Military and Strategic Affairs

Volume 6 | No. 3 | December 2014

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

ISSN 2307-193X (print) • E-ISSN 2307-8634 (online)

Military and Strategic Affairs

Volume 6 | No. 3 | **December 2014**

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 a refereed journal 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.

The Institute for National Security Studies is a public benefit company.

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

The Institute for National Security Studies (INSS)
40 Haim Levanon • POB 39950 • Tel Aviv 6997556 • 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

ISSN 2307-193X (print) • E-ISSN 2307-8634 (online)

From Plowshares to Swords? UN Forces on Israel's Borders in the Second Decade of the Twenty-First Century

Chen Kertcher

> And they shall beat their swords into plowshares, and their spears into pruning hooks; nation shall not lift up sword against nation, neither shall they learn war any more. (Isaiah 2:4)

This article examines the contribution made by peacekeeping operations on Israel's borders to regional stability since Israel's establishment, especially in the face of the challenge posed by armed non-state actors in the second decade of the twenty-first century. The article is divided into three parts. The first part presents the main changes in the operating principles of peacekeeping missions from the Cold War to the present. The second provides a concise overview of the rationale for peacekeeping operations on Israel's borders. The third examines the ability of peacekeeping missions to confront the political and security challenges they face, first and foremost, from armed non-state actors.

Key words: UN, peacekeeping forces, non-state actors

Peacekeeping Operations During and After the Cold War

In discussing the topic of Israel and peacekeeping forces, we must explain the theoretical and historical context of the phenomenon. The legitimacy to carry out international operations is anchored in the powers defined in the United Nations Charter, which was signed on June 26, 1945. In his

Dr. Chen Kertcher is a researcher at the Herzl Institute for Research and Study of Zionism and History, Haifa University and the Interdisciplinary Center, Herzliya.

book *Swords into Plowshares: The Problems and Progress of International Organization*, international relations scholar Inis L. Claude argues that the establishment of the UN was a second attempt by the nations of the world to establish a global system ensuring and strengthening collective security as an alternative to the system that regulated relations between the states of Europe starting in the second half of the seventeenth century, which was based on a balance of power.[1]

The UN's collective security system was intended to deter states from using force against each other by threatening that such use of force would lead to a collective response from the other members of the system. However, if these members undertook collective action on behalf of a state that had fallen victim to the use of force, they would pay a price for their intervention (economically or in the form of a security threat to their citizens) and endanger their system of interests and alliances because and in defense of the principle of collectivity, which is supposed to preserve their security.[2]

Consequently, the United Nations established an operational body responsible for issues of global security: the Security Council. The council has five permanent members—the United States, Russia (until 1992, the Soviet Union), Great Britain, China, and France—and another ten non-permanent members, which are elected for two-year terms. The UN Charter sets out two methods of dealing with conflicts: Chapter VI refers to peaceful settlement of disputes, and Chapter VII to methods of enforcement that can be used by the Security Council in an attempt to preserve international peace. During the Cold War, the Security Council was unable to reach resolutions to confront acts of aggression and wars on the basis of Chapter VII because of the conflict between the Western and Eastern blocs, and the UN as a whole failed at that time in its handling of most conflicts in the world.[3]

The collective security system's failure to provide protection led to the development of a new system involving the dispatch of military forces to areas of conflict or confrontation as part of the efforts to build trust among the parties to the conflict. These "peacekeeping forces" have been deployed along international borders or ceasefire lines. They even received the Nobel Peace Prize in 1988 in recognition of their contribution to world peace.

In order to differentiate between peacekeeping missions and military operations intended to serve national security interests, a number of

peacekeeping principles have been established. Such operations would not take place unless agreement was obtained from the parties to the conflict to stop fighting and to allow multinational forces deployment. Usually, peacekeeping forces include soldiers from nations that do not have a direct interest in the conflict, and therefore, it has generally been agreed that they will not include representatives from the superpowers. Nevertheless, it has been necessary to obtain the superpowers' consent to their dispatch, generally by means of Security Council resolutions. One of the basic requirements of peacekeeping forces is neutrality– in UN terms– impartiality. In addition, they are prohibited from using force, other than in self-defense. In order to ensure this principle, operations have generally been limited in scope, and the soldiers who manned them have been armed only with light weapons.

These principles were intended to ensure that a peacekeeping operation would be part of a process to resolve the conflict. To this extent, the military forces that participate in such operations are part of this process. According to Brian Urquhart, who conducted peacekeeping operations from the early 1960s until his retirement from the UN in the mid-1980s, "The moment a peacekeeping force starts killing people it becomes a part of the conflict it is supposed to be controlling, and therefore, a part of the problem."[4] In such cases, the peacekeeping forces' impartiality is questioned, possibly leading at least one of the parties to the conflict to revoke its consent to their presence.

During the Cold War, the UN undertook thirteen peacekeeping operations, which reflected the middle road between mediating conflicts on the one hand, and enforcement on the other. These operations can be seen as realization of the biblical vision of the Prophet Isaiah, "and they shall beat their swords into plowshares."

At the end of the Cold War, peacekeeping operations were designated as means to resolve intrastate conflicts, based on the understanding that every violent conflict or humanitarian disaster has the potential to cause economic damage, undermine social order, and the political-security-economic equilibrium among countries near the locus of conflict.[5] Because the traditional system of peacekeeping missions was not suited for operations within states, and such operations were even explicitly banned, there was a need to define new objectives for peacekeeping operations in order to adapt them to new needs, such as monitoring democratic elections,

supervising the establishment of civilian institutions, monitoring human rights preservation, monitoring the disarming of soldiers, humanitarian assistance, and economic development.

In order to differentiate the new generation of peacekeeping initiatives from their predecessors, new names were suggested, including "second-generation peacekeeping operations," "broad peacekeeping operations," "humanitarian aid operations," "peace-support operations," "peace-enforcement operations," "peace-stabilization operations," and "peace-building operations."

In contrast to the traditional missions, which were undertaken after agreement was reached between the parties to the conflict, second-generation multi-purpose operations were, in many cases, undertaken during active conflict, with the intention to create the conditions for its resolution. The forces that took part in these operations were larger than their predecessors and were deployed throughout the country in which the conflict broke out, in accordance with the purposes for which the force was established.

The success of the traditional operations was dependent on the support of the parties to the conflict and the other nations of the world. The success or failure of the multi-purpose operations since the Cold War has been dependent on the size of the contribution from the various countries of the world (political support, manpower, and funding) and on the length of time these countries were prepared to continue to invest in them. The precondition for carrying out traditional operations was the consent of the parties to the conflict to UN involvement. This lost its importance when different objectives were set for UN forces, such as preventing a humanitarian disaster after the war in Bosnia, the famine in Somalia, or saving the Albanian population in Kosovo in 1999.

Beginning in 2001, an international norm developed called "responsibility to protect," whose main aspect includes providing the Security Council authority to decide on an enforcement operation in cases involving significant human rights violation. For this reason, enforcement operations were authorized under Chapter VII of the UN Charter, thus allowing the multinational troops to use force against local armed elements. In these cases, such as in Darfur in the Sudan or in eastern Congo, UN forces operating in the area were granted permission to use force in order to protect the local residents. To ensure that these forces could fight effectively against the local forces if necessary, UN peace-enforcement operations sometimes numbered tens of thousands of well-armed soldiers.[6]

Peacekeeping Operations on Israel's Borders

Israel and the United Nations have shared a complex relationship; in Israel's eyes, the UN has consistently condemned Israel while taking a lenient approach to other serious incidents around the world.[7] One such example includes the General Assembly resolution from 1975 equating Zionism with racism.[8] At the same time, Israel's hostility towards the UN was not concealed. As early as 1955, Israeli Prime Minister David Ben Gurion coined the expression "UM, SHMUM" [expressing contempt for the UN], noting that "it doesn't matter what the gentiles say; what matters is what the Jews do."[9] This Israeli attitude toward the UN had not changed over the years. Prime Minister Benjamin Netanyahu, in his speech to the UN General Assembly in September 2011, stated that the UN was "a house of many lies."[10] These comments by Israeli officials emphasize Israel's fundamental approach over the years; it cannot trust the UN's principle of collective security and place its security in the hands of others.[11]

The tense relations between Israel and the UN deserve special examination, mainly in light of the role played by UN peacekeeping forces on Israel's borders. The history of the State of Israel and its wars and the history of UN peacekeeping operations are intertwined; in 1948, the first multinational mission was undertaken, involving the dispatch of military observers under the UN flag, intended to monitor implementation of the Armistice Agreements between Israel and the Arab countries. This mission, called the United Nations Truce Supervision Organization (UNTSO), continues to operate to this day. It includes some 150 soldiers, and its headquarters are in the Government House in Jerusalem.[12]

Eight years later, a decision was made to launch another UN operation connected to Israel, the United Nations Emergency Force (UNEF). This mission was intended to monitor the withdrawal of British, French, and Israeli forces from Egypt following the Suez Campaign in 1956 as well as to monitor the border between Israel and Egypt. The operation included some 6,000 soldiers from ten countries. When UNEF received a unilateral demand from Egypt in May 1967 to withdraw immediately from the Sinai Peninsula, the UN agreed, and to Israel's dismay, the force left the area. Shortly thereafter, Israel and Egypt (joined by Jordan and Syria) were involved in the Six Day War in 1967.[13]

At the end of the Yom Kippur War in 1973, two new operations were launched. The United Nations Emergency Force II included nearly 7,000 soldiers and was deployed on the ceasefire borders between Israel and

Egypt.[14] The United Nations Disengagement Observer Force (UNDOF), which was deployed in the Golan Heights starting in June 1974, numbered over 2,000 soldiers and civilians, with the main contributing nations being Austria, India, Japan, the Philippines, Cambodia, and Croatia.[15] In the wake of crises in the region and the internal conflict in Syria, the force currently includes a little over 1,000 soldiers.

In 1978, after an Israeli military operation in southern Lebanon in response to Palestine Liberation Organization (PLO) infiltrations into Israeli territory, the Security Council decided to establish the United Nations Interim Force in Lebanon (UNIFIL). In the wake of the Second Lebanon War (July-August 2006), the Security Council passed resolution 1701, which increased UNIFIL forces from 2,400 to 15,000 soldiers and civilians. The main purpose of these forces was to facilitate the Lebanese deployment along the "Blue Line" (the international border between Israel and Lebanon) and help transport humanitarian aid to residents of the region. In 2014, some 10,000 soldiers and civilians have served in UNIFIL.[16]

Following the signing of the peace treaty between Israel and Egypt in 1979, the Soviet Union used its veto power to prevent the Security Council from extending UNEF II's mandate in the Sinai, thus terminating the mission. In the wake of the Soviet veto, the governments of Israel and Egypt, which were interested in peacekeeping forces' aid in the implementation of the peace treaty, formulated a special protocol, signed in 1981, calling for the establishment of the Multinational Force and Observers (MFO), based on the principles of peacekeeping operations. The force operates to this day in the Sinai Peninsula.[17]

The Declaration of Principles on Interim Self-Government Arrangements (known as the Oslo Accords), signed in September 1993 between the government of Israel and PLO representatives, was supposed to lay the groundwork for ending the Israeli-Palestinian conflict. Over the years it has given rise to small peacekeeping operations intended to aid the parties in implementing certain articles in the agreements between them.[18] Following the events in the Cave of the Patriarchs in February 1994, the Security Council decided to establish the Temporary International Presence in Hebron (TIPH). Initially receiving a mandate for three months, it became permanent in 1997. Today TIPH consists of between 50 to 200 civilian observers, monitoring and reporting on incidents in Hebron to the parties

involved in the conflict along with the six nations that contribute to its operations.[19]

The European Union adopted a different model for the Israeli-Palestinian arena, and from November 2005 to June 2007, it operated a force including customs and police officers on the Rafah border crossing with the Gaza Strip: the European Union Border Assistance Mission (EUBAM) in Rafah.[20] The UN has never decided to establish a peacekeeping force for Israel and the Palestinians.

The above overview demonstrates that most peacekeeping missions on Israel's borders were undertaken during the Cold War, and as such, were heavily influenced and shaped by that period. Five of the thirteen UN missions during the Cold War took place on Israel's borders. An additional three operations took place in the Sinai Peninsula, the West Bank, and the Gaza Strip. While these missions were not undertaken under a UN mandate, they adopted the traditional operating principles of UN missions. Their main objective was to observe and report to the opposing parties, the Security Council, and the contributing nations.

Aside from UNIFIL, UN Missions deployed on Israel's borders were limited in number and scope. They operated according to political agreements reached between the two opposing sides, which represent sovereign entities, and enjoyed broad international consensus and support. Despite the limitations of these forces, Israel and its neighbors have preferred the Cold War model of peacekeeping forces under international auspices as part of confidence-building measures, believing that these forces will assist in creating dialogue between them.

First-Generation Peacekeeping Missions under Second-Generation Conditions

The main difficulties plaguing peacekeeping missions along Israel's borders in the past decade stem from the fact that they operate according to first generation rationale, while their environment is more suited to second-generation missions. The main reason being the ongoing process of weakening of governance capability in Middle Eastern countries as a result of the Arab Spring, which began in 2010, and the strengthening of armed non-state actors. These include Hizbollah, Hamas, and other armed political Islamic organizations, like Jabhat al-Nusra and the Islamic State (IS). These non-state actors are not bound by any ceasefire, armistice, or peace

agreements and in some cases, they even undermine them. Furthermore, the areas in which peacekeeping forces operate are limited while the forces themselves are armed with light weapons, making them an easy target for terrorist operations by non-state actors.

