into Lebanon in 1982 and its final withdrawal in 2000 were marked by Hizbollah waging war on Israel (and during the first years after its establishment, also on the United States and other Western targets). In the course of this fighting, Hizbollah, supported by Iran and Syria, developed guerilla and terrorist tactics, first and foremost suicide bombing attacks, abductions, and the use of powerful explosive charges against IDF troops, which

were subsequently copied by Hamas and other Palestinian terrorist organizations.

The disengagement from the Gaza Strip was preceded by two extended terror campaigns that featured suicide bombers and a prominent role played by Hamas. In the 1990s the terror campaign was aimed at undermining the Oslo Accords, and during the so-called second intifada lethal suicide bombings were frequent and became the trademark of the campaign. The focal points for these campaigns were based primarily in Judea and Samaria rather than the Gaza Strip.

From the security perspective, there is an important difference between the IDF's withdrawal from Lebanon and the disengagement from the Gaza Strip: the IDF left the security zone in Lebanon at the height of difficult fighting and after having sustained a series of severe blows (including the death of Brig. Gen. Erez Gerstein, commander of the Liaison Unit to Lebanon, and the helicopter disaster). Prime Minister Ariel Sharon's announcement about the disengagement from the Gaza Strip (December 28, 2003) came at the height of the second intifada, as Israel was engaged in difficult warfare against Palestinian terrorism, but the implementation itself took place after the intifada had already declined (as a result of Operation Defensive Shield and the drop in suicide bombings, the death of Arafat, and Abu Mazen's election).

The unilateral withdrawals from Lebanon and the Gaza Strip were first and foremost the product of the determined decision and execution of one person − Prime Minister Ehud Barak in the case of Lebanon and Prime Minister Ariel Sharon in the case of the Gaza Strip. Beyond the centrality of these two figures in the decisions, the withdrawals were also expressions of the fatigue of Israeli society and politics with the bloodshed in Lebanon and the prolonged preoccupation with Palestinian terrorism. The two withdrawals were carried out on the assumption at the time that the advantages of withdrawing would outweigh the advantages of the status quo, whether in Lebanon or the Gaza Strip.

At the regional level, the background to the withdrawal from Lebanon was the failure to achieve a political agreement with Syria that would also have solved the Lebanese problem (failure of the Shepherdstown talks in January 2000). In the Palestinian case, the background for the disengagement was the despair of arriving at a settlement with the PA in light of the Palestinian terrorism campaign. Regarding the Israeli-

Lebanese issue, the political decision was preceded by social pressures from an extra-parliamentary movement that garnered a great deal of public support (the Four Mothers group, for example). There was no such parallel movement in the Palestinian context in general or the Gaza Strip context in particular.

Hizbollah and Hamas: Similarities and Differences

Hizbollah and Hamas are movements deeply entrenched in, respectively, Lebanese and Palestinian society. Both were established in the 1980s – the former during the First Lebanon War (1982) and the latter at the outbreak of the first intifada (1987). Both exploited the weakness of the central government (be it the Lebanese regime or the PA) and effectively filled the governmental and military vacuums left by Israel after the withdrawals from Lebanon and the Gaza Strip.

Hizbollah and Hamas are both movements with sharp anti-Israel and anti-West radical Islamic ideologies and both can be characterized as profoundly jihadist in nature. Hizbollah embraced an Iranian-style radical Shiite Islamic ideology; this element constituted a central role in the organization's establishment and continues to play a central role in its operation. Hamas, by contrast, is a radical Sunni Islamic movement with roots in the Muslim Brotherhood. Neither movement sprang out of thin air: Hizbollah was established in part as a result of longstanding religious and cultural links between the Shiite communities in Lebanon and Iran, which intensified after the fall of the shah in 1979. Hamas was established as an offshoot of the Muslim Brotherhood, which maintained an extensive social and religious infrastructure in the Gaza Strip and some centers of activity in Judea and Samaria (e.g., Hebron).

Several internal and regional circumstances contributed to the establishment and growth of Hizbollah and Hamas. The first was the waning of secular Arab nationalism, à la Nasser, and the rise of radical Islam, both in Lebanon and in the Palestinian Authority. The second was the success of the Islamic Revolution, which generated shockwaves throughout the region, and the rise of a radial Islamic regime in Iran that adopted a strategy of exporting the revolution (from the Iranian point of view, Lebanon was its most prominent success). Third was the civil war in Lebanon, which dealt a severe blow to the Christian community and the traditional Lebanese regime and increased the strength of the Shiite

community, which had traditionally suffered from political, economic, and social discrimination. Fourth was the eradication of the PLO-Fatah military infrastructure in Lebanon during the First Lebanon War, creating in Lebanon, especially in the south, a military and governmental vacuum filled by Hizbollah. A fifth element was Palestinian criticism of the corruption within Fatah and among its senior personnel who returned to Judea and Samaria after the Oslo Accords (a decade after their expulsion from Lebanon).

Hizbollah in Lebanon and Hamas in the Palestinian Authority presented new models of terrorist organizations, different from their classical predecessors. These organizations' terrorist activity represented only one of their fourfold foundations: the military-terrorist module, waging war on Israel in a variety of ways and means (from suicide bombing attacks to rocket fire at population centers); the political module, which prompted integration into the Lebanese and Palestinian regimes (while Hamas took over the Gaza Strip by force after the Israeli disengagement, Hizbollah in Lebanon has been careful to play by the rules); the social module, providing extensive social, religious, and educational services to the population, thereby filling the vacuum left by the state; and the media module, based on a media empire of TV, radio, internet, and newspapers, given the importance of winning the battle for the hearts and minds of the population.

To these one may add another unique dimension characterizing Hizbollah, namely the Shiite sectarian aspect, which has great significance in light of the sectarian nature of Lebanese society and politics. This is absent in Hamas, which operates within a much more homogeneous Sunni Muslim population.

The Role Played by Iran and Syria

Hizbollah is the handiwork of Iran and serves as a tool to promote Iran's strategic goals. The organization was established during the First Lebanon War (summer 1982) in the Beqaa Valley in Lebanon by the Iranian Revolutionary Guards, with Syrian encouragement and assistance. From the outset, it was possible to define Hizbollah as an Iranian project, undertaken in close coordination with Syria. While Hizbollah also wears a "Lebanese hat" and is integrated into Lebanese society and politics, it

is the "Iranian hat" that dominates and ultimately dictates its ideology, policies, and nature.

With the Hamas movement, the picture is somewhat more complex. The movement receives massive assistance from Iran, in terms of weapons, financing, and training. At the same time, however, there is a basic, inherent tension between Hamas and Iran, stemming from the conflict between radical Shiite Islam and Iran's ambitions for hegemony over the Middle East on the one hand, and Arabism and radical Sunni Islam, home to Hamas, on the other. Senior Hamas figures, led by Khaled Mashal, operate out of Damascus and from there steer the organization's terrorist and political activities, and Hamas depends heavily on Syrian political and military assistance.

Expectations were that the withdrawal from Lebanon would weaken Syria and ease the pressure it exerted via Hizbollah on Israel. In hindsight, it is clear that the withdrawal did in fact weaken Syria's status in Lebanon but strengthened that of Iran, both in Lebanon and in the Gaza Strip. At a later stage, after Syria overcame the difficulties created by the withdrawal of its army from Lebanon, it again became an important player in the Lebanese arena.

In retrospect, it is also clear that the withdrawals from the security zone in southern Lebanon and from the Gaza Strip amplified the importance of Hizbollah and Hamas in the eyes of Iran and Syria. The withdrawals increased the ability and motivation of those two states to use Hizbollah and Hamas as their proxies to exert pressure on Israel, not only through intermittent fighting with the IDF but also by threatening the civilians in Israel's home front by means of the rockets stockpiled with their support in Lebanon and the Gaza Strip. Beyond their routine use, these rockets are supposed to be activated against Israel on "the day of reckoning" in accordance with the regional strategic interests of Iran and Syria.