It is evident that the weakening of governance capability in various countries in the region threatens the peacekeeping forces along Israel's borders. Since the revolution in Egypt in 2011, terrorist attacks in the Sinai Peninsula have undermined stability in the region. The Egyptian military coup in July 2013 led to an increase in the number of Egyptian military forces in the Sinai and to frequent operations against Islamic terror operatives (in addition to action against the Muslim Brotherhood). However, they were not able to stabilize the situation. Altercations with terrorist groups have cost the lives of numerous Egyptian soldiers and members of the multinational force. In fact, the latter are completely dependent upon Egypt for safety. Consequently, their current activities are limited to serving as liaisons between Israel and Egypt.[21]

The tension between Hizbollah and Israel on the border with Lebanon, reflected in Israeli operations to prevent the transfer of advanced weaponry from the Syrian army to Hizbollah,[22] affects UNIFIL's ability to function effectively. Its reports to the Security Council clearly indicate that it cannot promote the disarming of Hizbollah, nor can it implement the weapons embargo Cooperation between UNIFIL forces and the Lebanese government and army has not succeeded in preventing the formation and arming of military organizations in southern Lebanon, in violation of Security Council resolution 1701.[23] The European governments' inclusion of Hizbollah's military wing in a list of terrorist organizations may entail implications for UNIFIL's functioning: the Italian government—whose representative is the UNIFIL commander—objected to this move because it feared negative effects on the functioning of forces from European countries that are part of UNIFIL.

The ongoing civil war in Syria endangers the multinational forces that are part of the United Nations Disengagement Observer Force (UNDOF) in the Golan Heights. Following incidents in which UN soldiers were wounded or taken prisoner, Cambodia, Japan, and Croatia withdrew their forces from Syria. In addition, in early June 2013, as fighting escalated, the government of Austria, which had provided about one-third of the soldiers remaining in the force, announced that it would not continue to contribute

forces to the UN in the Golan Heights. In the summer of 2013, Russia, allied with Syrian president Bashar Assad, offered to replace these forces. The offer was categorically rejected by the UN Secretariat, which emphasized that according to the agreement between Israel and Syria, none of the five permanent members of the Security Council would have a presence in the Golan Heights.[24] The UN Secretariat ultimately succeeded in overcoming UNDOF's manpower crisis by persuading other countries to send troops to Syria. The escalation between rebel forces and the Syrian army in the summer of 2014 created new crises; during the fighting, UN soldiers were killed or wounded, and dozens of other UN soldiers were taken prisoner by the rebels. As a result, the force's command decided to evacuate many observation posts on the Golan Heights. However, UNDOF forces continue to enjoy the support of the IDF and the Syrian army, cooperating with it partly for fear that escalation in the fighting between Syria and the rebels could push them to intervene.[25] The main contributors to UNDOF manpower, as of September 2014, are Fiji (445 soldiers), the Philippines (344), India (191), Nepal (155), and Ireland (134).

The continuing instability in the Middle East may force the parties involved in UN peacekeeping operations to choose between several alternative courses of action. Since most of the discussion today focuses on the possible dissolution of the UN mission in the Golan Heights, the following are possible courses of action.

The first possibility is to continue the mission in the Golan Heights in its current form while ignoring the changes on the ground. This choice is dependent upon Israel and Syria's continued agreement to the force's presence as well as contributing nations' agreement to send forces despite the dangers. In the past, when the Security Council decided to extend UNIFIL's mandate, it was forced to operate in the security zone Israel created in southern Lebanon between 1985 and 2000 without the consent of the Lebanese government.[26] In the Lebanese case, Israel was able to protect the UN forces. In the event of a similar scenario in Syria, it is reasonable to assume that the nations contributing to UNDOF will demand guarantees to protect their forces, but that the provision of such guarantees is beyond the ability of the Syrian government. The course of events in the last two years constitutes proof of Syria's inability to protect UN forces on its territory, and therefore, it should be assumed that the danger they face in the Golan Heights will increase. This will require a fundamental change in mandate.

The second possibility is to terminate the mission on the Golan Heights. In May 1967, when the Egyptian government demanded the immediate withdrawal of UN forces from its territory, then-UN Secretary General U Thant determined that there was no point in their continued presence if the condition of "consent" was not fulfilled. Current conditions indicate a similar lack of consent and therefore some argue that the mission in its current form should be ended. Nevertheless, the members of the Security Council are reluctant to bring it to an end because of its contribution to maintaining dialogue between the governments of Israel and Syria, and thus helping to manage and contain the conflict.[27]

If the Security Council and the contributing nations view the end of the mission in the Golan Heights or its continuation in its current form as impracticable, there is a third option: they can demand a change in UNDOF's mandate from "plowshares into swords," or in other words, allow it to make more extensive use of force. In this context, initiatives have been introduced in the past two years by Western and Arab representatives, which have included the possibility of an enforcement operation by a large multinational military force that would take control of certain areas in Syria on the basis of the principle of "responsibility to protect," which has been promoted in the international arena in the past decade. Alternatively, there have been proposals to launch an air operation that would create a safe zone in Syria, like the model used in Libya during 2011. These initiatives have thus far been rejected by the Chinese and Russian governments.[28] As long as the great powers who have a vested interest in Syria refuse to act unilaterally and without a mandate from the Security Council, this option is not feasible either.

The last option for leaving the UN force on the Golan Heights intact would require the Security Council to adopt a complex model resembling those adopted in the civil wars in the Sudan, Sierra Leone, Mali, and the Congo in the past decade. This model would require approval for extending the forces operating in the area and for using force and providing appropriate means to enable UN forces to deter attacks in areas for which they are responsible. Such a model, which could include forces from a wide variety of countries, could fulfill the main purpose of the mission on the Golan Heights: to serve as a buffer force in a demilitarized zone that enjoys the support of governments that are interested in an agreement. Such a model could also address a variety of challenges in a way that could serve the interests

of all the parties involved: first, it would allow the contributing nations to protect their forces. Second, it would encourage Israel to perceive the force as a stabilizing factor that could maintain the demilitarized zone. Third, it would assure the Syrian government that the rebel forces fighting against it would not use areas under the UN force's supervision for operations against the Syrian army. Fourth, Security Council members could find in such a model a solution to the disputes among them. Additional advantages that could stem from a peacekeeping operation that is based on this model are providing humanitarian aid to civilians in the area, similar to UNIFIL in southern Lebanon, and perhaps even encouraging the warring parties in Syria to shift their operations to other arenas in the country. The success of such a UN operation in the Golan Heights could strengthen the trust of all stakeholders in the area in other UN missions there as well. On the other hand, if the mission fails, could deteriorate to a total dissolution of the UN force on the Golan Heights. Such a situation could encourage non-state actors to attack other UN forces in the area under the assumption that they can exploit their weakness in order to entrench themselves in their areas of operation.

In conclusion, UN forces on Israel's borders operate according to traditional principles. The rise in the influence of armed non-state actors is undermining their ability to contribute to regional stability and could even bring UN operations in the area to an end. Such a development has the potential to lead to a clash between Israel and its neighbors.

From Israel's point of view, UN peacekeeping operations based on second-generation models, which will be more complex than those of the first generation but will not necessarily have enforcement powers, could aid in preventing or reducing violent incidents between Israel's military forces and those of Syria or other countries in the region. A change in the mandate of UN forces and the way in which they are used could also have a positive and cumulative effect on overall security stability in the region, as well as on the level of trust between Israel and the United Nations.

Peacekeeping Missions on Israel's Borders

Acronym	Mission Name	Start Date	Closing Date
UNTSO	United Nations Truce Supervision Organization	May 1948	Present
UNEF I	First United Nations Emergency Force	November 1956	June 1967
UNEF II	Second United Nations Emergency Force	October 1973	July 1979
UNDOF	United Nations Disengagement Observer Force	June 1974	Present
UNIFIL	United Nations Interim Force in Lebanon	March 1978	Present
MFO	Multinational Force & Observers	January 1982	Present
TIPH	Temporary International Presence in Hebron	1997	Present
EUBAM Rafah	The European Union Border Assistance Mission at the Rafah Crossing Point	November 2005	June 2007

Notes

1 Inis L. Claude, Jr., *Swords into Plowshares: The Problems and Progress of International Organization* (New York: Random House, 1961), pp. 250-94; Henry Kissinger, *Diplomacy* (London: Simon & Schuster, 1994), pp. 17-28; Thomas G. Weiss, David P. Forsythe and Roger A. Coate, *The United Nations and Changing World Politics* (Colorado: Westview Press, 2001), pp. 21-27, 38-44.

2 Claude, *Swords into Plowshares*, pp. 250-94; Alan C. Lamborn, "Theoretical and Historical Perspectives on Collective Security: The Intellectual Roots of Contemporary Debates about Collective Conflict Management," in *Collective Conflict Management and Changing World Politics,* eds. J. Lepgold and Thomas G. Weiss (Albany: State University of New York Press, 1998), pp. 31-56; Joseph Lepgold and Thomas G. Weiss, "Collective Conflict Management and Changing World Politics: An Overview," in *Collective Conflict Management and Changing World Politics*, pp. 3-21.

3 Sydney D. Bailey and Sam Daws, *The Procedure of the UN Security Council* (Oxford: Clarendon Press, 1998); Yoram Dinstein, *War, Aggression and Self-Defense* (Cambridge: Cambridge University Press, 2005), pp. 85-328;

Malcolm N. Shaw, *International Law* (Cambridge: Cambridge University Press, 2003), pp. 914-50, 1119-47.

4 Brian Urquhart, *A Life in Peace and War* (New York: Harper & Row, 1987), pp. 178-79.

5 Chen Kertcher, "From Cold War to a System of Peacekeeping Operations: The Discussions on Peacekeeping Operations in the UN during the 1980s up to 1992," *Journal of Contemporary History* 47, no. 3 (2012): 611-37.

6 Martha Finnemore, *The Purpose of Intervention: Changing Beliefs about the Use of Force* (Ithaca: Cornell University Press, 2004), pp. 52-84; Nicholas J. Wheeler, *Saving Strangers: Humanitarian Intervention in International Society* (Oxford, New York: Oxford University Press, 2000), pp. 139-284; Thomas G. Weiss, *Humanitarian Intervention: Ideas in Action* (Cambridge: Polity, 2012).

7 Avi Beker, *The United Nations and Israel–From Recognition to Reprehension* (Lexington: Lexington Books, 1988); S. D. Bailey and M .J. Peterson, *The UN General Assembly* (London: Routledge, 2005).

8 A/RES/69/19, November 29, 2012.

9 Attributed to David Ben Gurion's speech at the IDF's Independence Day parade, Ramat Gan, April 27, 1955.

10 Speech by Israeli Prime Minister Benjamin Netanyahu to the UN General Assembly, September 23, 2011, http://mfa.gov.il.

11 Avi Shlaim, *The Iron Wall: Israel and the Arab World* (Tel Aviv: Yediot Ahronot, 2005); *The UN and Israel: Can they Cooperate?* Eli Fried, ed. (Tel Aviv: Tel Aviv University, 2004-5).

12 United Nations Truce Supervision Organization, UN website, http://untso.unmissions.org/.

13 First United Nations Emergency Force, UN website, http://www.un.org/en/peacekeeping/missions/past/unefi.htm

14 Second United Nations Emergency Force, UN website, http://www.un.org/en/peacekeeping/missions/past/unefii.htm

15 United Nations Disengagement Observer Force, UN website, http://www.undof.unmissions.org/.

16 United Nations Interim Force in Lebanon, UN website, http://unifil.unmissions.org.

17 Multinational Force and Observers, MFO website, http://mfo.org/.

18 Ministry of Foreign Affairs, *Declaration of Principles on Interim Self-Government Arrangements*, September 13, 1993, http://www.mfa.gov.il.

19 Temporary International Presence in Hebron (TIPH), http://www.tiph.org/.

20 European Union Border Assistance Mission in Rafah, EUBAM website, http://www.eubam-rafah.eu. In addition, various Western advisory forces operating in the West Bank are intended to promote the development of civil and security institutions. This article does not refer to these forces because as a rule, they do not operate in accordance with the principles of peacekeeping operations and are primarily bilateral operations agreed upon between the Palestinian Authority (PA) and international bodies.

21 Nikola Kovač and Trista Guertin, "Armed Groups in the Sinai Peninsula," Civil-Military Fusion Center, February 2013, http://reliefweb.int/sites/reliefweb.int/files/resources/20130228%20Armed%20Groups%20in%20the%20Sinai%20Peninsula.pdf; Inna Lazareva, "Sinai Peacekeepers under Siege as Egypt Battles Islamists," *Telegraph*, September 17, 2013.

22 "Report: Israel Warns Syria to Stop Sending Arms to Hizbollah," *al-Arabiya*, May 16, 2013.

23 S/2013/381, June 26, 2013; S/S/2013/650, November 13, 2013; S/2014/130, February 26, 2014; S/2014/438, June 26, 2014; Nicholas Blanford, "UNIFIL Increasingly Frustrated with Hizbollah," *Daily Star*, Lebanon, May 1, 2013; Gavriel Fiske, "EU Threatens Pullout of South Lebanon Peacekeepers," *Times of Israel*, May 12, 2013; Jean-Loup Samaan, "UNIFIL's Uncertain Future," *al-Monitor*, June 14, 2013; Justyna Pawlak, "Britain Fails to Get EU Backing for Hizbollah Blacklisting," *Reuters*, June 19, 2013; Soeren Kern, "Hizbollah Rearmed under EU Monitors: Is Hamas Next?" The Clarion Project, September 2, 2014.

24 Martin Nesirky, Spokesperson for Secretary-General Ban Ki-Moon, *Highlights of the Noon Briefing*, June 10, 2013, http://www.un.org/sg/spokesperson/highlights/?HighD=6/10/2013&d_month=6&d_year=2013.

25 S/2014/401, June 10, 2014; S/2014/665, September 12, 2014; S/PRST/2014/19, September 19, 2014.

26 The security zone is the name given by the government of Israel to the area in southern Lebanon to which the IDF withdrew in June of 1985 in order to prevent terrorist infiltration into Israeli territory. The IDF maintained control over this area, which was about 10 percent of the entire area of Lebanon, until its withdrawal to the international border on May 24, 2000.

27 UN, SC/10962, March 27, 2013; UN, SC/10999, May 7, 2013; UN, SC/11011, May 16, 2013; UN, SC/11027, June 6, 2013.

28 The most the Security Council can manage is to express concern over the continuation of the conflict in Syria. See, for example, the council's declaration after the heavy fighting in the Syrian city or al-Qusayr, UN, SC/11028, June 7, 2013.

Hasn't the Time Come for the Political Training of Senior IDF Officers?

Yoram Peri

The Harpaz Affair has revealed one of the worst crises in the history of the relations between the political and military echelons in Israel. Despite the great interest in the affair, one crucial aspect of the relations between then-Minister of Defense Ehud Barak and then-IDF Chief of Staff Gabi Ashkenazi has been ignored: the battle between the two over the "general headquarters" section of the IDF Supreme Command orders, which sets forth the status of the Defense Minister vis-à-vis the IDF Chief of Staff and reflects who is head of the military. This is a struggle on the very principles determining the relations between the political echelon and the subordinate military echelon. While the reasons for the recurring crises between the two echelons are generally known and various plans for correcting the situation have been devised, systematic steps to rectify the situation have yet to be taken. What are the reasons for preferring ambiguity in defining the relations between the two? Whose interest does this ambiguity serve, and to what end?

Key words: Harpaz Affair, civilian oversight of the army, ambiguity in relations between the political and military echelons, crisis in relations between the Defense Minister and the IDF Chief of Staff, authority of the Defense Minister, military-political partnership, Agranat Commission Report, Winograd Commission

A long list of books, articles, interviews, and testimonies–the most recent of which is a biographical study of former head of IDF Military Intelligence

Prof. Yoram Peri holds the Kay Chair in Israel Studies, and is Director of the Gildenhorn Institute for Israel Studies at the University of Maryland at College Park. He is the founder and former head of the Chaim Herzog Institute for Media, and a professor of political sociology and communication in the Department of Communications at Tel Aviv University.

Aharon Yariv[1]–reiterate and highlight the depth of the IDF's involvement in national politics in Israel. Yariv himself regarded this phenomenon with alarm while still in uniform. "I told Golda Meir numerous times, 'You must not use me, the head of IDF Military Intelligence, as a liaison with the American administration. The close connections I maintain with them are liable to affect my ability to be a good, neutral, and impartial evaluator. For that, I need distance from the decision makers,' but she didn't accept my opinion."[2] Despite these views of the general who later became a cabinet minister, the new biography reveals previously unknown details about the depth of his involvement in determining Israeli policy.

If Yariv's views–though not his deeds–conformed to the rule that the military should not be involved in these civilian processes, the case of Moshe ("Bogie") Ya'alon stands in complete contrast. In the view of the former Chief of Staff-turned-Defense Minister, the fundamental problem underlying Israel's security strategy is the need for national recognition that we are a "nation at war." At present, and for the foreseeable future, Israel in in a state of perpetual war, as a "war between the wars" continues with various peaks of intensity. The ability to withstand a war of this kind depends first and foremost on the civilian population's conceptions, and therefore one of the military's first missions is to prepare the country for this situation.[3]

Ya'alon was the first to systematically develop this concept, expanding the fields of military endeavor, thinking, and planning to non-military dimensions. These, in turn, affect the military effort and enhance the army's activity within civilian society and the political system. He formulated, developed and realized this doctrine when he served as Commander of the IDF Central Command, and expanded it when he was appointed Chief of Staff.[4]

Between the actual behavior of Gen. Yariv in the 1960s and the reasoned concept of Gen. Ya'alon in the first decade of the 21st century, much evidence was published by academic researchers and members of the military or political system indicating that the IDF's relationship with the political sphere does not coincide with what Israel's first Prime Minister and Defense Minister David Ben Gurion envisioned. In fact, never in its history was the IDF an instrumental army, divorced from politics and merely carrying out policy dictated to it by the civilian echelon.[5]

In addition to the empirical evidence, the symbiotic relations between the military and civilian sectors have been the focus of theoreticians and researchers.[6] A pioneer in this field was Rebecca Schiff, who presented the Theory of Concordance, asserting that the military and civilian spheres must engage in dialogue and agree to share responsibilities. Douglas Bland spoke of shared responsibility and a regime of norms shared by "friendly adversaries." Elliot Cohen, who improved Huntington's concept of professionalism, coined the term "unequal dialogue." In addition, I proposed the "military-political partnership" model.[7]

The wars in Iraq and Afghanistan have provided a plethora of material for examining the military-political relations in the United States, specifically the Pentagon and the president,[8] facilitating the development of additional theories; Snyder and Gibson's Network of Connections model, for instance, was adopted by Sheffer and Barak in their description of the "defense network," in which the distinction between the two sectors is essentially meaningless.[9]

Kobi Michael aptly described the tension, or dialogue, between the political and military echelons in terms of a "discourse space" in which this dialogue is conducted. He described an "intellectual meeting of exchanges of information and knowledge, in which the political objectives and their military significance are defined."[10]

The most recent in the series of writers was Yagil Levy, who analyzed the relationship between the military and political echelons, and the "bargaining space," a repertoire of operative possibilities from which the Chief of Staff can choose at times of conflict between the military and political echelons.[11] Levy bases his theory on the following rationale: the military and the civilian institutions maintain relations based on exchange, as the military accepts subordination to the civilian echelon in return for resources and legitimization. When the military feels that these relations are unbalanced, it expresses opposition to the political authority. For its part, the political echelon is limited in its ability to restrain the military, because its needs the services provided by the military. To the extent that the political echelon is in need of such legitimization–for example, the dramatic decisions to go to war or peace measures subject to public dispute–its position in the dialogue with its military partner is weaker.

Despite the growing body of research examining the symbiotic nature of the relationship between the military and civilian echelons, it seems that

researchers tend to think in terms of the old instrumental model as they advocate for strengthening civilian oversight by at the military's expense. This model, which former IDF Planning Directorate member Lieutenant Colonel Alon Paz referred to as the "delineation approach," reflects the most common perception of the issue. However, the alternative model of a symbiotic partnership or, as Paz puts it, "the interventionist approach," in which there is constant negotiation and a dynamic equilibrium between the two "spheres of knowledge" is a better description of the situation in Israel.[12]

Should it therefore be concluded that in order to rectify the situation an emphasis must be placed on the military side of the equation? Does the fact that the military bears a direct influence on politics require that senior military leadership gain a deeper understanding of the political process and rules of the game? Shouldn't senior officers' training include broader historical knowledge in addition to military knowledge? Should the IDF incorporate the "civilian leadership" theme in its officers' education, referring not to electoral politics or ideology but rather comprehension of political theory and rules, similar to the education of political science students in the university? Instead of completely ignoring the military's political character and influence, perhaps familiarity with political thought may help strike a better balance between the army and civilian spheres.

The following provides an in-depth analysis of the crisis between former Defense Minister Ehud Barak and former IDF Chief of Staff Gabi Ashkenazi, preceded by an analysis of the source of the conflicted relations between the military and the Chief of Staff.

Crises in Relations between the Political and Military Echelons in Israel

In the summer of 2010, the Prime Minister and the Defense Minister notified then-IDF Chief of Staff Gabi Ashkenazi that they intended to declare Order P+30 on the Iranian question. This meant that Ashkenazi had to prepare the military for an attack on nuclear facilities in Iran within 30 days. Ashkenazi, supported by heads of the Mossad and the Israel Security Agency (ISA), opposed the measure. As Mossad head Meir Dagan said: "P+30 is not something that can be kept secret. After five days, reserves must be called in and supplies of blood transfusions, fuel, and ammunition must be ensured. There isn't an intelligence organization in the world that wouldn't pick up on it."[13] The security officials told the politicians

that the very commencement of such measures would inevitably bring about an Iranian response, and create a chain of unavoidable reciprocal steps that would cause the outbreak of war, without any explicit decision being made in advance. Netanyahu and Barak were also faced with an argument of constitutional nature: decisions of this kind must be made by the government, or a cabinet authorized by the government–not the Defense Minister, or even the Prime Minister. As the head of the IDF, the Chief of Staff was therefore not obligated to do as asked.

The second event that occurred at that time was coined the "Harpaz Affair," and attracted significant media coverage. In his description of the affair, the State Comptroller wrote, "In the State of Israel, where the security establishment is an existential system and part of the national ethos, trust in the heads of the security establishment must not be undermined by bitter relationships that have deteriorated to the point of loathing and mistrust."[14] His language was restrained in comparison to other descriptions. Senior commentators in Israel, quoting the Defense Minister himself, referred to a "colonels' rebellion."[15] On February 2, 2011, he appeared on television and accused the serving Chief of Staff of having "severe professional and ethical issues."[16]

Later, in a conversation with the State Comptroller, Barak described Ashkenazi's actions as "a putsch... illegal action... deliberately subversive and unilateral measures were employed to damage the Defense Minister."[17] In a court affidavit filed by the Defense Minister on August 13, 2013, he accused Ashkenazi of "an action against the political echelon through criminal behavior," describing his conduct as being "in violation of the criminal code, the Basic Law: The Military, the norms of command, and the spirit of the IDF."[18]

The accusations voiced by the Chief of Staff and his supporters against Barak were no less severe. From their perspective, what happened was not a putsch by the Chief of Staff against the Defense Minister; it was a putsch by the Defense Minister against the government.[19] According to Ashkenazi and his supporters, Barak assumed a level of authority that is only given to the entire government, and following the failure of this endeavor, he began a campaign "designed to target a serving Chief of Staff... The conduct of Barak and his office was based on his plan to cause the Chief of Staff to either resign or to end his term battered and worn-out."[20]

Israel's political history is replete with cases of friction between the political and military echelons. On numerous occasions, Defense Ministers have been on the verge of dismissing the Chief of Staff for this reason, including Defense Minister Ezer Weizman and Chief of Staff Mordechai (Motta) Gur in 1977, and Defense Minister Binyamin Ben-Eliezer and Chief of Staff Shaul Mofaz in 2001. On both occasions the Prime Minister restrained the Defense Minister. Nevertheless, the Iranian event and the "Harpaz Affair" are different, culminating in a true crisis. In these two cases, not only did the military object to the government's policy, but they also entailed a conflict over the principles regulating the relations between the military and the government. According to Yehuda Ben Meir, "the relations between the Prime Minister, the Defense Minister, and the Chief of Staff are slippery... they occasionally cause improper behavior by, or power struggles between these officials."[21] Over the past two decades, research regarding the friction between the two echelons has reached a point of saturation, as the recommendations did not differ from those first mentioned by the Agranat Commission.

This Commission, examining the failures of the Yom Kippur War, indicated in its 1974 report that there is no clear definition of the division of authority between the Prime Minister, Defense Minister, and Chief of Staff. In Section 17 of its partial report, the Commission stated, "the lack of definition of authority prevailing in the existing situation in the field of defense, a field second to none in its essentiality, diminishes the effectiveness of operations, detracts from the focus of responsibility, and also causes a lack of clarity and confusion among the public." The Commission, however, merely made a recommendation in principle about the need to define the authority and responsibility in the law, and did not propose a detailed and clear format for doing so.

Following the publication of the Agranat Commission's recommendations, the Knesset enacted Basic Law: The Military, 1976. The law's provisions state, "the military is subject to the authority of the government" and "the Minister in charge of the military on behalf of the government is the Defense Minister." This basic law defines the status of the Chief of Staff as "the supreme command level in the military... subject to the authority of the government and subordinate to the Defense Minister," and nothing else. The new law failed to eliminate ambiguity in the definition of that authority and responsibility within the political echelon, as well as the

relations between the political and military echelons. Consequently, it did not prevent further frictions that led to other commissions of inquiry, such as the Winograd Commission that investigated the war in Lebanon in 2006.[22]

While the ambiguity has persevered and facilitated the incidents mentioned above, the correct question has yet to be asked and answered: why has nothing been done to right this wrong? How is it possible that the few initiatives for change did not emanate from the political establishment, but rather from the judicial system or academia? And when such a political initiative existed, why did it fail to yield results?[23]

This article discusses the unanswered question as to the reason for the lack of real initiative to alter the situation and clear the ambiguity. The discussion will focus on two key players in the arena: the Chief of Staff and the Defense Minister, who most clearly represent the friction in the interface between civilian and military spheres, and between the government and the military.

The Institutional Explanation for the Crisis: The Structure of the Government Coalition

Israel's constitutional structure is at the root of the friction between the military and the political echelons; the multi-party coalition government creates a situation in which the military has no single commander in chief. In addition, aside from the guiding principle adopted from the pre-state era according to which the military is subordinate to the elected civilian political institution, there is no concrete delineation of the nature of this subordination. Unlike the US or France, in which the president is the armed forces' commander in chief; Germany in which the Minister of Defense (or at times of crisis the Chancellor) is the armed forces' supreme commander; or the UK, Greece and Spain in which the military is subordinate to the Prime Minister, the Israeli military is subordinate to a collective entity rather than a single official.

The multi-party coalition structure in Israel sets the stage for tension between and within political parties, and this tension does not skip the military. The situation is even worse in cases in which the Prime Minister and Defense Minister are not from the same party. During the country's first years, its Prime Minister David Ben Gurion also served as Minister of Defense. The IDF Chief of Staff, therefore, had no question as to his supreme commander. When in 1953 the positions were filled by two different people,

friction and chaos emerged, as noted by Moshe Sharett, Ben Gurion's first (and temporary) successor as Prime Minister, in his diaries.