The Territory and the Population

In Lebanon and the Gaza Strip the IDF undertook full withdrawals, i.e., to the international border (which does not prevent Hamas and its supporters from claiming that the Gaza Strip is still occupied by Israel). In both cases, the step was taken unilaterally, without the agreement of the Lebanese government or the PA, as the assessment of the Israeli decision makers was that there was no realistic chance of achieving

such agreements. In both cases, the State of Israel rejected the option of retaining a "security zone." In Lebanon, the South Lebanon Army (SLA) had stopped existing and the IDF did not leave outposts of tactical importance in the security zone. In the Gaza Strip, no Israeli military positions or settlements were left. Even the Philadelphi Axis along the Egyptian-Israeli border, where presence is important for preventing arms smuggling into the Gaza Strip, was evacuated by the IDF.

Nonetheless, there is a basic difference between Lebanon and the Gaza Strip that has influenced the responses by the UN and the international community to the withdrawals: after the withdrawal from Lebanon, the IDF deployed on a recognized international border (along the Blue Line) with no loose ends (the issues of the village of Rajar and Shab'a Farms are unconnected to the Israeli-Lebanese border question; they are linked to the unmarked Lebanese-Syrian border). In the Palestinian arena, however, there was an expectation of further withdrawals in Judea and Samaria, in addition to the withdrawal from the northern part of Samaria that took place in conjunction with the disengagement from the Gaza Strip. However, given the problematic results of the two unilateral withdrawals and the lack of progress in the negotiations over the Israeli-Palestinian conflict, no further unilateral withdrawals occurred.

In addition, both withdrawals entailed difficulties and complications in that the areas were home to population groups that ultimately paid a steep price. In Lebanon there were no Israeli settlements, but the so-called security zone was inhabited by Christian, Shiite, and Druze populations, some of whom became SLA soldiers. They and their families, out of mutual interests that became evident during the Lebanese civil war, had fought alongside the IDF since 1976. As a result of the IDF's withdrawal from Lebanon, 6,800 people fled into Israel, most of them SLA soldiers and their families. Over time, some 4,000 of those who fled either returned to Lebanon or left for destinations abroad, while some 2,800 remained in Israel. In the Gaza Strip there was no local Palestinian militia such as the SLA, but there were some 8,600 Jewish settlers who found themselves uprooted from the villages where they had built their communities and homes.

Both population groups were particularly traumatized by the Israeli withdrawals, although the decisions were inevitable: it was impossible to maintain the SLA over the long term in the security zone or the Jewish

settlements in the Gaza Strip without the presence of the IDF. Similarly, the pictures of SLA refugees massing on the northern border crossing and the evacuation of the Jewish residents from the Gaza Strip were traumatic for Israeli society. The State of Israel invested massive resources to deal with these two groups, but the treatment has been ineffective for a number of reasons. In both cases, Israel failed to deal properly with those who paid the price, which should have been done without regard to one political orientation or another. Israel showed determination in implementing the military aspect of the withdrawal from Lebanon and carried it out successfully without casualties, but it did not employ the same determination and effectiveness in rehabilitating SLA refugees or those who were evacuated from the Gaza Strip settlements.

Post-Withdrawal Processes in Lebanon and the Gaza Strip

The withdrawals from Lebanon and the Gaza Strip were seen by the Lebanese, Palestinians, and the Arab world in general as evidence of Israeli weakness resulting from the pressures of terrorism and the weakened stamina of Israeli society. The events, therefore, had a negative impact on the image of Israel, the IDF, and Israeli society. The "spider web" metaphor coined by Hizbollah Secretary General Hassan Nasrallah in the May 26, 2000 speech in Bint Jbail was widely accepted in the Arab world for at least a few years (the Second Lebanon War and the end of the second intifada actually demonstrated Israel's stamina when it is pushed to the wall).

An analysis of the two arenas after the IDF withdrawals reveals certain negative developments and processes. While the withdrawals themselves did not cause them, they did contribute to their acceleration. The first process occurred at the political level. The political weight of Hizbollah and Hamas has grown in intra-Lebanese and intra-Palestinian politics and in the Arab world in general. Hizbollah has increased its representation in the Lebanese parliament and emerged as a terrorist organization enjoying political legitimacy and wielding a great deal of influence on government decisions. For its part, Hamas participated in the January 5, 2006 elections for the Palestinian Legislative Council (less than six months after the disengagement) and won by a landslide. By June 2007 it lost patience and took over the Gaza Strip by force, in what has been described by the PA as a military coup. This move de facto

created two separate Palestinian entities, one in the West Bank and the other in the Gaza Strip, and the political and social gaps between them grew steadily wider.

The second process entailed the construction of military infrastructures**:** the withdrawals from Lebanon and the Gaza Strip were exploited to build extensive military infrastructures with the support of Iran and Syria. Unprecedented amounts of weapons were smuggled from Iran and Syria into Lebanon and the Gaza Strip, reaching Hizbollah Hamas, and other terrorist organizations. Israel and the international community found this difficult to contain. The infrastructure that has been built includes the capabilities to launch rockets that threaten the heart of the State of Israel. Hizbollah has more than 40,000 rockets, while Hamas has several thousands at its disposal. While rocket fire was a part of life in northern Israel and the western Negev towns even before the unilateral withdrawals, there has been a significant change for the worse in terms of the quantity and quality of the rockets and other weapons at the disposal of Hizbollah and Hamas. Before Israel withdrew from Lebanon the rocket range encompassed Kiryat Shmona, Safed, Nahariya, and Sderot; today greater Tel Aviv is also within range – both from the north and from the south.

The third process is continued terrorist activity. Israel's declarations that after its unilateral withdrawals it would respond quickly and decisively to terrorist attacks did not stand the test of reality. Neither withdrawal ended terrorism, and Israel's "proportionate" responses in both arenas did nothing to restrain terrorist activity. On the contrary, they were often seen as reflections of weakness. Of particular importance was the abduction of three IDF soldiers at Mt. Dov in October 2000, some five months after the withdrawal, without any significant Israeli response (for reasons having to do with giving preference to the Palestinian arena, which was already engaged in a terrorist campaign, the second intifada). After the disengagement, there was a dramatic increase in Hamas rocket fire directed at Israel from the Gaza Strip, which did not incur severe repercussions until Operation Cast Lead. In the northern part of Samaria, the security situation improved after the withdrawal, though not necessarily as a result of evacuating the Jewish settlements there, rather because of the end of the second intifada, the construction

of the security fence, and preventive activity by Israel and the PA security services after Operation Defensive Shield.

The withdrawal from Lebanon did not itself prompt the outbreak of the second intifada some four months later. Rather, the second intifada was caused by a host of factors stemming from difficulties in the peace process, Arafat's personality, the growing strength of Palestinian terrorist organizations, and Israel's longstanding occupation of Palestinian areas. However, the image of the State of Israel and Israeli society as weak and willing to undertake unilateral withdrawals to international borders as the result of the pressure of terrorism (an image that during the second intifada proved incorrect) perhaps contributed to the Palestinians' decision to prefer terrorism over political negotiations.

Hizbollah and Hamas were naturally accorded credit for ejecting Israel from Lebanon and the Gaza Strip, as they ostensibly succeeded in causing the withdrawals by means of a terrorist and guerilla campaign ("the resistance"). Neither organization stopped its armed struggle against Israel after the withdrawals, though its nature changed: Hizbollah lowered its profile after the withdrawal from Lebanon, while Hamas raised it by exchanging suicide bombing attacks for rocket fire aimed at civilian centers in the western part of the Negev.

Two "corrective" wars – the Second Lebanon War some six years after the withdrawal from the security zone, and Operation Cast Lead some three and a half years after the disengagement – were needed for the State of Israel to be able to reap the (albeit imperfect) security benefits of the unilateral withdrawals. Herein, therefore, lies an additional important lesson: the need to back up Israeli withdrawals, especially if unilateral, with a big stick, including at times military moves, particularly if the other side persists in terrorist activity and, as was the case with Hamas, increases it.