When the leader of the largest party in the government wields great political power in his party and in the coalition, he will usually choose to fill both positions. This was the case with Ben Gurion in the 1950s; Levi Eshkol after 1965; Menachem Begin in the short period after Ezer Weizman left the government in 1980; Yitzhak Rabin in 1992; and Barak in 1999. A more frequent pattern, however, is that in which the governing party is not strong enough to enable the party leader to demand both positions. As Prime Minister, Eshkol was forced to relinquish the position of Defense Minister to Moshe Dayan, and Prime Minister Yitzhak Shamir from the Likud had to appoint Rabin from the Labor Party as Defense Minister.

The same situation prevails when the Prime Minister is forced to include his party rivals in the center of political power, as happened in the Likud with Begin and Weizman, and later with Ariel Sharon, and in the Labor Party with Rabin and Shimon Peres.

In contrast to the multifaceted government composition, the IDF's leadership is extremely centralized, awarding the Chief of Staff significant organizational and operational power, extending beyond that of his counterparts in other countries.

Every committee of inquiry established following a crisis in relations between the military and political echelons indicates the ambiguity and multifaceted nature of the military's civilian oversight. According to Basic Law: The Military, there is no question as to the military's subordination to the government; ambiguity arises, however, as to the Prime Minister's status vis-à-vis the military. The Prime Minister is not mentioned in the law at all. To this extent, the Agranat Commission reflected the norm according to which the government as a whole holds the highest level of executive authority, and each minister is held accountable for the government's activity.

The definitions set forth in the law do not take into account an imbalance in the government-Prime Minister-Defense Minister triangle in which the Prime Minister's power exceeds that of the other two. For example, several days following Prime Minister Levi Eshkol's abdication of the Defense portfolio in May 1967, the new Defense Minister Moshe Dayan directed the Northern Command to initiate an offensive in the Golan Heights, thus circumventing the Chief of Staff and undermining the Prime Minister. As a result, Minister Yisrael Galili formulated a document dubbed "the

constitution" delineating the military operations that require approval from the Prime Minister.[24]

While at any given time operations outside the borders of Israel require the Prime Minister's approval, there are some instances in which the Prime Minister may decide to limit the Minister of Defense's authority. Thus, in the First Lebanon War in 1982, when Prime Minister Begin felt that Defense Minister Ariel Sharon was misleading the government, Begin deprived Sharon of his authority to order the Air Force into action. To this extent, in light of the tension between his predecessors Prime Minister Rabin and Defense Minister Peres, Ehud Barak assumed both positions when he became Prime Minister. "I'm embarking on a controversial peace process, so I want to be confident that I have full control over the military, and that I am not dependent on a Defense Minister who can play independent political games against me," he said.[25]

The balance of power within the government is more complex, because the leaders of other parties in the coalition want to be in a decision making position when defense is involved, and demand cooperation from the Prime Minister in such decisions. None of them wants the Prime Minister's status and authority to be cemented in binding legislation; the ambiguity is convenient. In a situation like this, they can obtain power in practice, while at the same time avoiding responsibility in the event of failure.

What Authority Does the Defense Minister Wield?

No less complicated is the affinity between the two echelons, first and foremost the status of the Defense Minister vis-à-vis the Chief of Staff. Under the Basic Law: The Military, the Defense Minister is in charge of the military on behalf of the government, and the Chief of Staff is subordinate to him. But what does this subordination mean? According to the accepted interpretation of the law, the Defense Minister has no independent status; his status is derived from the government as the minister supervising the military on the government's behalf. The Defense Minister is like a pipeline between the government and the military. He speaks to the military in the name of the government, and communicates what the military has to say to the government, without detracting from the government's authority to act directly vis-à-vis the military.[26]

Although the Basic Law: The Military was enacted following the Yom Kippur War, there is no agreement on the status of the Defense Minister and

the nature of the Chief of Staff's subordination to him. Various interpretations of the law award different degrees of involvement in military affairs, and this is what underlies the many disputes between the Chief of Staff and the Defense Minister. This dilemma was first discussed in a document written by former IDF Military Advocate General and later Supreme Court Justice Hanan Meltzer as a special opinion on November 4, 1977.[27] In the section about relations between the Chief of Staff and the Defense Minister, Meltzer wrote that there were three approaches to the concept of subordination that correspond to three different levels of intervention: absolute subordination, strategic subordination, and relative subordination.

According to the absolute subordination approach, the Chief of Staff is subordinate to the Defense Minister at every level of the military's activity. The minister's authority over the Chief of Staff is the same as the government's authority in regards to both power and scope. He is entitled to intervene and order the Chief of Staff to act in any way he wishes: not only in matters of a strategic nature, but also in tactical and operational matters. According to this version, this is the reason for the use of the term "supreme command level in the military" for the Chief of Staff instead of the term "the military's supreme command level," meaning within the military, but not above the military. At the same time, this regulation also means that the Defense Minister does not given orders to IDF soldiers other than through the Chief of Staff.[28]

Opponents of this approach argue that absolute subordination of the Chief of Staff to the Defense Minister renders the law's provision that the Chief of Staff is the supreme command echelon in the military meaningless. In their opinion, the correct approach is the strategic subordination approach. This version holds that the Chief of Staff is subordinate to the Defense Minister only in matters of political and strategic significance; in all other matters, the Chief of Staff is authorized to act according to his judgment. Otherwise, the advocates of this semi-restrictive approach believe the minister will be exactly what the Agranat Commission did not want him to be: a super-Chief of Staff. This is particularly important in Israel, because Defense Ministers are often former chiefs of staff, and as such tend to intervene excessively in regular management of the military.

In practice, the military establishment has always operated according to a third, in-between approach, favoring the principle of relative subordination. Under this approach, the Chief of Staff's subordination to the Defense

Minister is absolute in strategic matters, but the minister has only the power to approve or oppose in tactical-operational matters; he cannot initiate or impose his opinion. This approach, however, is not explicitly stated in the law, or even in documents having constitutional weight. The unstable, evasive, and vague character of this arrangement has therefore created a wide opening for misunderstandings, and allowed negotiations and power games between the Chief of Staff and the Defense Minister.

The ambiguity resulting from the state of relative subordination is more convenient for both sides, especially in a prolonged war, such as the Arab-Israeli conflict. For example, if a decision about war requires approval at the government level, what about military action that is less than full war, such as a "war operation"? Ambiguity enables the Prime Minister to act without government constraints.[29] This is even more prominent in a low-intensity conflict in which the traditional boundaries between the civilian and professional echelons are blurred.

Ambiguity in Relations among the Leadership

Friction between the Chief of Staff and the Defense Minister or Prime Minister over policy has attracted a very large degree of public scrutiny. Two examples are then-Chief of Staff Shaul Mofaz's opposition to then-Prime Minister Ehud Barak's decision to withdraw from Southern Lebanon in 2000, and then-Chief of Staff Moshe Ya'alon's lack of support for then-Prime Minister Ariel Sharon's plan to withdraw from the Gaza Strip in 2005. The history of relations between the Chief of Staff and the Defense Minister, however, is replete with disputes on many other questions, with the Chief of Staff endeavoring to carve out autonomy in regular operation of the military, while for his part, the minister seeks to deepen influence on the military.

The relations prevailing in practice between the Defense Minister and the Chief of Staff prove the penetrability of each player's area of operation, and how far the formal legal situation is from reality. For example, the Chief of Staff customarily communicates with officials outside the military not through the Defense Minister, while the Defense Minister communicates with officers in the military not through the Chief of Staff. When Barak became Defense Minister in Ehud Olmert's government in 2007, he ordered the Chief of Staff to discontinue the tradition of having a personal meeting with the Prime Minister once every two weeks. Olmert opposed Barak's position, but could not enforce his opinion on his minister. Instead, he

barred the heads of the Mossad and the ISA, who were directly subordinate to him, from participating in the regular weekly meetings conducted in the Defense Minister's office, and ordered them to send only junior officials to these discussions. Barak understood the message, and retracted his order.[30]

The gap between the law and reality is particularly conspicuous with respect to the Prime Minister's status. How is it possible that the Basic Law: The Military does not mention him at all, even though his role is self-evident? After all, he has the supreme authority in security matters; controls the ISA and the Mossad; decides on differences of opinion between the Minister of Finance and the Defense Minister on the defense budget; approves certain operational actions; and brings the appointment of the Chief of Staff to the government. Why have Israeli Prime Ministers refrained from demanding that their status be explicitly anchored in law, even though "a constitutional practice of also subordinating the Chief of Staff to the Prime Minister has been created"?[31]

The reason is that the ambiguity allows the Prime Minister more flexibility and greater maneuverability in the use of the defense apparatus. It is convenient for the Prime Minister to have someone serve as a pipeline to the military, and who bears direct responsibility for it. This is true when the Prime Minister does not have professional authority, and can rely on the prestige of a minister among the senior officer corps, as was the case in Netanyahu's first government, and even more so in his second government. In his bargaining with the military, in situations requiring difficult decisions liable to exact a high political price, especially in cases of failure, the Prime Minister prefers to deal with the military through a mediator. He can then disavow responsibility, and claim that someone else is responsible–the Defense Minister.

The vagueness in defining the nature of the subordination relationship is convenient for the Prime Minister. The Prime Minister's ability to affect the appointment of the Chief of Staff enables him to bring about the appointment of a candidate who is closer to him than to the Defense Minister, thereby detracting from the latter's control and strengthening the Prime Minister's position vis-à-vis the Defense Minister, without the constraints of a formal definition. For example, Prime Minister Eshkol preferred to appoint Haim Bar-Lev, who was politically close to him, as Chief of Staff, against the wishes of Defense Minister Moshe Dayan, who preferred Ezer Weizman.

The ambiguity also serves the political interests of the Defense Minister. When his power and authority rest on appreciation of his professional capability, he does not need to fear any competition from the Prime Minister or the Chief of Staff (Defense Ministers Dayan, Rabin, Sharon, and Barak, who were all called "Mr. Security," all enjoyed such status). A state of ambiguity, however, enables the Defense Minister to evade responsibility when it is convenient for him. He will then defend himself by saying that his authority is limited, not absolute. That was the main argument by which Moshe Dayan saved himself from a deadly verdict by the Agranat Commission for the Yom Kippur War debacle. He said that all he did was give the Chief of Staff "ministerial advice." In Israeli political culture, this concept has become a notorious expression epitomizing the evasion of political responsibility.

The Chief of Staff also benefits from the rather undefined authority of the Defense Minister above him. In situations in which the minister has no professional military standing, the Chief of Staff can easily expand his maneuvering room. This was the case with Defense Minister Binyamin Ben-Eliezer and Chief of Staff Shaul Mofaz, and with Defense Minister Amir Peretz and Chief of Staff Dan Haloutz. The Chief of Staff can also appeal the Defense Minister's decisions to the Prime Minister, thereby reinforcing his status and making it in effect almost equal to that of the Defense Minister. The Chief of Staff's political proximity to the Prime Minister, if it exists, will further improve his standing. For this reason, Defense Ministers have objected to direct meetings between the Chief of Staff and the Prime Minister, as happened with Barak and Olmert.

Ambiguity is not limited to the top level of the defense establishment; it is a prominent feature of Israeli political and organizational culture. Politicians have always preferred flexibility, even procedural lack of clarity, to precise definitions that put them into a straitjacket of binding constraints. In Israel, ambiguity is used as a "political lubricant."[32] In analyzing Israeli strategic culture, Dmitry Adamsky determined that, "egalitarian social norms set by the founders of the State have created extreme patterns of informal behavior and a lack of attention to hierarchal norms. This stems from the fact that Israel is a society with 'small power gaps,' that is, extremely narrow distances in superior-subordinate relationships."[33] One aspect of this characterization is that it encourages a plethora of ideas that originate in the lower echelons and grow upwards through informal

organizational shortcuts; the other aspect is the ambiguity in relationships between managerial levels.

Although jurists and members of academia, as well as military officers and politicians, have argued that the ambiguity inherent in Basic Law: The Government is not conducive to healthy governance, the situation suits the general pattern of behavior in the Israeli public sphere, and the top political and defense echelons have had no real interest in changing the law. They preferred to leave the state of affairs as is–until the next crisis erupts, as happened in Lebanon in 2006.

Following that war, an investigative commission headed by Justice Winograd was appointed, and no one was surprised when its final report, published in January 2008, included recommendations for improvement in decision-making processes within the political echelon. On page 578, the Commission's report reiterated what is by now virtually a cliché: that the present situation must be corrected, inter alia, by "clarification of the authority and responsibility of the political echelon and the security echelon, and the interface between them."[34] Several of the Commission's recommendations were actually implemented, and a few heads did indeed roll, but with regard to the division of authority between the Chief of Staff and the Defense Minister, and within the military and the political echelons, once again nothing was done.

The Barak-Ashkenazi Confrontation

Thus, by the end of the first decade of this century, the state of the national security system had reached a low point worse than any of the crises in Israel's history: the revolt of the generals during the War of Independence, the Lavon Affair, the failure in the Yom Kippur War, and the Israel Security Agency's Bus Line 300 incident. The State Comptroller described the relations between the Defense Minister and his office and the Chief of Staff and his office as "bitter and charged," and in his final report repeatedly emphasized the damage that the two officials had caused each other, and to the entire security establishment over a two-year period.