Domestic and International Ramifications

The withdrawal from Lebanon won almost unanimous support within Israel, and a great sigh of relief accompanied the exit from the "Lebanese swamp." The difficulties of SLA soldiers and their families in resettling in Israel, the sporadic terrorist attacks that continued from the Lebanese border, and Hizbollah's accelerated military buildup all escaped exceptional social and political criticism by Israel, which was

preoccupied with a bloody confrontation with the Palestinians and aimed to contain Hizbollah attacks along the Lebanese border. It was only the Second Lebanon War that made people question the wisdom of the unilateral withdrawal in 2000. The disengagement was different. It caused a significant crisis within Israel and a crisis of trust between some segments of religious Zionists and the state, with wounds that to this day have remained open. The ineffective handling of rebuilding the life of those evacuated from the Gaza Strip only heightened the anger and frustration. This has implications for many areas, but that discussion lies beyond the scope of this essay.

One of the most important – albeit underplayed, if not outright ignored – differences between the withdrawals is that the withdrawal from Lebanon was accompanied by intensive political efforts that generated a supportive UN and international environment, whereas the withdrawal from the Gaza Strip lacked such efforts.

In the Lebanese arena, Israel managed to enlist support from the UN and the United States: leaving Lebanon occurred in the context of Security Council Resolution 425 (1978), preceded by dialogues with UN Secretary General Kofı Anan and the UN Secretariat. This dialogue produced the demarcation of the Blue Line (on the basis of the international border) by UN cartographers, and the UN formally confirmed that Israel had indeed withdrawn to the international line. Prior political dialogue also took place with the United States, which supported the withdrawal and lent it political backing.

By contrast, no similar process was undertaken on the eve of the disengagement from the Gaza Strip. In retrospect, this emerges as a serious mistake that lies at the core of the significant differences in the results of the two unilateral withdrawals: the international community recognized that Israel had abided by Security Council Resolution 425, and the efforts of the Lebanese government to challenge the demarcation of the Blue Line or the attempts by Hizbollah and the Lebanese to foment trouble over Shab'a Farms did not change the international community's support for the Israeli move. Moreover, the Second Lebanon War ended with Security Council Resolution 1701, which states that the Lebanese government must impose its authority and control over southern Lebanon and prohibits the presence of terrorists and weapons not under control of the Lebanese army. The resolution also reaffirms the Blue Line drawn by

the UN when the IDF withdrew from Lebanon. Resolution 1701 and the deterrence Israel achieved have contributed to the unprecedented calm on the Israeli-Lebanese border (although it is exploited by Hizbollah to accelerate its military buildup, including significant expansion of its rocket stockpiles, with Iranian and Syrian support).

By contrast, Operation Cast Lead ended without a Security Council resolution, and for good reason. The situation in the Gaza Strip differs from the one in Lebanon. To this day, political and legal arguments are made to the effect that Israel has not completely withdrawn from the Gaza Strip, as it controls the crossings, skies, and seas and continues therefore to be responsible for the population. Israel's attempts to shrug this off have not always been successful and have been rebuffed on the international arena.

As a result, the status of the State of Israel internationally is much more solid on the Lebanese question than it is on the Gaza Strip: the support of the international community has become an inseparable part of what constitutes Israel's deterrence capability in Lebanon, it backs up the unprecedented calm on the Israeli-Lebanese border, and allows Israel greater scope to act there. One could go further and say: it was no accident that no Goldstone-type report was composed after the Second Lebanon War and that no aid flotillas sail to help the Shiites of southern Lebanon; it is no accident that world public opinion does not support the conduct of Hizbollah in Lebanon. The way Israel left Lebanon had an important effect, and it is clear that the UN is an element that must be taken into consideration. The lesson is that in every military operation or military-political step such as a unilateral withdrawal, there is a greater need to take into account the stances of the UN, the international community, and world public opinion

Conclusion

The withdrawal from Lebanon and the disengagement from the Gaza Strip demonstrated that a unilateral withdrawal is not a magic formula for achieving what diplomats have failed to attain (peace agreements with Syria and Lebanon) or can attain (an agreement with the PA). Nonetheless, one cannot ignore the positive results that the unilateral withdrawals brought in their wake, especially in the Lebanese arena. Israel extricated itself from direct involvement in Lebanon, IDF losses

dropped, and the intensity of the fighting on the Israeli-Lebanese border abated (before the Second Lebanon War and more so afterwards). This allowed Israel to focus on the serious problems in the Palestinian arena and to avoid a comprehensive confrontation on both fronts.

The picture emerging from the comparison between the two withdrawals is complex and not unequivocal, and it is possible to point to advantages and disadvantages to the withdrawals in both arenas. However, from a strategic perspective one may conclude that Israel has not altogether left either the "Lebanese swamp" or the "Gaza swamp," because fundamental changes in Israel's relations with its neighbors cannot be attained by unilateral withdrawals but only by political agreements backed by the willingness to use military force when necessary, and by support of the international community. This is an important lesson and it behooves Israel to learn it well.

Basic Concepts in Cyber Warfare

Lior Tabansky

Introduction

Developments in computers have made possible far reaching changes in all areas of life, and the rapid progress in computing, communications, and software has led to a dramatic reduction in the cost of producing, processing, and disseminating information.[1] The scientific-technological developments of recent decades gave rise to "the information revolution," which involves the processing and dissemination of information. Information technologies continue to develop at an accelerated pace, and a new era has arisen in the information revolution.

The rapid growth in the fields of computing and communications and the ongoing improvement in the performance of computerized systems have created a new space in the world.[2] Cyberspace, a space created not in nature but by human beings, has the potential for tremendous benefits as well as unknown risks. Since it has existed for forty years at most, an understanding of the phenomenon is just beginning. The interface between a new topic that enables unprecedented capabilities, a technical field that demands professional understanding, and mass media that compete for the consumer creates − perhaps predictably − the potential for obfuscation.

National security has also been affected by the information revolution and the cyberspace phenomenon. In the national security context, the far reaching changes in information technology that have brought about a quantum leap in the availability and quality of intelligence, in the pace of information transfer, and in weapons precision[3] spawned the notion of a "Revolution in Military Affairs" in the 1990s. Smart use of new

Lior Tabansky is a Neubauer research associate working on the Cyber Warfare Program at INSS, which is supported by the Philadelphia-based Joseph and Jeanetter Neubauer Foundation.

technologies allows previously unknown capabilities, which together with new methods have generated a qualitative change in the military field. However, a public discussion on the issue of cyber security, as of other new hi-tech fields, is lacking in Israel.

This essay focuses on the question of national security in light of the cyberspace phenomenon. It aims to survey the field and create a common language for a fruitful public discussion of the developing issue of cyber security, proposing operative definitions for the issues that can be applied in a discussion of Israel's national security. The essay first addresses the properties of cyberspace, its inherent vulnerabilities, and possible threats within its realm, and then proceeds to related issues of defense, attack, and deterrence in cyberspace.

Cyberspace: Fundamentals and Properties

The term "cyberspace" − cyber(netics) + space − appeared for the first time in science fiction.[4] The word comes from the Greek *kybernetes*, which means one who steers or governs,[5] and its modern form appeared in a 1948 book by mathematician Norbert Wiener to describe the study of command and control and communications in the animal world or the mechanical world.[6] "Space" has many meanings in English, referring to philosophical, physical, mathematical, geographical, social, psychological, and other properties. One definition of space is "a boundless, three-dimensional extent in which objects and events occur and have relative position and direction."[7] This simple definition is sufficient for most of the daily experience of human beings, but it is not sufficient for the computerized world, which is inherently different from physical space.

Thus, use of the word "space" without precise delimitation is apt to lead to conceptual difficulties, as indeed occurs with "cyberspace." Moreover, the simple joining of two words does not provide an adequate understanding of the concept. Rather, the concept must be defined by addressing the intended use, in this case, with an understanding of the processes taking place in the computerized world and their interaction with issues of national security. In contrast to land, sea, air, space, or electromagnetic spectrum, cyberspace is not part of nature and would not exist without the information technologies that were developed in

past decades; cyberspace is much less concrete than natural spaces, and therefore this conceptual discussion is essential.

Cyberspace is composed of all the computerized networks in the world, as well as all end points that are connected to the networks and are controlled through commands that pass through these networks. By the end of the first decade of the twenty-first century, the public commercial internet became an integral part of daily lives.[8] In the first quarter of 2010, 2 billion people in the world were connected to the web, and the rate of internet penetration in developed countries is about 80 percent.[9] Access to the internet has moved quickly from stationary end points and fixed physical infrastructures to mobile devices and wireless infrastructure. The price for use continues to drop, and the web's dimensions and complexity are growing. A discussion of cyberspace developments tends to focus on the commercial internet.