The Harpaz Affair relates to a document of instructions allegedly written in the Defense Minister's office designed to influence the selection of the next IDF Chief of Staff by tainting the image of Chief of Staff Gabi Ashkenazi and General Benny Gantz, while at the same time shaping a positive image for General Yoav Galant, the candidate chosen by Defense

Minister Barak. Following the publication of the document on prime time television news show, it was discovered that Lt. Colonel (res.) Boaz Harpaz, who was close to the Chief of Staff, had, over a period of time, collected information intended to cause damage to the Defense Minister and those close to him. However, it also became clear that the appointment of the Chief of Staff was merely one in a series of severe disruptions to the working relationship between the two.

At the same time, it also became evident that the Chief of Staff's improper behavior was a response to the Defense Minister's ongoing undercutting of his position, undermining his authority, and sabotaging his ability to lead the IDF. Examples of this included the appointment of senior military officers by the Defense Minister (including the deputy Chief of Staff and the IDF Spokesperson, among others) against the Chief of Staff's will, and even without his knowledge; delaying the appointment of hundreds of other senior officers for many months; refusing to approve important Supreme Command Orders concerning the mission and function of several of the directorates in the general staff; preventing the Chief of Staff from meeting with civilian officials; barring various civilians from appearing before the military, despite approval by the Chief of Staff; and–for the Chief of Staff, the casus belli–initiating a round of interviews of candidates for the position of Chief of Staff many months before the usual time, in order to turn the incumbent Chief of Staff into a lame duck. The Comptroller detailed this behavior in his report, and did not hesitate to condemn the Defense Minister.

Throughout this period, senior officers were actively involved in the conflict between the Defense Minister and the Chief Staff. The case of IDF spokesperson Brigadier General Avi Benayahu is particularly striking, because he has been accused of acting against the Defense Minister while in uniform.[35] Indeed at all stages of the affair, the two camps tried to influence public opinion by means of systematic leaks, including classified material; fought over publication of press releases; published photographs and announcements designed to damage the Chief of Staff, the Defense Minister, or their associates; blocked the participation of officers belonging to the other camp in essential meetings; and refrained from orderly briefing of senior officers about regular conclusions and decisions pertaining to their areas of responsibility. It is no wonder that the situation prevailing

at the time has been described as the "worst crisis of leadership in the history of the IDF."[36]

This was a clear effort by the Defense Minister to undermine the Chief of Staff's status and his ability to function, so that he would resign from the IDF. For his part, the Chief of Staff defended himself against the Defense Minister by undermining his status and authority and by pushing him out of decisions and decision-making forums in the IDF. Ashkenazi attempted to thwart the Defense Minister's plans for the appointment of the next Chief of Staff, and ultimately tried to change the Basic Law: The Military in order to rein in the Defense Minister's authority by making the Chief of Staff directly subordinate to the government.

The Israeli media covered the drama known as the "Harpaz Affair" for more than two years. Most of the Comptroller's report also dealt with various aspects of the campaigns conducted by the Defense Minister and the Chief of Staff against each other. Only a small part of the report, however, featured a story almost completely ignored by the media, even though in principle its importance far outweighed the other aspects of the affair: the instructions of the Supreme Command Orders: General Headquarters. More than anything else, this incident reflects the structural crisis in relations between the military and political echelons in Israel, and the attempt by each of these parties to shape a different structural, functional, and legal meaning for these relations.

In the face of the fierce enmity between them and the Defense Minister's ongoing attempts to constrain his power and position, Ashkenazi tried to improve his position by redefining the relationship between the Chief of Staff and the Defense Minister. Since the Knesset, the legislative branch, refused to deal with this matter, the Chief of Staff decided to take action where he could: within the military, through an amendment to the General Headquarters section of the Supreme Command Orders, which according to military law are the "general orders issued by the Chief of Staff and approved by the Defense Minister, intended to determine the principles related to the military's organization and administration, regime and discipline therein, and to ensure its proper operation."

Already in early 2008, before relations between the Chief of Staff and the Defense Minister deteriorated, Ashkenazi ordered the preparation of the new order. The staff work took two years to complete. The new order was approved by the Chief of Staff in October 2009 and by Barak in November

2009, after which it was distributed to IDF units. This critical event took place without the knowledge of the public, or even of the political echelon, other than the Defense Minister, even though it determined the principles governing the status of the Chief of Staff and the Defense Minister with respect to each other and vis-à-vis the government.

In January 2010, as the relationship between Barak and Ashkenazi further deteriorated, the Defense Minister retracted his approval of the new wording of the order. In March, his office issued a directive ordering its immediate annulment. For the next year, the offices of the Defense Minister and the Chief of Staff contested the legality of its preparation, not the contents of the directive, especially the legality of the minister's annulment order. A large proportion of the State Comptroller's report also concerned the procedure of the order's drafting and annulment, not its content, and contained severe criticism of the Defense Minister. The dispute between the Defense Minister and Chief of Staff over the division of authority between them highlights the inherent problem around which our analysis is centered.

The new version of the order defines the Chief of Staff as "the commander **of** the military" instead of "the supreme command level **in** the military." The government was defined as the supreme command level, to which the Chief of Staff was subordinate. As strange as it may seem, the Defense Minister was not mentioned at all in the order. There was a good reason why Barak wanted to change the wording by replacing "commander of the military" with "the supreme command level" and replacing the phrase "The Chief of Staff is responsible for translating the decisions of the highest political echelon into operative military action" with "responsible for translating the decisions of the Defense Minister, who is in charge of the military on behalf of the government, into operative military plans of action."

The IDF Military Advocate General, representing the Chief of Staff's point of view, opposed this. He contended that the version prepared by the IDF Planning Directorate did not contradict the Basic Law: The Military, and proposed a compromise that essentially entailed a return to the previous state of ambiguity before the initiative to change the provisions of the Supreme Command Order–General Headquarters. He proposed that instead of stating that the Chief of Staff "is responsible for translating the decisions of the political echelon," a compromise wording would be used: "... translate the government's decisions and the decisions of the Minister

of Defense in charge on behalf of the government." Barak also objected to this, however, and ordered the immediate annulment of the order.

As noted above, it was at this stage that the dispute between the two bureaus over the Defense Minister's cancellation notice began in earnest. However, the battle was actually over the position of the Defense Minister vis-à-vis the Chief of Staff and the government. In testimony provided to the State Comptroller in early November 2011, Yoni Keren, director of Barak's offices, explained the Defense Minister's position by stating, "The facts show that for a long period of time… the Chief of Staff has adopted views detaching him from the Defense Minister, was not adhering to the Basic Law: The Military, and for all intents and purposes, has appointed himself as a commander in chief of the military who has no need for a Defense Minister. These actions have no place in a democracy."

According to Keren, the contention that the Chief of Staff is directly subordinate to the government as a whole "undermines the authority of the Defense Minister, while eliminating the link between the Defense Minister and the IDF… The Chief of Staff is upgrading his status from head of the general staff to the commander of the military, thereby removing the Defense Minister from the entire equation." Koren also attacked the constitutional change that the Chief of Staff had made in the military, saying that these issues were province of the legislative branch. "This means that the Supreme Command order amends the Basic Law: The Military, and effectively creates a situation in which the IDF seems to be above the law, and does not need the Knesset in order to change legislation."[37]

As expected, the Chief of Staff's position was diametrically opposed. As stated in his testimony before the Comptroller and his supporters' media appearances, the amendment was made in order to improve the military's functioning and efficiency, following lessons learned from the Second Lebanon War. It was asserted that the process of preparing the order was entirely correct. As evidence, they emphasized that the amended order had been forwarded to the Defense Minister's offices, and that Barak had fully approved them. It was therefore the Defense Minister who had acted inappropriately, first by rescinding his approval, then by issuing instructions to cancel a legal order. Furthermore, they contended, he had done these things as part of the war he had declared on the Chief of Staff, and with the intent of injuring the latter, diminishing his professional standing,

making it difficult for him to command the IDF properly, and constraining his ability to function within and outside the military.

An impartial interpretation, such as in the State Comptroller's report, can easily provide a complete picture. It is clear that the original formulation excluding the Defense Minister from the order went too far in its interpretation of the law. However, it seems as though the Chief of Staff's unwillingness to accept the minister's position was a defensive act; he felt as though the Defense Minister was hindering his ability to command the military, trying to force him out of the military.

Barak's motivation is related to the main theme of this paper: the nature of the Israeli political game. Barak felt that the public gave popular Chief of Staff Ashkenazi credit for rehabilitating the military after the Second Lebanon War, that Ashkenazi had made even greater political strides following Operation Cast Lead in Gaza, and that these gains by Ashkenazi were at his expense, as Barak was losing his luster in public opinion. This was therefore a head-to-head battle for the "Mr. Security" title–a zero sum game in which the success of one side depended on the defeat of the other–even if it involved targeting a uniformed officer on one hand and undermining a ministerial superior on the other.

Barak assumed that Ashkenazi intended to convert his public support into political capital upon retiring from the military, and that he would join the Labor Party, perhaps even become party leader as an alternative to Barak, who was losing his grip on the leadership. Barak therefore believed that he had to block this ambitious officer before he could realize his plans. The first step was to tarnish his reputation by cutting his period of service short and forcing him to leave the military "battered and worn out." Does this sound familiar? Prime Minister Netanyahu used the same rationale in his relationship with popular Chief of Staff Amnon Lipkin-Shahak.[38]

When the Harpaz Affair continued to attract the media's attention, the Attorney General ordered the police in the summer of 2013 to begin a criminal investigation of the episode, and many more details about the tangled relations between the security leadership under Barak and Ashkenazi were disclosed. When this article was written, the affair remained unresolved, but the state of legal and political ambiguity at the top of the defense establishment remains unchanged.

The Political Nature of the Chief of Staff Position

The position of Chief of Staff is inherently political, because it affects the political, social, and economic spheres, in addition to the very broad security sphere. Four aspects of Israeli reality make this fact more salient: the perpetual state of war or preparation for war; the "military-political partnership" nature of the relations between military and government; the asymmetric wars in which Israel is involved which emphasize this relationship pattern; and the fact that the military is involved in the country's key political issues–responsibility for the territories, defending their Jewish residents and managing the Palestinian population.

As a result, the position of Chief of Staff has traditionally been filled by officers with a political orientation, including Moshe Dayan, Motta Gur, Ehud Barak and Moshe Ya'alon. In addition, the intense involvement in national politics may, at times, entice ostensibly a-political officers to join politics, as did Amnon Lipkin-Shahak, Rafael Eitan and Shaul Mofaz. Indeed, 13 out of 19 Chiefs of Staff have embarked on a political career following the end of their military career.

Compatibility or conflict between the political interests of the Defense Minister and the Chief of Staff is therefore one of the most crucial factors in the quality of their relationship. If their interests are in conflict, as was the relationship between Barak and Ashkenazi, the situation is more likely to result in serious friction. In contrast, as Chief of Staff, Barak's political aspirations did not threaten Defense Minister Rabin, and their political proximity encouraged Rabin to look favorably upon his Chief of Staff. If the Prime Minister is more dominant than his Defense Minister, the same principles also apply to relations between the Prime Minister and the Chief of Staff.

In his first term, Prime Minister Netanyahu felt alienated from the senior IDF leadership, whom he viewed as cooperating with the Labor Party. He was especially concerned, unjustifiably so, that popular Chief of Staff Lipkin-Shahak would compete against him in the political arena, and therefore employed various tactics exhibiting disdain, even hostility, towards the Chief of Staff, such as refusing to meet in the course of regular work. As a result, Lipkin-Shahak, initially devoid of political aspirations, stated that he had decided to embark on a political career in order to put an end to the rule of Netanyahu, whom he regarded as a danger to Israel. Relations of distrust also prevailed between Sharon and Chief of Staff Ya'alon.[39]

In Israel, the military is a highly valuable resource for political capital, status, and prestige. As a result, the battle between political players for involvement in defense matters is intense–it is a struggle to make political gains of military achievements, and avoid blame for military failures. This battle determines political fates (see the success stories of Dayan after the 1956 Sinai campaign and Rabin after the Six Day War in 1967, in contrast to Sharon's failures following the first Lebanon War in 1982 and Dan Haloutz's failures following the Second Lebanon War in 2006). For this reason, control over the defense sphere has great potential for becoming a source of tension between the Chief of Staff, who may later become a politician, and the Defense Minister, to whom the Chief of Staff is currently subordinate.

In Israel's first years, the loyalty of officers with potential to become Chief of Staff was also assessed according to their political affiliation. It would be a mistake, however, to assume that considerations of loyalty have disappeared in the early 21st century with the decline of Israel's polarized political parties. Politics have changed, and are now much more personal. Knowing that Chief of Staff Ya'alon objected to disengagement from the Gaza Strip (even though he would obviously perform the task if entrusted with it by the political echelon) led Defense Minister Mofaz (as an agent of Prime Minister Sharon) to instigate Ya'alon's dismissal, and replace him with Haloutz, an officer more acceptable to him and close to Sharon's inner circle, popularly known as "the forum on the ranch"–the kernel of Sharon's camp.

Section C in Basic Law: The Military states, "the Chief of Staff shall be appointed by the government in accordance with the Minister of Defense's recommendation." Yet, once again, we see that the definition is ambiguous. The law does not even mention the Prime Minister, despite his decisive influence over the procedure. After all, in the final analysis, it is the Prime Minister who will bring, or decide not to bring, the appointment to the cabinet for approval, and can therefore force his opinion on the Defense Minister. According to tradition, although the exiting Chief of Staff has no formal standing in the Defense Minister's decision, great weight is given to his opinion. Disagreement between them is liable to create a protracted struggle that can at times have a negative impact on the military. That is exactly what happened when Ashkenazi objected to Barak's attempt to

appoint Yoav Galant as his successor, a bone of contention that became the basis of the Harpaz Affair.

Conclusion: The Nature of Political-Military Interdependence

Since it is very difficult to foresee any change in the coalition character of Israel's governments or in its political culture, in which the government constitutes a theater for power struggles between the coalition partners, there is also little reason to expect any reform in the relationships between the military and political echelons. The division of authority within the political sphere–government, Prime Minister, and Defense Minister–will persist. The ambiguous definitions of the military's relationships with the government will also remain unchanged. For these reasons, there will not be any changes in the relationship between the Defense Minister and the Chief of Staff. The interests of the Defense Minister and the Chief of Staff in preserving the ambiguous relationship will remain, as they compete for power in maneuvers that can easily deteriorate into a "balance of terror."

This balance is rooted in the fact that the government needs legitimacy in the eyes of those in uniform. As former deputy Chief of Staff and deputy Defense Minister Matan Vilnai once put it, "the political echelon is dependent on the military echelon. It cannot move without the military; it is needed for public legitimacy and for coping with challenges in the field."[40] On the other hand, senior officers are subject to the good graces of the politicians, on whom they depend for their professional advancement. As former minister Yossi Sarid observed, "the political echelon has one clear point of strength that gives it an advantage over the military echelon and provides leverage for action. The political echelon appoints senior officers, promotes them, and can also suspend or damage their careers. Since officers naturally want to get ahead in life, the military echelon relies on the good will of the political echelon, and tries not to anger it. After all, who wants an officer who is a troublemaker?"[41]

An abundance of recurring recommendations by various investigative committees, private bills, academic publications, and editorials in the media have all called for reforming the present system. They spell out the advantages for both the military and government with regard to decision-making processes and Israel's overall security policies. But these are no match for the fundamental interests of the major protagonists.

The ambiguity in the relationships between the Defense Minister and the Chief of Staff subordinate to him stems from both constitutional structure and political culture, which create a background that was conducive to conflict between Barak and Ashkenazi: a conflict between a Defense Minister who made every effort to intervene intensively in the IDF because his political stature was facing a critical historical test and a Chief of Staff at a critical stage in building his political future. That crisis blew over because both of them vacated the scene, but the conditions for the next crisis remain.

Because the nature of neither civil-military relations nor the political culture will change in the foreseeable future, it is very doubtful whether civilian oversight of the military can be improved. If so, is not reform on the military side of the equation worthy of consideration? Should we not upgrade the political training given to senior officers, deepen their political awareness, and give them better training in political knowledge? These questions call for a very serious and close examination.

Notes

1 Amos Gilboa, *Mr. Intelligence* (Tel Aviv: Yediot Ahronot, 2013).
2 Personal interview, 1977.
3 Moshe Ya'alon, *Derekh Aruka Ketzara* (A Long Short Road) (Tel Aviv: Yediot Ahronot–Hemed Books, 2008).
4 Kobi Michael, "The Dilemma behind the Classical Dilemma of Civil–Military Relations," *Armed Forces and Society* 33, no. 4 (2007): 518-46; and Kobi Michael, Between *Militarism and Statesmanship in Israel* (Tel Aviv: Tel Aviv University, 2008).
5 For example, see Alon Paz, *Generals from Mars, Statesmen from Venus* (Tel Aviv: IDF Publishing House, 2010), pp. 28-33; or Charles D. Freilich, *Zion's Dilemmas: How Israel Makes National Security Policy* (New York: Cornell University Press, 2012).
6 Assaf David, "Military Civilian Relations in Israel: The Dispute and the Missing Link," *Megamot* 41 (2013): 326-40.
7 Rebecca L. Schiff, "Concordance Theory: Response to Recent Criticism," *Armed Forces and Society* 23 (Winter 1996): 277–83; L. Douglas Bland, "A Unified Theory of Civil-Military Relations," *Armed Forces and Society* 26, no. 1 (1999):7-25; Elliot Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime* (New York: The Free Press, 2003); Yoram Peri, *Generals in the Cabinet Room: How the Military Shapes Israeli Policy* (Washington DC: United State Institute of Peace, 2006).
8 Bob Woodward, *Obama's Wars* (New York: Simon and Schuster, 2010); Peter D. Feaver, *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge: Harvard University Press, 2003); Dale R. Herspring,

The Pentagon and the Presidency: Civil-Military Relations from FDR to George W. Bush (Lawrence: University Press of Kansas, 2005); Fred Kaplan, *The Insurgents: David Petraeus and the Plot to Change the American Way of War* (New York: Simon and Schuster, 2014).

9 Oren Barak and Gabi Sheffer, "The Defense Network in Israel and its Effect," in *An Army Having a Country? A New Look at Defense-Civilian Relations in Israel,* eds. G. Sheffer, O. Barak, and A. Oren (Jerusalem: Carmel Publishing House), pp. 16-44.

10 Kobi Michael, *Between Militarism and Statesmanship in Israel*.

11 Yagil Levy, "Military Contrarianism in Israel: Room for Opposition by the Chief of Staff to Politicians," *Military and Strategic Affairs* 5, no. 2 (2013).

12 Alon Paz, *Generals from Mars, Statesmen from Venus*.

13 Ben Caspit, *Evasive: Ehud Barak, the Real Story* (Or Yehuda: Kinneret Zmora-Bitan, 2013).

14 State Comptroller's Report of the "Harpaz Document" Affair, 2012, http://www.haaretz.com/print-edition/news/state-comptroller-completes-draft-report-on-boaz-harpaz-affair-1.414220.

15 Aluf Ben, "The Galant Document: as Severe as the 'Lavon Fiasco,'" *Walla*, August 18, 2010, http://news.walla.co.il/item/1723164.

16 Caspit, *Evasive*, p. 313.

17 State Comptroller's Report, 2012, p. 244.

18 Yaniv Kobovitz, "Harpaz Investigation Coming to a Close: Suspicions of Ashkenazi, Benayahu and Wiener Rise," *Haaretz*, August 14, 2014, http://www.haaretz.co.il/news/law/1.2405431.

19 Amir Oren, "The 'Putsch': Ehud Barak vs. the Government," *Haaretz*, August 25, 2013, http://www.haaretz.co.il/opinions/.premium-1.2105081.

20 State Comptroller's Report, p. 244.

21 Yehuda Ben Meir, *Civil-Military Relations in Israel* (New York: Columbia University Press, 1995).

22 Mordechai Kremnitzer and Ariel Bendor, *Basic Law: The Military* (Jerusalem: The Harry and Michael Sacher Institute for Legislative Research and Comparative, Hebrew University, 2000); Shmuel Even and Zvia Gross, "Proposed Legislation on the IDF," *Strategic Assessment* 11, no. 1 (2008).

23 As occurred in 2003 in the Knesset Constitution, Law, and Justice Committee, which discussed the "Basic Law: The Military" in the framework of the Consensual Constitution initiative (Protocol no. 112, December 5, 2003), http://huka.gov.il/wiki/index.php/ פרוטוקולים.

24 Yoram Peri, *Between Battles and Ballots: The Israeli Military in Politics* (Cambridge: Cambridge University Press, 2003).

25 Personal interview, 2003.

26 Even and Gross, "Proposed Legislation on the IDF," p. 13.

27 Hanan Meltzer, "Constitutional Aspects of Relations between the Government, the Ministry of Defense, and the Chief of Staff: A Summary of

Approaches," IDF Military Advocate General's Corps, Opinion no. 100101, November 4, 1977.

28 Even and Gross, "Proposed Legislation on the IDF," p. 14.

29 Eyal Nun, "The Legal Constraints on the Military: A proposal for reformulation of Basic Law: The Military," *Law and Military* 16 (2002).

30 Caspit, *Evasive*.

31 Meltzer, "Constitutional Aspects."

32 Ira Sharkansky, *Ambiguity, Coping, and Governance: Israeli Experiences in Politics, Religion, and Policymaking* (Portsmouth: Greenwood Publishing Group, 1999).

33 Dmitry Adamsky, *Strategic Culture and Military Innovation* (Tel Aviv: Modan, 2012), pp. 174-90.

34 Commission to Investigate the Lebanon Campaign in 2006, Winograd Commission Final Report, Volume 2.

35 As testified by officers and journalists in court. For example, see "Barak Attacks Ashkenazi: 'He Led a Group of Criminals,'" *Maariv- NRG Online*, August 14, 2013, http://www.nrg.co.il/online/1/ART2/499/162.html.

36 Dan Margalit and Ronen Bergman, *The Pit* (Tel Aviv: Kinneret Zmora-Bitan, 2012), p. 12.

37 Caspit, *Evasive*, p. 196.

38 Yoram Peri, "The Democratic Putsch of 1999," in *In the Name of Security*, M. Al Haj and U. Ben-Eliezer, eds. (Haifa: Haifa University Press, 2003), pp. 125-43.

39 Peri, "The Democratic Putsch."

40 Michael, *Between Militarism*, p. 138.

41 Yossi Sarid, "Relations between the Political and Military Echelons–A Personal View," in *Civil-Military Echelon*, ed. P. Yechezkeli (Tel Aviv: Defense Ministry Publications, 2008), pp. 117-22.

The RMA Theory and Small States

Francis Domingo

The current Revolution in Military Affairs (RMA) theory has been the focus of academics and military analysts, trying to define the role of technology in transforming military affairs during the past three decades. However, despite the vast literature on the subject, only a limited number of studies look into the implications of RMA on small states. The emphasis on great powers, as some scholars suggest, is a reflection of the fact that the broader strategic studies literature does not necessarily consider small states, as their capabilities significantly limited compared to their great power counterparts. In this context, the article argues that the relevance of the current RMA theory is dependent on the strategy employed by small states. For the purposes of this article, a small state is defined as a state that has "limited capacity to influence the security interests of, or directly threaten, a great power and defend itself against an attack by an equally motivated great power." The article is divided into three parts. The first part discusses the characteristics of the current RMA. The second part surveys the strategies that small states in employ to survive in the international system. The third part assesses the current RMA theory's relevance to the strategies of small states.

Key words: Revolution in Military Affairs, small states, foreign policy, limited military capabilities, strategic options, geostrategic predicaments

The current Revolution in Military Affairs (RMA) theory has been the focus of academics and military analysts, trying to define the role of technology in transforming military affairs during the past three decades. However, despite the vast literature analyzing this theory, there are very few studies that focus on the implications of RMA on small states. The emphasis on

Prof. Francis Domingo teaches International Studies at the Department of De La Salle University, Manila and is an incoming PhD student at the School of Politics and International Relations of University of Nottingham.

great powers is a reflection of the fact that the broader strategic studies literature does not necessarily consider the situation of small states, as they have much more limited capabilities than their great power counterparts.[1] Eliot Cohen admits that the "failure to look at the response to RMA-type capabilities on the part of weaker opponents" may have been a mistake.[2] In their influential article on "complex interdependence," Robert Keohane and Joseph Nye placed much significance on the concept of information revolution, arguing that that it will "reduce the power of large states and enhance the power of small states and non-state actors."[3] While Keohane and Nye made an important point, they were not able to sufficiently explain how small states are affected by the information revolution. Given this gap in the literature, how is the current RMA theory relevant to the strategies of small states?

This article argues that the relevance of the current RMA theory is dependent on the foreign policy employed by small states.[4] A small state, for the purposes of this article, is defined as a state that has "limited capacity to influence the security interests of, or directly threaten a great power and defend itself against an attack by an equally motivated great power."[5] The remainder of this article is composed of four sections. The first section discusses the characteristics of the current RMA. The second section defines the central research question in the context of the debates regarding RMA. The third section reviews the survival strategies employed by small states. The fourth section assesses the relevance of the current RMA theory on the strategies of selected small states.

The Revolution in Military Affairs

The RMA theory is based on the idea that substantial changes in any number of variables of war will generate changes in the entire military structure as well as its operations.[6] Proponents of the theory have provided numerous definitions; however this article accepts the definition of RMA proposed by Andrew Krepinevich: "the application of new technologies into a significant number of military systems… in a way that fundamentally alters the character and conduct of conflict."[7] Several RMAs have transpired during the course of history. A prominent example was the revolution during the Napoleonic Wars during which the French military developed and implemented dramatic technological and organizational changes (standardization and mass production of weapons, and *levée en masse,*

respectively) that allowed France to forcefully dominate most of Europe for more than a decade.[8]

Another case was the naval revolution that involved the British and French navies during the late nineteenth and early twentieth centuries, where wooden ships powered by the wind gave way to metal-hulled ships that used turbine engines. The advances in naval technology were also accompanied by doctrinal shifts that addressed the new capabilities of metal-hulled ships including more accurate weapons, greater speed, more durable armor, and additional space for supplies.[9] In previous RMAs, it is evident that the main drivers were different variables of war: organization, technology, and doctrine. To understand the current RMA, it is necessary to review its characteristics and determine the variables leading the transformation.

According to proponents of the theory, the current RMA is predominantly technical in nature and was first manifested during the 1991 Gulf War against Iraq. The key innovation behind this RMA is information processing, which is manifested in three elements: information dominance, precision weaponry, and joint-service operations. Information dominance integrates information capabilities, systems and resources to ensure command and control, battleground awareness and limit the enemy's "freedom of maneuver and action."[10] These capabilities are expected to mitigate the "fog" and "friction" of warfare, allowing military units to operate more effectively across different domains.

"Advanced precision targeting" involves the use of guided munitions to destroy specific targets. The pin-pointed nature of these strikes allows the military to dominate the battlefield while minimizing the number of casualties during an attack.[11] The doctrine of joint operations enabled by information technology is the third element of the current RMA. Joint operations are coordinated through networking, which facilitates an organizational awareness of the battleground and rapid delivery of services accessible by all units anytime. Through information technology, joint operations are globally integrated, creating a critical advantage over adversaries.[12] While powerful states are realizing the advantages inherent in the current RMA, most small states are left with the challenge of constantly upgrading their military force structures, capabilities, and doctrines just to maintain modest defense capabilities.[13]

Literature on RMA and Small States

The current RMA evolved from a unique set of geopolitical circumstances, and is designed to address specific strategic conditions. The technologies that underpin this current RMA were originally intended to provide technological solutions to the problem of a hypothetical conventional military encounter between great powers during the Cold War.[14] Despite the emphasis on great powers, scholars have offered several accounts of the relevance of the current RMA for small states.