However, the public internet is only part of cyberspace. That is, cyberspace includes the internet, but it also includes a range of other computer networks that are not accessible through the internet. Many networks have been designed and built in order to carry out defined tasks.[10] Some of the specific networks are built from the same building blocks as the public internet, but are separate from it, while others use completely different techniques from the internet. Cyberspace was formed by connecting computerized networks that communicate among themselves

Cyberspace can be described as composed of three layers.[11] The most concrete layer, the infrastructure of the cyber world, is the physical layer. Electrical energy, integrated circuits, processors, storage devices, communications infrastructures, copper cables, optical fibers, transmitters and receivers comprise the building blocks of this space.[12] These building blocks have natural properties of width, height, depth, mass, and volume. The second layer is software logic: a variety of systems of instructions for action and reaction that were programmed by human beings. The physical components are controlled largely by the various computer programs, and the stored information in computers is subjected to processing through software instructions. Most of cyberspace today uses standard hardware and software. The third layer of cyberspace is the layer of data that the machine contains and that creates information.

This is the least concrete layer of the three, mainly because information properties are very different from the properties of physical objects.

Much of cyberspace is organized and managed by private and cooperative organizations without state or geographical overlap. The internet, which is a central and growing component in this space, is built in a decentralized manner. The ideology of the internet's creators and its leading thinkers is opposed to any type of state management.[13] Moreover, the continuing development of information technologies enables new applications that take advantage of the internet's open infrastructure. Thus, for example, it is possible to transfer non-text content (picture, voice, and video) over the internet's infrastructure, and wireless communications and the reduction in the price of processing power allow internet connectivity for many devices that were not computerized such as industrial machines and technological accessories.

Given these structural and organizational properties, cyberspace has a high level of complexity and it is subject to frequent changes. Significantly, these properties accumulated empirically; the organizational properties in particular reflect the existing situation, but it does not necessarily follow that a priori these properties are an essential, inherent part of cyberspace.[14] Therefore, these properties will not appear in the definition of the field. However, the goal of this essay is to contribute to the public discussion of Israel's national security issues in cyberspace, and the working definition must faithfully reflect the existing situation in order to be applicable.

On this basis, what follows is an operative working definition of "cyberspace": inter-connected networks of information technology infrastructures, including the internet, telecommunication networks, mission-specific networks, computers, and computer embedded systems. The virtual environment − data stored and information processed by computers and transferred over these networks − is also included.[15]

Cyberspace and National Security

Security is one of the fundamental needs of human beings, societies, and states, and a significant portion of human endeavors in all natural spaces (land, sea, air, space, electromagnetic spectrum) stems from security issues. Yet historical experience, together with philosophy, has shown that scientific development has not changed human nature enough to

eradicate conflicts between human beings and among societies.[16] Thus cyberspace, which is man made, will also be exploited by human beings for their purposes; in this space too, there will be fights and conflicts. However, the nature of cyberspace is such that fundamental familiar security-related concepts such as violence, identity, location, defense, attack, and speed do not necessarily describe events correctly. Rather, the properties particular to cyberspace require specific professional treatment of security as it pertains to the cyber realm.

The United States began to address cyberspace in the context of national security as early as 1996.[17] American attention to the issue of security in cyberspace has been increasing, and as expressed by President Obama, "It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country."[18]

The American investment in this area is not limited to the declaratory level, but is backed up by significant financial and organizational resources. Government agencies, the military, industry, and academic institutions lead the work in this field, and publish numerous research and position papers. A full discussion of the American approach to the issue is beyond the scope of this article; suffice it here to mention that this issue attracts a great deal of interest among a wide range of circles. Similarly, although cyberspace is a young field, its potential for impact has not escaped the notice of those involved in national security all over the world, even if practices and details are shrouded in obscurity and a veil of secrecy in most countries.

What follows is an explanation of some of the basic concepts in the field of cyber security, to allow a common language when discussing cyberspace and Israeli national security.

Weaponry

Cyberspace is dependent on physical infrastructures, which include computers, sources of electricity, communications cables, antennae, and satellites. It is clear that kinetic damage to the physical infrastructure will harm cyber capabilities, but there is a difference between traditional kinetic weapons, even if they are aimed at a cyber target, and the new phenomenon of cyber weapons.

Cyber weapons are composed mainly of software, though at times hardware as well. They can be divided into three groups:

a. Unequivocally offensive weapons: different types of malware (viruses, worms, Trojan horses, logic bombs, and the like); denial of service actions.
b. Dual use tools: network monitoring; vulnerability scanning; penetration testing; encryption; and camouflage of content and communications.
c. Unequivocally defensive tools: firewall, disaster recovery systems.

Vulnerabilities

Vulnerability refers to weak points that are built-in properties of a defined system. In risk analysis, vulnerability is part of the risk equation: risk is a product of vulnerability, threat, and probability. Table 1 charts the weak points in cyberspace in light of the properties reviewed above.

Table 1. Cyberspace Properties and Vulnerabilities

Property	Vulnerability
Rapid pace of change	Rapid obsolescence of means, including defensive systems.
Rapid reduction in price	Low entry threshold leads to a multiplicity of significant players.
Structure of TCP/IP protocol	Difficulty identifying the source of the signal that arrives via the network.
Wide scale use of standard, commercial off the shelf equipment	Narrowing of the gaps in capabilities among various players; vulnerability of hardware and identical operating systems endanger a wide range of systems.
High level of complexity	It is difficult to differentiate between a glitch and an attack. It is very difficult to determine cause and effect.
Asymmetry	No great investment is needed to develop and operate the weapons. Defense against cyber threats must include all channels of attack and be updated frequently, at progressively high costs.
Vague laws	There is no common definition of "cyber warfare" in the world; significant legal differences between various countries concerning cyber crime.

Defense

Defense from a cyber threat is derived from its broad common denominator, which is unauthorized access to a computer system. Therefore, defense is focused on using technological methods to identify an unauthorized intrusion, locate the source of the problem, assess the damage, prevent the spread of the damage within the network, and to the extent necessary, reconstruct the data and the computers that were damaged. Defense involves the ability to be positioned in the path of penetration, identify such an attempt, and foil it through preemption. For this purpose, computer systems are used to monitor activities and communications; block access routes; limit permissions; verify identity; provide encryption, and enable backup and disaster recovery.

While this appears to be a proper logical response to the threat, cyber-defense is necessarily limited. The volume of activity alone places the defending party in an inferior position. The decentralization of computer resources and networks complicates the attempt to define the areas of responsibility. The situation in compartmentalized networks is simpler: the compartmentalized body knows that the network is under its control and that it must maintain and defend it. (This is one of the reasons that this article does not address the subject of military networks and electronic warfare.) However, networks of this type are diminishing, and an increasing number of industrial systems exploit the advantages of IT and thereby become prone to risks of cyberspace. Critical infrastructures have been brought into cyberspace, and the security forces use commercial infrastructures for most of their communications, so that the burden of passive defense is growing.

Attack

A cyber attack does not include kinetic damage to cyberspace's physical infrastructure. An attack in cyberspace uses cyber tools, and its weapons are software and hardware. Again, the very identification of an attack is not simple. The symptoms of glitches and the possible results of an unauthorized intrusion into computer resources are often identical. Even identifying an intrusion and ruling out the possibility of a technical glitch is not sufficient. Such an intrusion is used for the entire spectrum of cyber threats, and when an unauthorized approach to a computer resource occurs, it can be used for all kinds of activities, and it is very difficult to

determine the identity of the intruder and his motives. The properties of cyberspace today lend a clear advantage to attack over defense.[19]

Cyber War

Wars have been a part of human experience since the dawn of history. Cumulative experience of destruction has brought about a series of understandings intended to reduce the horrors of war: establishment of international institutions; creation of various international treaties that govern the boundaries of what is permitted in war; the establishment of humanitarian aid organizations; and a judicial system against war criminals. Because of the newness of cyberspace and its lack of correspondence to the fundamental concepts of the physical world, no definition of the concept of cyber war has been formulated. In Israel, discussions on the issue of war in the information age, computer warfare, and information warfare have been underway for at least a decade.[20]

Hostile activity in cyberspace can be ranked according to types of activity undertaken and damage caused. What follows is a proposed classification, arranged in descending order of severity.

a. An attack on various civilian targets that causes physical damage.
b. Disruption of and attack on critical national information infrastructures, which causes physical damage.
c. Disruption of and attack on military targets in the state's sovereign territory.
d. Disruption of and attack on military targets outside the state's sovereign territory.
e. Insertion of dormant attack tools, e.g., a Trojan horse or logic bomb that are likely to be preparations for an attack.
f. Criminal activity, industrial espionage.
g. Use of dual use weapons: intelligence gathering, probing for common security vulnerabilities, penetration tests.
h. Conducting a propaganda media campaign, abuse and defacement of official websites.