The first explanation considers RMA as a way for small states to develop a deterrent against more powerful states. In the case of Singapore, Tim Huxley has argued that Singapore's defense posture has traditionally been based on the need to deter against threats posed by much larger neighbors such as Malaysia and Indonesia. Consequently, Singapore's leaders have emphasized the significance of exploiting technology to compensate for the lack of strategic depth and military power.[15] Similarly, James Mulvenon maintains that Taiwan's motivation to implement an RMA has been driven by the threat of military force from its dominant neighbor, the People's Republic of China. Aside from this threat, Mulvenon points out that Taiwan's efforts to develop an RMA-enabled military force has been influenced by the US-Taiwan military relationship, which has increased in scope and depth since 1997.[16] This explanation, however, is flawed because both authors failed to emphasize that the RMA efforts of both Singapore and Taiwan would only be useful if developed with more powerful allies such as the US.

The second explanation argues that engaging in an RMA is relevant to developing a forward-active defense capability. Referring to South Korea, Michael Raska argues that this state needs to have advanced military capabilities to absorb the momentum of a North Korean invasion by "trading territory for time, regrouping, and engaging in counterattack in superior strength with large-scale reinforcements from the continental United States."[17] While Raska's explanation is valid, the unique geostrategic circumstances of the case study limit its representativeness.

A third explanation can be derived from the case of Israel during the 1980s. In *The Culture of Military Innovation*, Dima Adamsky explains that to counterbalance Israel's difficulty to wage a prolonged military campaign, preventive offensive was seen by military leaders as a better strategy. Adamsky explains that advanced military technology was central to Israel's

strategy: "They demanded a sophistication of the iron fists of the IDF that would bring the offensive deep into the enemy rear. They did not ignore new technologies; they saw in them promising force and protection multipliers against enemy countermeasures."[18] This argument is valid, but again lacks the ability to generalize to other states. Israel's case is unique because it does not fit the criteria of a small state since its military capabilities are superior to those of most if not all of its neighboring states.

A fourth explanation involves the relevance of RMA for Military Operations Other Than War (MOOTW). David Betz argues that the RMA is relevant to MOOTW because the different types of operations involved, including peace enforcement, counter-narcotics, humanitarian assistance, and freedom of navigation also require advanced military capabilities to achieve operational success.[19] Betz's argument is compelling given that small states engage in more MOOTW compared to large-scale and force-on-force combat situations. A counterargument, however, is that not all small states have the capabilities and resources to acquire military technology for MOOTW. For instance, narcotics pose a significant threat to South American countries. However, small states in the region do not have the resources to obtain technological capabilities required to effectively eliminate the drug cartels. Another example is the South China Sea where small states are dependent on the US for the enforcement of freedom of movement because they do not have the means to obtain advanced maritime capabilities to defend their respective territories.

This article maintains that the relevance of RMA theory is dependent on the foreign policy employed by small states. Considering that small states implement a range of strategies, the four explanations presented by other scholars are insufficient. Before directly evaluating the relevance of the RMA theory, it is first necessary to review the existing strategies that small states employ for survival in the international system.

Strategies of Small States

Implementing an appropriate strategy is absolutely critical to the survival of small states. Since it cannot shape its environment through force, a small state must rely on a range of strategies suited to its capabilities and characteristics. In terms of military power, small states have limited capabilities for self-help. Therefore, they cannot maintain defensive operations against external threats. They are highly dependent on external

sources for weapons, and mobilize a high proportion of their military strength during conflicts, which effectively decreases their ability to engage in large-scale conflicts.

In terms of international politics, small states have a limited scope of interest and have minimal influence, if at all, on the balance of power in the international arena. Moreover, small states are depicted by some researchers as reactive in terms of foreign policy, risk averse and highly supportive of international law, norms and organizations.[20] Given these characteristics, there are four broad categories of strategies that small states employ for survival in the international system: international organizations, self-reliance, alliance building, and hedging.

International Organizations

International organizations were initially established to address the imbalance between great powers and small states by placing negotiations and disputes between states within the framework of international institutions. Despite the understanding that cooperation is advantageous to all states, literature on the subject indicates that small states tend to be more supportive of international institutions because of their inability to act independently.[21] More importantly, as Robert Rothstein points out, international organizations are essential to the strategy of small states due to: the promise of formal equality; the collective security provided by the organizations; and, the potential capacity of the organizations to restrain great powers.[22]

Self-Reliance

The limitations created by lack of resources, political influence, and military power do not prevent small states from challenging great powers based on measures of self-reliance. Diplomacy is a classic example of a self-reliance strategy; small states use diplomatic means to secure their national interests and appeal to world opinion, particularly in situations where they face violence and conflict. Diplomacy, combined with a modest military capability, will also allow small states to resist the demands of great powers. In her study of the behavior of small states during World War II, Annette Baker Fox argues that small states are capable of resisting great powers using different means including "economic, ideological, diplomatic and military measures."[23]

Neutrality is another example of a self-reliance strategy. The adoption of this strategy is premised on the assumption that the state chooses to depend solely on its internal resources without seeking any potential allies. Nevertheless, neutrality is a product of European diplomacy and has not been proven effective outside the region. The strategy's effectiveness is dependent on the credibility of the state, and permanent neutrality cannot be achieved if states are situated in a sensitive geostrategic location.[24]

Alliance Building

Developing alliances is a key strategy for small states. States form alliances for two essential reasons: to prevent more powerful states from dominating a particular region or continent and as protection from an external threat. These circumstances limit states to two options - *balancing* or *bandwagoning*. Balancing refers to joining alliances to protect themselves from states or coalitions whose greater resources could become a threat.[25] A good example of balancing was the case of Cold War where several small states in Europe joined the North Atlantic Treaty Organization (NATO) to protect their national interests from the Soviet Union.

Bandwagoning, on the other hand, refers to facing an external threat by building an alliance with the most threatening power.[26] An example of bandwagoning was the behavior of Cuba during the Cold War. Since Cuba was considered a significant threat to the US, the latter constantly oppressed the former through different methods, pushing Cuba to develop an initially weak alliance with the Soviet Union during the early 1960s, which was later consolidated through Cuba's show of support in the Soviet's invasion of Czechoslovakia in 1968.[27]

Hedging

The literature on the strategy of hedging has not been as extensive as the other strategies discussed above. Hedging, as defined by Malaysian international relations researcher Kuik Cheng-Chwee, is "a behavior in which a country seeks to offset risks by pursuing multiple policy options that are intended to produce mutually counteracting effects, under high-uncertainties and high-stakes."[28] Due to Chinese dominance in the Asia-Pacific region, several small states have chosen to adopt a hedging strategy to avoid specific alliances with other regional powers. Although there are numerous debates regarding hedging's general elements, one of the proponents of the

strategy, Evelyn Goh, suggests that the hedging behavior in Southeast Asia is based on the following measures: soft balancing, complex engagement with China, and involving a number of regional powers.[29]

Relevance of RMA

Following a review of small state strategies, the next section will evaluate the implications of RMA theory using four examples. The states were selected based on their geostrategic predicaments and dominant foreign policy strategy: Albania's dependence on international organizations, Switzerland's strategy of neutrality, the Philippines' dependence on alliances, and Singapore's strategy of hedging.[30]

Albania

Previous altercations with great powers have largely influenced Albania's foreign policy. It was conquered by Italy from 1939 to 1944; it allied with the Soviet Union from 1944 to 1961; and finally, it developed an alliance with China from 1961 to 1978.[31] Albania's dependence on an external protectorate continues to influence its foreign policy, with its heavy reliance on the US, NATO and potentially the European Union. The Government of Albania highlights three main priorities in its foreign policy: integration with NATO, increased engagements with the EU and other international organizations, and enhancing its bilateral ties with the US.[32]

Albania was one of the first states in Europe to signal their intention to join NATO after the fall of communism in the region in 1991. However, NATO initially rejected Albania's application because member states believed that it could not provide an acceptable contribution to their security. After more than a decade, Albania was invited to begin accession deliberations with NATO in 2007 and was finally accepted as a full member in 2008.[33]

The cooperation between NATO and Albania covers a wide range of aspects such as security, defense and security reform, civil emergency planning, and public diplomacy. Among these areas, only security cooperation, defense and security reform would involve advances in military technology, which is the core of the RMA theory. Albania benefits from NATO's sophisticated military equipment and training, as it deploys military personnel in conflict zones as part of the International Security Assistance Force.[34] Furthermore, RMA is also relevant to the wide-raging institutional reforms that were undertaken by the Government of Albania in

line with the requirements of obtaining NATO membership. Since Albania's objective is establishing interoperability with NATO, it had implement improvements in military communications systems, surveillance systems, maritime units, and logistics.[35]

Multilateral engagement through other international organizations is another core strategy employed by Albania. Based on this strategy, Albania plans to increase its level of participation in organizations such as the United Nations (UN) and Organization for Security Co-operation in Europe (OSCE), but its main focus is seeking membership and eventual integration into the European Union. RMA would not be relevant in this particular case since the development of advanced weapon systems and drastic improvement of member states' military capabilities is not the goal of the European Union. Although the OSCE works closely with Albania, its mission areas are focused on non-military activities, specifically promotion of democratization and the rule of law, and human rights.[36]

The government of Albania considers its relationship with the US "a special priority and of strategic and paramount importance for the country."[37] In this regard, Albania has consistently supported the Anti-Terror Coalition formed by the US in the aftermath of the 9/11 terrorist attacks through providing intelligence regarding terrorist organizations in the region. The US has reciprocated the support by providing an average of $20 million for defense training and equipment to the Albanian Armed Forces (AAP) facilitating their adherence to NATO requirements.[38] Similar to Albania's engagement with NATO, the relevance of RMA is central to its alliance with the US because of the importance of interoperability between both military forces.

Since Albania's strategy predominantly depends on international organizations and alliances, the RMA theory is certainly relevant considering that AAP will constantly have to coordinate and operate with the most advanced militaries in the world.

Switzerland

The objective of the Swiss foreign policy is "to safeguard the independence, security, and prosperity of the country."[39] This policy is based on three principles: rule of law (international law), good relations with all countries in the world (universality), and non-participation in international conflicts involving other states (neutrality).[40] Due to these principles, the Swiss

defense priorities do not include warfare, as they mainly focus on conflict prevention, collective security, and peace- supporting operations.

The Swiss identify conflict prevention as a top priority. While the strategy involves limited military operations, it requires diplomatic and communication measures more than the use of advanced weapons and information systems. Indeed, information technology can assist in providing early warning, situational awareness and increased mission success but it cannot account for negotiations, assessments and political judgments, which are necessary for conflict prevention.[41] Therefore, the relevance of RMA is limited in the area of conflict prevention.

Collective security is another main priority in Swiss strategy. The literature suggests that RMA is relevant for some collective security arrangements, particularly NATO. RMA provided the basis for NATO's Defense Capabilities Initiative addressing the organization's insufficient technological capabilities, doctrines, and organizational structure.[42] Moreover, these advancements significantly enhanced small states' defense capabilities within NATO; capabilities that some of these states could not have developed independently. However, Switzerland is a member of the OSCE and not NATO. Even though RMA can be relevant to the activities of OSCE, the theory will not have the same implications because the objectives and priorities of the organization are different from NATO. Therefore, the relevance of RMA is again limited due to its inability to account for the different strategies employed to face similar threats.

Similar to collective security, the literature on RMA acknowledges that the advantages it provides are applicable even for peace support operations. Elinor Sloan maintains that technological advancements presented by RMA are effective for peace support operations.[43] More specifically, she explains that precision-guided munitions, for example, are useful for peace operations because they can minimize collateral damage and, ultimately, casualties. Furthermore, reliable intelligence, surveillance, and reconnaissance, which are central to warfare, are necessary to determine the condition and movement of refugees in order to implement effective operations.[44] RMA is relevant to the NATO peace support operations but is not necessarily relevant to other military alliances such as the OSCE because its capabilities are different. Consequently, the relevance of RMA is limited and has not been proven relevant to the peace support operations of the OSCE in which Switzerland participates.

Overall, the relevance of the RMA to the Swiss strategy is limited because it is not inclined to develop a lethal and offensive military force. Instead, Swiss military forces are focused on conflict prevention, collective security, and peace support operations that are considered non-traditional military missions.

Philippines

Philippine foreign policy is anchored in the principles of international law, peace, equality, and justice. Its objective is to pursue an independent foreign policy through the "preservation and enhancement of national security, promotion and attainment of economic security, protection of the rights and promotion of the welfare and interest of its citizens overseas." [45] But, since the capabilities of the Armed Forces of the Philippines (AFP) are still underdeveloped, the government has prioritized the following strategies: regional cooperation and cooperative security arrangements.[46]

Bilateral and multilateral engagements with neighboring states in Southeast Asia and the Association of Southeast Asian Nations (ASEAN) in general are critical to the Philippine strategy, mainly, because of its limited resources and military capabilities. While ASEAN is not a military alliance and does not maintain any military force, the Philippines gains benefits from its diplomatic (dialogue and negotiations) and political (influence in the UN) functions. In this context, the relevance of RMA would be limited to developments in the next few decades since most of the states in the region do have the resources to drastically transform their military capabilities.