The difficulty in discussing cyber war derives from the non-trivial nature of the concepts of attack, defense, and violence in cyberspace. In order to determine that a cyber attack is part of a war, several properties must be examined:

a. Organizational source and geographic origin: is a nation state behind the action?[21]
b. Results: could the attack have caused damage, and did it in fact cause damage and casualties?
c. Level of complexity: did the attack require complex planning and coordinated resources that are available mainly to states?

In light of the properties of cyberspace today, it is very difficult to answer these questions, let alone answer them in a manner sufficient for designing public policy.

Deterrence

Advanced research on the subject of deterrence occupies researchers in political science, security studies, game theory, economics, and psychology. Thus far, the world has succeeded in coping with nuclear weapons that are capable of destroying the earth through deterrence based on assured retaliation.

However, the Cold War model of nuclear deterrence is utterly impracticable in the cyber battlefield, especially given the structure of cyberspace today, which makes it impossible to identify an attack with certainty and makes it impossible to pinpoint quickly the source and identity of the attacker.[22] Deterrence based on exacting a heavy price from the attacker is practically impossible; thus any deterrence in cyberspace today must be based on preventing the attacker from scoring an achievement. It is essential to invest in focused research on the subject of deterrence in order to reduce the threats to national security.[23]

Cyber Threats

Many actors with threat potential operate in cyberspace, including:

a. Hacktivists: individuals attacking websites in order to implant a political message, or acting to break censorship mechanisms and expose secrets.
b. Hackers: individuals who break into a computer system remotely through a communications network.
c. Writers of malware; spammers; collectors of personal user data.
d. Botnet herders: individuals who break into computers remotely through a communications network, but obtain partial control over many other computers in order to turn them, without their

knowledge, into a means of carrying out a future task. In recent years, there has been a fertile market in capabilities to attack networks, numbering tens of thousands to millions of computers.

e. Organized crime organizations use hackers, mainly botnet herders, for purposes of profit: identity theft, fraud, spam, pornography, camouflaging of criminal activity, money laundering, and so on.
f. Employees belonging to inner circles of a closed organization: an insider threat. Computer networks of compartmentalized organizations are separated from the general network in order to make break-ins difficult. In such a situation, recruiting an embittered employee is a good way to infiltrate a compartmentalized network. A hacker who confronts technical obstacles may exploit innocent workers in the target organization through social engineering.
g. The security services adopt cyberspace tools to achieve their goal; information technologies provide spies a wide range of ways and means to carry out their tasks.
h. Terrorists and radicals also take advantage of cyberspace to convey encrypted messages, recruit supporters, acquire targets, gather intelligence, camouflage activity, and so on.

There is no technical measurement to assess how critical a computer system is that it can exist on a national level isolated from the social values, goals, and forces that use it. Therefore, the relative importance of a computer system, and as a result, the amount of public investment required to defend it, are subject to a public discussion and a political fight. Critical infrastructures (manufacture and supply of energy and food, land and air transportation, water and sewage, communications systems, and the like) existed in developed societies before the appearance of the computer. Why do they receive attention in the discussion of the new phenomenon of cyberspace? After all, these infrastructures were essential to states even before computers appeared, and were mainly used for strategic goals in international conflicts. The current attention is a function of two factors.

First, when computers and communications penetrated into every aspect of life, cyberspace itself became essential to the full functioning of developed states. Cyberspace is like the body's nervous system. Therefore, it has become essential to secure normal, undisturbed action

in cyberspace, and to provide all strata of the populace with the ability to access it.[24]

Second, with the development of computing, computers were integrated into the existing production, command, and control systems of the traditional industries. The cyber layer, with its high level of complexity, was added to the already complex engineering systems. In fact, the old infrastructures were placed in cyberspace,[25] thereby making them vulnerable to the weaknesses of cyberspace. For the first time, potential arose to reach protected targets through the dimension of communications and software that does not depend on defense in physical space. Once essential infrastructures function at least in part in cyberspace, potential exists to directly harm essential state targets by exploiting their cyberspace vulnerabilities. The major threat is damage to the physical functioning of the essential infrastructures through cyber means, while bypassing the traditional military defense systems that guard the physical space, conceal the attacker's identity, and ultimately avoid a response and armed conflict.

A threat is made possible by exploitation of a vulnerability, and it is intended to disrupt a system or to harm the enemy's assets. There are threats to cyberspace (risks *to* cyberspace), which are intended to harm the cyber infrastructure, and threats that use cyberspace but do not harm it (risks *through* cyberspace).[26]

Defense against the first type of threat is called critical information infrastructure protection. A critical information infrastructure is a system with a computer dimension that controls the functioning of another physical system that is essential to the functioning of the economy and to state security. Defending such infrastructures is emerging as a major layer in the discussion of the security implications of cyberspace.

The second type of threat (risks *through* cyberspace) includes a range of actions made possible by cyberspace, including: encrypted communications for political opposition, instructions for terrorist activity, or international crime; traditional crime (fraud, theft, pedophilia) that is intensified by computer networks; new crime that is unique to cyberspace; computerized espionage; an attack on the provision of network services; and use of malware for a variety of purposes.

Threats can also be distinguished based on their geographic source: outside the country's borders or within, outside the computer network or

within. The current structure of the internet communications protocol and the open architecture of the web, together with inherent vulnerabilities of software and hardware, make it almost impossible to locate the geographic source. In general, the path of data packets that move through the network is not fixed; the stations along the way are not required to examine the content of the data or their source, and are not required to document the path of the data packets. However, this is not a necessary property of cyberspace; rather, it is the result of a policy that encourages openness in access to information and free communications. This policy is rooted in the liberal ideology of the American pioneers of the web. With the privatization and commercialization of the information industries, the free market ideology, which recoils from any state intervention, also makes it more difficult to have a discussion about a different technical and legal organization of cyberspace.

Threats can also be distinguished based on the goal of the threat: crime, terrorism, industrial espionage, military espionage, cyber warfare. Such a classification ignores the fact that an identical method of operation can be used for many purposes. In addition, this classification is problematic in light of the great difficulty in tracing the source of the electronic signal moving through cyberspace and the identity of those who sent it.

Assessing the Cyber Threat

Unauthorized access to computer information resources is common to every kind of cyber threat. However, the unauthorized intrusion into a computer information resource opens a broad spectrum of possible results. What is the extent of the threat from the various actors? Are all the actors and the threats relevant to national security? How can we assess their importance and prioritize the response policy? A public discussion is needed in order to provide a serious answer to these questions.

Risk assessment is a wide and varied field used in various professions, and a professional discussion of it is beyond the scope of this article. For the purposes of the discussion, we will define threat assessment as the product of the probability of the event's occurrence and the assessment of the damage caused by the event.

In order to formulate policy, we need to assess the threat, i.e., the scenario that makes a policy necessary. However, it is not possible to make an assessment that is unequivocal, precise, and objective, because

Table 2. Characteristics of Cyber Threats

Type of Threat	Newness Level	Probability	Threat Effect
Harm to security forces' ability to function	Medium (relatively old threat)	Rising (widespread technological possibilities)	Intensified
Security espionage	Medium (relatively old threat)	Reasonable (widespread technological possibilities)	Intensified
Industrial, financial, information espionage	Medium (relatively old threat)	Rising (widespread technological possibilities)	Intensified (newness has great importance)
Direct harm to essential state services	*New* (not possible previously)	*Rising* (new technological possibilities)	*Highly intensified*
Full scale cyber war	New (not possible previously)	Low (cost/ benefit vs. kinetic war)	Medium

threat assessment on a national level requires that the social and cultural values of the country and the society be addressed. These values guide the relative importance of scenarios and potential threats to society. Such an assessment is a subjective one, but this is the most appropriate way to conduct a policymaking process. In a democratic state, the representative institutions and the media serve as a channel for the public to make itself heard and influence national security, wellbeing, and other issues. Regarding national cyber security, technical experts do not have a monopoly on assessing scenarios and making policy. Just as economists should not be allowed to determine the state budget by themselves, cyber security should not be entrusted to computer experts.

An approach to cyber warfare resembles an approach to any new weapon system. In order to assess the relative weight of the cyber threat in the framework of war, familiar variables such as effective range, extent of destruction by the attack, cost of use, political limitations on use, and others must be examined.

The cyber threat has the potential to be realized independently of the traditional security system. Cyberspace as it exists today is a wild battlefield. It makes possible direct transfer of data and commands while disregarding national and geographic borders and defensive arrays. As opposed to space, air, land, or sea, existing security organizations are only starting to function in cyberspace. There is a critical potential in cyberspace to undermine national security while bypassing traditional national defense frameworks and directly hitting critical targets on the home front. Thus, the developing phenomenon of cyberspace is creating a strategic change in the field of national security.

Table 2 is a proposed schematic summary of the types of cyber threats vis-à-vis their newness, probability of occurrence, and threat effect.

Conclusion: Strategic Properties of National Security in Cyberspace

The article is intended to conceptualize the developing field of cyber security and to create a common language for a public discussion. In light of the lack of conceptual clarity regarding cyber security, the article proposes explanations and operative definitions for these new topics. It reviews the properties of cyberspace and the existing weak points and threats, and presents problems of defense, attack, and deterrence in cyberspace.

Given the properties of cyberspace today, cyber warfare makes it possible to attack remotely tactical and strategic targets with little risk to the attacker. This limited risk is a function of: the difficulty in distinguishing between a glitch and an attack; the difficulty in connecting an event with a result; the difficulty in tracking the source of the attack and identifying the attacker; widespread use of inexpensive, off the shelf technologies; and the many vulnerabilities of a computer system. The cyber threat is asymmetric: no great investment is required for developing and using the weapons. In contrast, defense against cyber threats must encompass all channels of attack and keep up to date with new developments, and the cost of defense continues to grow.[27]

Do the cyber threats reviewed here threaten the national security of the State of Israel? A significant portion of the answer is derived from the concept of the role of the institution of the state and is beyond the scope of this article, which is not intended to provide an authoritative answer to the troubling questions that arise with the development of cyberspace. In

an open, democratic state, the answers to questions of this type emerge through public debate and political process. The article is intended to contribute to an informed public discussion in Israel, and to focus the attention of the political system on new issues in national security.

The state has responsibility for national security, even when the playing field is developing and changing in form. The information age is causing far reaching changes in national security. Any computer network is exposed to an attack. There is no system that is immune from an attack or a glitch, and it is important to recognize this in order to free ourselves from the futile aspiration for total security. Nevertheless, it is necessary to aspire to optimal security while adapting to the nature of the threat and the target. An answer to the cyber security threat will be adapted to its special characteristics. To formulate a policy that suits the needs of the state, a public discussion and professional research are needed. Scientific and organizational work methods should be harnessed in order to provide security in the information age.

Notes

1 There was a reduction in price of at least three orders of magnitude between the early 1970s and the middle of the first decade of the 21st century. A gigaflop cost $15 million in 1984 and $.14 in 2009. Regarding storage capacity on magnetic media, the price per gigabyte in 1993 was $1000; the price per gigabyte in 2009 was $.02.

2 Since the dawn of history, human beings have aspired to survive and develop in the physical spaces surrounding them, first of all in the immediate physical space, the near environment: from animal domestication and agriculture and building, and extending to control and processing of raw materials using mechanical, chemical, and other methods. Since the scientific revolution, developed societies have learned to maneuver and sometimes even control their environment with the aid of the scientific method. The land space has naturally attracted most of the efforts. The maritime space was conquered by different civilizations throughout history, and states that succeeded in controlling the maritime space first enjoyed long term wellbeing. The aerial space was conquered in the last one hundred years, and there too those who were in control had a major relative advantage over their competitors. Since the 1950s and the launch of the first satellite in 1957, there has been competition between the superpowers over the means of reaching and staying in space, and over nearby planets. Progress in this field gained momentum as a result of the appearance of computing and electronics. Cyberspace is a new phenomenon. See Isaac

Ben-Israel, "From the Sword's Blade to Computer Memory," *Odyssey* 9 (October 2010).

3 For a discussion of the information technology revolution in military affairs (IT RMA), see Michael E. O'Hanlon, *Technological Change and the Future of Warfare* (Washington, D.C.: Brookings Institution Press, 2000); Stuart E. Johnson and Martin C. Libicki, *Dominant Battlespace Knowledge: The Winning Edge* (Washington, D.C.: National Defense University Press, 1995); Isaac Ben-Israel, "Security, Technology, and the Future Battlefield," in Haggai Golan, ed., *The Texture of Security* (Tel Aviv: Maarachot, 2001), pp. 269-327.

4 Andrew M. Colman, *A Dictionary of Psychology* (Oxford University Press, 2009), "cyberspace *n*." *Oxford Reference Online*, Oxford University Press, http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t87.e2037.

5 Julia Cresswell, *Oxford Dictionary of Word Origins*, "cybernetics." *Oxford Reference Online*, Oxford University Press, http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t292.e1374. The Hebrew word *kvarnit* [captain, leader] also derives from the Greek *kybernetes*.

6 Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine* (New York: John Wiley and Sons, 1955).

7 *Encyclopædia Britannica*, 2010, "space," *Encyclopædia Britannica Online*, http://www.britannica.com/EBchecked/topic/557313/space.

8 The internet is an open network of end points, devices, and computer networks that communicate with each other using the TCP or IP communications protocol. It is built in an open, decentralized manner, and from any end point in it it is possible to communicate with any other end point. Countless applications have been created on top of this basic design, and among them are those that are intended to limit access, verify identify, encrypt information transferred over the web, verify receipt of information, and so on.

9 "World Internet Usage Statistics News and World Population Stats."

10 For example, GPS, ACARS, SWIFT, GSM Cellular, and thousands of other mission-specific computer networks.

11 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009).

12 Electronics is the infrastructure of the computer world today. However, before electronics, computers were mechanical, and electronics is not immune to the future: the possibility of exploiting a biological infrastructure for computer purposes has already been proven. The computerization of DNA uses molecular biology and DNA instead of electronic components. Another possibility is the computerization of peptides: bio-molecular computerization, which is based on compounds made of at least two amino acids.

13 The pioneers, such as Reinhold or Barlow, saw the internet as being an open system, not hierarchical, and also anti-establishment. They hoped it would

allow a collaborative and egalitarian community and organization. See John Perry Barlow, "A Declaration of the Independence of Cyberspace." Lawrence Lessig describes the internet's principle of action: "Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end. This minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about optimal network design." Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999). However, the reality is more complicated. For a discussion of the control structure of the internet, see Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

14 Induction (drawing conclusions from the specific to the general) is a very widespread tool, but it has a built-in limitation of logic: a view of an event and its recurrence does not offer a valid logical inference that this event is unavoidable. The problem of induction is that an inference from the specific to the general does not necessarily have validity.

15 The definition proposed here intentionally resembles the definitions appearing in official documents of the various arms of the United States government. The United States and Israel share significant values and have similar scientific and economic levels, and therefore they see and interpret the situation with similar tools. The United States leads the scientific-technological research and development in the world, and at the same time, it leads policy on cyber topics. A comparative study that includes countries like China, Russia, India, France, and others will identify very different definitions. However, this research is beyond the scope of this article.

16 Thucydides, *The Peloponnesian War*. The realistic theory of international relations enlists the history of ancient Greece to understand fixed human nature and international anarchy, which guide current events: Steven Forde, "International Realism and the Science of Politics: Thucydides, Machiavelli, and Neorealism," *International Studies Quarterly* 39, no. 2 (1995), and Azar Gat, *War in Human Civilization* (Oxford and New York: Oxford University Press, 2006).

17 The Presidential Critical Infrastructure Board was established in 1996.

18 Barack Obama, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

19 William Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (2010).

20 Isaac Ben-Israel, "Information Warfare," *Maarachot* 369 (February 2000): 18-25.

21 Following the terrorist attacks of September 11, 2001, the threshold for state support was lowered: it was enough that there be circumstantial evidence, such as ideological support of the enemy or provision of logistical services to terrorists, to be held accountable.

22 Lynn, "Defending a New Domain."

23 Libicki, *Cyberdeterrence and Cyberwar*.

24 In France, Finland, Estonia, and Greece various government institutions have recognized the right to internet access as a basic right.

25 This should be regarded as an expected phenomenon: the exponential development of information technologies is liable to fundamentally change existing fields of practice. As futurist and entrepreneur Ray Kurzweil writes, in this way the paradigm of biological research changed from traditional experiments to computation and simulation.

26 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010).

27 The argument about the difficulty of protection is similar to the argument against active anti-missile defense and today's argument about the Iron Dome system. It is also similar to the argument about the futility of defense against suicide bombers. Nonetheless, with the aid of the scientific method it is possible to create an answer to the new threats. See Lior Tabansky, *The Anti-Terrorism Struggle in the Information Age: Palestinian Suicide Bombers and the Implementation of High Technologies in Israel's Response, 2000-2005*, position paper published by Tel Aviv University, May 2007.

Protecting Critical Assets and Infrastructures from Cyber Attacks

Gabi Siboni

The impact of computer and communications systems in recent decades has not bypassed the national security of states in general, and the State of Israel in particular. Most systems in developed societies rely on computer and information infrastructures, and this growing dependence on information and communication technologies means that a blow to computers and information flow processes is liable to disrupt, paralyze, and sometimes even cause substantive physical damage to essential systems. Computer-based capabilities and their near-global ubiquity expose states to harm in cyberspace by various elements, including hostile countries, terrorist organizations, criminal elements, and even individuals driven by personal challenges or anarchist motives. The threat is particularly acute as management, control, and monitoring systems can be disrupted through changes to a computer program, and no physical attack is needed. Thus, it stands to reason that the face of future conflicts will be transformed beyond recognition.

The strength of a sovereign state is a function of economic, societal, and scientific strength combined with military strength, and the purpose of the military strength is to protect the state's territory and its citizens so that they can cultivate and maintain economic strength. The vulnerability of computers and communications systems to cyber attacks entails a dramatic change in the concept of military strength. For the first time, it is possible to mortally wound national economic strength by paralyzing economic and civilian systems without using firepower and force maneuvers. Thus, the ability of states to operate in cyberspace for

Dr. Col. (ret.) Gabi Siboni is head of the Military and Strategic Affairs Program at INSS and head of the Cyber Warfare Program at INSS, supported by the Philadelphia-based Joseph and Jeanetter Neubauer Foundation.

both defensive and offensive purposes coincides with classic military capabilities to play a significant role.

In the past two decades, states, along with their progress, profitability, and wellbeing – and their production and provision of national services in particular – have been exposed to new threats, yet insufficient attention has been paid to the appropriate means of confronting such threats. In the recent past, industry (private and public) was protected by the state. For example, excluding workplace accidents, power stations producing electricity, whether in private hands or publicly owned, were exposed to physical damage only if the state encountered a physical war, and it was the state's job to protect such infrastructures along with economic institutions, industrial facilities, and so forth. Public institutions were protected by the state by virtue of their existence in the territorial space under its authority and control. That has changed. In addition, the trend in recent decades to privatization has placed a large portion of the infrastructure plants that were traditionally in the hands of the government in private hands, including those relating to communications, transportation, electricity, energy, and heavy industry. Moreover, traditional industries have in recent decades been joined by new industries in the hi-tech realm that constitute a significant component of states' GDP.

Due to the universal understanding that "he who defends everything defends nothing,"[1] various countries have developed ways of protecting infrastructures and systems that are critical to their functioning. In 2002, the State of Israel established the Information Security Authority, "in charge of professional direction of the bodies for which it is responsible regarding securing essential computer infrastructures from the threats of terrorism and sabotage to the security of classified information, and from the threats of espionage and exposure."[2] In this context, a steering committee was established in the National Security Council whose role is to examine the risks in information security. It was also decided that the rules of the steering committee would apply to a number of bodies and institutions whose information systems are defined as critical, including the electric company, banks, government offices, and the like, and the committee is authorized to add to this list.[3]

The public service bodies that are required to protect themselves from a cyber attack have been under the direction of the Information Security

Authority for quite a while. At the same time, changes in the structure of the Israeli economy and the emergence of elements, processes, assets, and projects – which if damaged could potentially cause significant harm on a national level – have exposed and increased the range of weak points and the targets for cyber attacks. Moreover, potential damage is not restricted to what can be quantified in financial terms or what impacts on the GDP: significant damage can also be caused to assets and values that have Israeli and Jewish national importance. Thus, for example, in the United States, defensive plans also apply to heritage and memorial sites.[4]

Consequently, it is highly important to be able to examine which additional entities require guidance by the Information Security Authority. This article proposes an approach that will make it possible to implement a systematic process using existing statutory tools, in order to identify other bodies (mainly from the private sector) whose damage might impact on national security, and therefore requires them to operate appropriate defensive mechanisms for their critical assets and infrastructures.

What Should be Protected?

In a US Department of Homeland Security document,[5] Patrick Beggs[6] reviews how authorized officials in the United States see the interface between defense-critical infrastructures and resources and their physical and cyber infrastructures.

In the United States, the mapping of defense-critical infrastructures covers water, energy, communications, transportation, the chemical industry, agriculture and the food industry, information systems, banking, commercial and financial services, health services, and finally, areas of importance to the American collective memory (national monuments, heritage sites, and so on). These sectors are grounded on two basic infrastructure components: the first regards physical infrastructure components, such as power stations, dams, airports and sea ports, roads, railroads tracks, various types of delivery infrastructures,[7] hospitals, factories, and the like. The second component concerns cyber infrastructures, including software and hardware systems, internet servers, command and control systems, and information systems.

In order to enable an appropriate basis for formulating defense plans, the US uses a methodology called Cyber Resiliency Review (CRR)

of institutions and critical infrastructures that belong to the sectors described above. This approach makes it possible to assess a number of aspects, including the definition of defense-critical assets, management of communications, continuity of services, technological management, dependence on external components, management of unforeseen incidents and accidents, ability to assess the situation, and identification and management of weak points. From this review, decision makers can formulate a plan of action to improve the cyber resiliency of the organization.

The process is organized and well ordered once the organization or body is identified for review through this methodology. However, lacking is an effective way to identify these bodies and organizations. The situation in Israel is fairly similar. From time to time, the Information Security Authority brings additional bodies to the steering committee of the National Security Council that will need to examine and meet the agreed upon guidelines. At the same time, there is no binding systematic statutory process that allows these organizations to be identified.

Because an area or a sector that constitutes a critical national infrastructure comprises a large number (hundreds, and sometimes thousands) of organizations and systems, protecting a "sector" is meaningless. Rather, in practice, protection entails actions taken by specific organizations, companies, facilities, and processes. Therefore, the question is how is it possible to locate these bodies, since almost every company or government office interfaces with sectors that are defined as defense-critical infrastructures. For example, protection of water supply and water quality infrastructures in Israel does not only affect processes in Mekorot, Israel's national water company, but also dozens of other water suppliers, associations, water corporations, desalination and delivery facilities, sewage and wastewater treatment facilities, and so forth. A large number of these facilities are operated by private entrepreneurs who do not see activating protective mechanisms as a top priority. The situation is similar in other industries.

Furthermore, in many cases it is also necessary to protect interfacing systems that are connected to the supervised bodies. For example: an industrial factory that has been declared an essential component of a particular sector works under the direction of the Information Security Authority. Sometimes this factory is dependent for its operations on

other manufacturers (smaller satellite manufacturers) that supply input (sometimes critical) for the production process of this protected factory. In many cases, some of these satellite manufacturers are not included in the group of critical infrastructures for protection and therefore they do not use satisfactory information defense processes. Thus, it is possible that cyber damage to one of these manufacturers will cause significant damage to a protected factory.

The use of information technologies in Israel is widespread, both in the public and the private sectors. As such, Israel offers a wide range of targets for a potential cyber attack. Therefore, identifying additional bodies for guidance by the Information Security Authority is an essential task for building an optimal defense system. Reviews taken from time to time and information from various government offices are essential to this process, but they are not sufficient. A built-in mechanism must be created that will allow a significant improvement in these processes, especially concerning certain projects in the private sector that if exposed to cyber damage could suffer extensive damage that might have an impact on national security.

The Proposed Process: Use of Existing Statutory Tools

The principal proposal aims to make cyber protection a built-in component of the existing statutory process, both in the establishment stages (i.e., the approval of the projects in the various planning commissions) and in the operational process (the business licensing law). It is proposed that in the framework of the national planning processes, every project submitted to the planning commissions for approval will be required to submit a Cyber Resiliency Assessment. This assessment will constitute the main statutory tool for examining the project's exposure to the possibility of cyber attacks and the measures protecting against these exposures. This assessment will also provide the Information Security Authority a tool for identifying and managing the critical infrastructures for defense. At the same time, in the framework of the business license, which is a license requiring periodic renewal, the relevant authority can check the ongoing compliance with cyber protection instructions of the body under review.

The establishment of every project in Israel, including national infrastructure projects, requires compliance with the customary processes of statutory planning. Thus, projects that are required to

build facilities and structures must be approved by various planning commissions in accordance with the relevant regulations on the local, regional, and national levels. Review of the planning documents submitted for approval is the planning authorities' central tool of control over these projects. Among the documents submitted for review by the planning commissions today are reports concerning firefighting, public health issues, environmental aspects, handling of hazardous materials, home front defense, and so forth. These documents define the steps that the project initiator will take in order to comply with the necessary requirements in each of the areas described above. These steps are then relayed to the authorized regulatory authorities, which employ experts to ensure that at the end of the process, the project is implemented with public interests in mind and that public security is maintained throughout the various spheres. In Israel, dozens of projects that if damaged might harm national security are discussed every year, including infrastructure facilities, water and sewage treatment facilities, delivery systems, transportation projects, energy facilities, and communications. Expansion and establishment of industrial factories and a wide range of other projects are discussed as well. Cyber damage to some of the projects and ventures is liable to harm the country's economy, not only directly, such as through the inability to supply an essential service, but also in the form of commercial damage, e.g., the inability of Israeli companies that were attacked to supply their products for a given period.

An example that clarifies the proposed process is the requirement to submit an Environmental Impact Assessment. The goal of the assessment is to identify the environmental hazards that are likely to be caused by the project, along with ways to minimize this damage to a tolerable level. Submission of the review is anchored in the planning and building regulations (of 1982, and in its final version of 2003). The idea for this review originated in the enhanced public awareness in the United States of environmental issues, which in 1970 led to legislation requiring preparation of an Environmental Impact Assessment as part of the planning process.

Together with the planning component of new projects, it is also possible to make use of the business licensing process, which requires periodic renewal to ensure that over the years the project meets the necessary criteria in various spheres, including protection from cyber

attacks. According to Justice Mishael Cheshin, "the goal of the [business licensing] law is to preserve and protect various values that our society considers important . . . such as the value of public safety, with the value of maintaining public health and safety, and the value of preserving the environment and quality of life . . . protecting the goals of society."[8] Use of the tools provided by the business licensing law for cyber protection and upholding its goals provides the Information Security Authority with an additional legal tool to ensure that existing activities are required to meet the necessary criteria. In certain cases, there has even been a demand of private business owners to submit a Cyber Resiliency Assessment and a requirement to meet security guidelines.

Projects in the pre-establishment process and in certain cases those that have already been set up will be required to submit a Cyber Resiliency Assessment to the Information Security Authority, which can ensure that essential protection instructions are followed. A number of guidelines can be proposed for the content of this assessment and for those authorized to submit and those authorized to check it. From a statutory point of view, the review process must be applied comprehensively and govern all requests, unless the authorized authority grants an exemption. However, from a practical point of view, the Information Security Authority will be required to draft criteria that define the projects and ventures for which an assessment must be submitted. These criteria could address a number of components, such as the size of the project, its sector (for example, the energy sector, natural gas, and the like), the project's interfaces with elements already under the purview of the Information Security Authority, and the expected damage in the event of a cyber attack.

When a decision is made that the body must submit a Cyber Resiliency Assessment, the process will adhere to a defined procedure, as follows:

a. *Assessment guidelines*. It is the responsibility of the Information Security Authority to prepare guidelines for carrying out the assessment. These guidelines must be suited to the project or the specific body and cover a number of components, including: mapping the potential damage from a cyber attack; mapping the weak points of the project/plan; and issuing instructions that will make it possible to minimize exposure and damage.
b. *Assessment preparation*. The assessment will be prepared under the auspices and with the funding of the project initiator. For this

purpose, there will be consultants from a group of designated consultants trained and authorized by the Information Security Authority. These consultants will work according to the assessment preparation guidelines.

c. *Checking the assessment*. By virtue of its responsibility, the Information Security Authority can use external advisors trained and authorized to check the reviews, with the cost charged to the project initiator. In this process, it is possible that there will be a number of rounds of questions and answers between officials in the Information Security Authority and the party under review.

d. *Approval of the assessment*, meaning examination and review by the authority's officials and a decision on guidelines in this context for the project. This approval can also address aspects of the stipulations for the business license, as well as instructions that should be applied to the project initiator's plans.

Similarly, the business licensing law also constitutes an appropriate platform for implementing instructions and guidelines in the realm of protection from cyber attack. Due to the restrictions applying to the security and flow of information, it will be necessary to define this process as a departmentalized process that is not open to the wider public, but only to specific authorized officials.

Conclusion

Threats to civilian companies have grown not only because of increased competition in the marketplace but also because of their exposure to attacks by hostile elements. Hostile parties identify the potential damage to the country's economic infrastructure inherent in attacking these companies. States tend to protect mainly bodies that have a direct connection to national security, which traditionally included primarily government offices; intelligence and security bodies; organizations engaged in sensitive classified security manufacturing; and classical critical infrastructures, such as electricity, water, transportation, and so on. The logic that defined the criterion of this privileged class was derived from the classic strategic concept: a list of national infrastructures susceptible to disaster in the event of war, and which if damaged could cause direct harm to the country's fighting ability and resiliency. However, what will be the fate of civilian companies such as

Teva Pharmaceutical Industries, or food manufacturing companies such as Tnuva, the Strauss Group, and the like? And what of cable companies and insurance companies, not to mention memorial and heritage sites? A quick examination shows that damage to these organizations is liable to cause significant damage to the country and harm the fabric of civilian life.

The establishment of the Information Security Authority and the steering committee of the National Security Council were first steps in the right direction. Now, with the increasing realization that cyberspace is becoming a combat zone before our eyes, the ability of the State of Israel and its economy to weather attacks of this type must be enhanced. Introducing cyber defense in the statutory processes can allow ongoing, systematic monitoring of the immunity of Israel's cyber security system.

Notes

1 This saying is usually attributed to Frederick the Great.
2 The website of the Information Security Authority, http://www.shabak.gov.il/about/units/reem/pages/default.aspx.
3 Gal Mor, "Plan for Information Security Approved by Government," *Ynet*, December 11, 2002, http://www.ynet.co.il/articles/1,7340,L-2310234,00.html.
4 Patrick Beggs, "Securing the Nation's Critical Cyber Infrastructure," US Department of Homeland Security, February 25, 2010.
5 Ibid.
6 Patrick Beggs is the director of Cyber Security Evaluations – National Cyber Security Division in the US Department of Homeland Security.
7 The term "delivery systems" serves to describe infrastructures that conduct materials: water, sewage, waste water, gas, oil, electricity, communications fibers, and the like.
8 Justice Mishael Cheshin, Criminal Appeals Authority (CAA) 4270/03, State of Israel vs. Tnuva.