The 1951 Mutual Defense Treaty with the US is still its most extensive cooperative defensedefense arrangement. Despite complications in the security relations of both countries during the past two decades, the alliance was revitalized after the 9/11 terrorist attacks with the development of large-scale military training exercises in the country. In order to develop the interoperability between military forces, the US provided military equipment and carried out joint training programs focused on counter-insurgency, counterterrorism, intelligence training, and civic-military operations.[47]

The improvement in AFP's organizational and operational capabilities further progressed with the restoration of the Philippine Defense Reform Program and the Capability Upgrade Program, supported by the Bush Administration. Presently, with an increasingly aggressive China, the US-

Philippine alliance, under the Obama Administration, has shifted focus from counter-insurgency and counterterrorism to strengthening the AFP maritime security capabilities.[48] While this shift would not be considered a path towards dramatic military transformation in the Philippines, RMA is highly relevant to the effectiveness of US-Philippine alliance, which is one of the core strategies for the country's survival.

Given the circumstances, RMA would be beneficial for the AFP because of its dependence on US military assistance. The initiative towards improving the capabilities of the AFP is essential to ensure forces' interoperability and to strengthen the alliance. Although the Philippines also engages the support of it neighbors in Southeast Asia, these states and even ASEAN do not have the military capability to properly protect the Philippines from external threats.

Singapore

The development of Singapore's foreign policy is based on three main objectives: survival, national security, and economic well-being.[49] Due to its vulnerabilities and with China's aggressive posture in Southeast Asia, Singapore's foreign policy-makers have employed a hedging strategy that consists of a range of economic, political, and military approaches for preserving its sovereignty and national security.[50]

Singapore's economic achievements are well documented. It had an estimated GDP per capita of $51,709 in 2012, making it one of the riches countries in the world.[51] The Government of Singapore has exploited this economic advantage by actively promoting bilateral trade with the Chinese Government. Even during the absence of official diplomatic relations, during the 1960s through the early 1980s, Singapore was already initiating bilateral economic cooperation with China. Aside from trade, bilateral economic imperatives have manifested in terms of investments and management skills transfer, as evidenced by the completion of the Suzhou Industrial Park Project in 1994.[52] This strategy had allowed Singapore to become one of China's largest trading partners in Southeast Asia, making it more attractive compared to other states in the region. In this aspect of Singapore's strategy, the RMA theory has no relevance because economic relations between China and Singapore do not involve the exchange of any type of military weapons and defense systems.

In terms of diplomacy, Singapore's hedging strategy has concentrated on engaging both China and the US by using institutions such as ASEAN Regional Forum (ARF) as a mechanism to bind both powers in ensuring the status quo in terms of freedom of navigation at sea, a cohesive ASEAN, and a stable distribution of power in the region. As discussed previously, the relevance of RMA in the multilateral engagements between Singapore and other states in Southeast Asia is limited because multilateral institutions in the region are mechanisms for employing soft balancing or actions that do not directly challenge a great power through military means but through nonmilitary instruments in order to delay, frustrate, and undermine aggressive unilateral behavior.[53]

The Singapore Armed Force (SAF) is a critical component of Singapore's hedging strategy because it acts as a deterrent in case there is a need to use force against threats in the region. The SAF is the most capable military force in Southeast Asia and has accepted the notion of an RMA through transformation of its platforms (Endurance Class Landing Ship Tanks) and capabilities (stealth and unmanned technology), doctrines (from COIN to high-intensity operations) and organizational structure (integrated knowledge-based command and control) over the past two decades.[54] More significantly, due to its economic success, Singapore has been able to afford a wide range of advanced military weapons and is currently one of the largest importers of major conventional weapons in the world.[55]

The influence of the RMA theory on Singapore's strategy is extensive because RMA became an impetus for the Singapore Government to start the transformation of all aspects of the SAF. While hedging involves non-military approaches to maneuver around great powers, a credible military industrial complex is certainly a strategic advantage for a small state, considering the constraints and challenges it faces in the international system.

Conclusion

The RMA theory is generally relevant to small states engaged in protecting their sovereignty and advancing national interests; however, very few of these states can actually afford to transform their military forces. Therefore, to gain the benefits of revolutionary technology, they develop different strategies to adapt to the rapidly changing international system. In examining the different strategies, this article argued that the RMA theory has limited relevance in cases where a state employs a strategy of

neutrality (Switzerland) because such states are not inclined to develop a lethal and offensive military force. RMA theory, is of significance to small states that are highly dependent on international organizations (Albania) and alliances (Philippines) for their survival. Lastly, the RMA theory is relevant to small states engaging in a hedging strategy (Singapore) because they require a credible military capability in case all of the non-military policy options have been exhausted.

Notes

1 *Military Transformation and Strategy: Revolution in Military Affairs and Small States*, Bernard Loo, ed. (New York: Routledge, 2009), p. 1.
2 Eliot Cohen, "Change and Transformation in Military Affairs," *Journal of Strategic Studies* 27, no. 3 (2004): 395-407
3 Robert Keohane and Joseph Nye, "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (1998): 87-88.
4 "Strategy" and "foreign policy" are used interchangeably.
5 Miriam Elman, "The Foreign Policies of Small States: Challenging Neorealism in Its Own Backyard," *British Journal of Political Science* 25, no. 2 (1995): 121-71.
6 Loo, *Military Transformation*, p. 4
7 Andrew Krepinevich, Jr., "Cavalry to Computer: The Pattern of Military Revolutions," *National Interest* (Fall 1994).
8 Elinor Sloan, *The Revolution in Military Affairs Implications for Canada and NATO* (Montreal: McGill-Queen's University Press, 2002), pp. 21-22.
9 D. Jordan et al., *Understanding Modern Warfare* (Cambridge: Cambridge University Press, 2009), pp. 143-46
10 United States Navy, *The US Navy Information Dominance Roadmap 2013-2028* (Washington D.C.: Pentagon, 2013).
11 Loo, *Military Transformation*, p. 5
12 US Joint Chiefs of Staff, *Joint Information Environment White Article 2013-2028* (Washington D.C.: Pentagon, 2013).
13 Loo, *Military Transformation*, pp. 6-10
14 Ibid., pp. 11-12.
15 Tim Huxley, "Singapore and the Revolution in Military Affairs" in *The Information Revolution in Military Affairs in Asia,* E. Goldman and T. Mahnken, eds. (New York: Palgrave Macmillan, 2004).
16 James Mulvenon, "Taiwan and the Revolution in Military Affairs" in *The Information Revolution in Military Affairs in Asia.*
17 Michael Raska, "Searching for New Security Paradigms: Israel and South Korea's Defense Transformation (1990-2011)," PhD dissertation (Lee Kuan Yew School of Public Policy National University of Singapore, 2011).

18 Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (California: Stanford University Press, 2010), pp. 96-97.
19 David Betz, "The RMA and 'military operations other than war'" in *Military Transformation and Strategy.*
20 Michael Handel, *Weak States in the International System* (London: Frank Cass & Co., 1990), pp. 52-53.
21 Nazrin Mehdiyeva, *Power Games in the Caucasus* (London: I.B.Tauris & Co. Ltd., 2011), pp. 18-19.
22 Robert Rothstein, *Alliances and Small Powers* (New York: Columbia University Press, 1968), pp. 39-43.
23 Annette Fox, *Power of Small States* (Chicago: University of Chicago Press, 1959), p. 2.
24 Mehdiyeva, *Power Games in the Caucasus*, p. 22.
25 Stephen Walt, *Origins of Alliances* (New York: Cornell University Press, 1987), pp. 17-20.
26 Ibid., pp. 32-33.
27 Kristen Williams, Steven Lobell, and Neal Jesse, eds., *Beyond Great Powers and Hegemons: Why Secondary States Support, Follow, or Challenge* (California: Stanford University Press, 2012), pp. 51-53.
28 Kuik Cheng-Chwee, "The Essence of Hedging: Malaysia and Singapore's Response to a Rising China," *Contemporary Southeast Asia* 30, no. 2 (2008): 163.
29 Evelyn Goh, *Meeting the China Challenge* (Washington, D.C.: East West Center Washington, 2005), pp. 2-3.
30 Geostrategic predicaments refer to the political, geographical and security challenges encountered by each state within their respective regions. The dominant foreign policy strategy is determined based on official government documents released by each state.
31 Central Intelligence Agency, "Country Profile of Albania," accessed November 29, 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/al.html.
32 Ministry of Foreign Affairs, "Foreign Policy Priorities of Albania," accessed November 29, 2013, http://www.punetejashtme.gov.al/al/Misioni/prioritetet.
33 North Atlantic Treaty Organization, "NATO's relations with Albania," accessed November 29, 2013, http://www.nato.int/cps/en/natolive/topics_48891.htm#key.
34 Ibid.
35 General Directorate of Defense Policies, *The Military Strategy of the Republic of Albania* (Tirana: The Ministry of Defense of the Republic of Albania), pp. 6-7.
36 Office of Head of Presence, *Presence in Albania Factsheet* (Tirana, Albania: OSCE, 2012).

37 Ministry of Foreign Affairs, "Foreign Policy Priorities of Albania."
38 Coordinator of US Assistance to Europe and Eurasia, *Foreign Operations Assistance Fact Sheet* (Washington DC: US Department of State, 2013).
39 State Secretariat, *Swiss Foreign Policy Strategy 2012–2015* (Bern: Federal Department for Foreign Affairs, 2012).
40 Ibid.
41 Betz, "RMA and 'military operations other than war.'"
42 Sloan, *The Revolution in Military Affairs*, pp. 77-87.
43 Ibid., pp. 91-97.
44 Joseph Nye Jr. and William Owens, "America's Information Edge" *Foreign Affairs* 75, no. 2 (1996): 24.
45 Department of Foreign Affairs, "Philippines Foreign Policy," accessed November 22, 2013, http://www.dfa.gov.ph/index.php/articles/2013-04-03-07-46-09.
46 Office of the National Security Adviser, *Philippine National Security Policy 2011-2016* (Quezon City: National Security Council, 2011).
47 Renato De Castro, "Balancing Gambits in Twenty-first Century Philippine Foreign Policy," *Southeast Asian Affairs* (2011): 236-38.
48 Renato De Castro, "The Aquino Administration's 2011 Decision to Shift Philippine Policy from International Security to Territorial Defense," *Korean Journal of Defense Analysis* 24, no. 1 (2012): 74-78.
49 Amitav Acharya, *Singapore's Foreign Policy, The Search for Regional Order* (Singapore: World Scientific, 2007).
50 Cheng-Chwee, *The Essence of Hedging*, pp. 176-77.
51 World Bank, "World Development Indicators," accessed November 27, 2013, http://data.worldbank.org/indicator/NY.GDP.PCAP.CD.
52 Cheng-Chwee, *The Essence of Hedging*, pp. 176-77.
53 Robert Pape, "Soft Balancing against the United States," *International Security* 30, no. 1 (2005): 9-10.
54 The transformation of the SAF is discussed in detail in Ministry of Defense, *Defending Singapore in the 21st Century* (Singapore: Ministry of Defense, 2000).
55 Mark Bromley, Pieter D. Wezeman, and Siemon T. Wezeman, *Trends in International Arms Transfers, 2012* (Solna: Stockholm International Peace Research Institute, 2013).

A Multidisciplinary Analysis of Cyber Information Sharing

Aviram Zrahia

The emergence of the cyber threat phenomenon is forcing organizations to change the way they think about security. One of these changes relates to organizations' policy on sharing cyber information with outside parties. This means shifting away from the view of the organization as an isolated, compartmentalized entity towards a view of the organization as a sharing one. Sharing generates a complex, multifaceted challenge to technology, law, organizational culture and even politics. Establishing a system of sharing serves many parties, including regulatory bodies, governments, legal authorities, intelligence agencies, the manufacturers of solutions and services, as well as the organizations themselves, but it also arouses opposition among elements within the organization, and organizations defending the right for privacy. The purpose of this essay is to present the various challenges posed by cyber information sharing, expose the reader to its conceptual world, and present some insights and forecasts for its future development.

Key words: cyber, information sharing, privacy, regulation, information security, trust

Introduction

One of the most difficult challenges faced by organizations is confronting the cyber threat phenomenon. The increased use of technology in organizations of any kind–government, public, and private–turns them into targets of attacks aimed at gathering or damaging information, or suspending services. Attacks on commercial organizations are liable to harm the organizations'

Aviram Zrahia is a cyber security expert at Juniper Networks and a lecturer on cyberspace, and is an intern at INSS.

reputation, endanger physical assets and intellectual property, and cause serious financial damage. Attacks on governments, public bodies, and infrastructures may also disrupt the routines of entire nations and jeopardize the health and safety of their citizens.

Over the last decade, traditional crime has crossed into cyberspace; the growing sophistication of cracking tools and attack vectors has led to the creation of a new, developed and sophisticated cyberspace crime economy. A similar process has also occurred in the sphere of warfare between nations, as many now view cyberspace as the fifth dimension of the modern battlefield, in addition to sea, land, air, and space.

Confronting the cyberspace threat requires an investment in human and technological infrastructures based on an organizational or national risk management policy. The quality of an organization's information security system is affected by different factors, among them the ability to gather and analyze information on legitimate user traffic as well as attacks, regardless of their success. This allows one to identify vulnerabilities in the security system and prevent their exploitation, while identifying and responding to attacks and breaches quickly and effectively, thereby preventing or at least minimizing the damage.

Sharing organizational cyber information is the act of communicating information regarding an organization's security to an external party. While such sharing results in gains for both parties, it does, however, create a complex, multifaceted challenge and represents a shift in the traditional information technology paradigm. The sharing model may exist within the same sector, across different sectors, between commercial enterprises and government bodies, and between different governments. The last two years have seen an increase in the sharing trend; regulatory and law enforcement bodies, both local and international, are promoting it by means of incentives, guidelines and legislation. Concurrently, a security solutions industry based on information sharing among bodies is developing rapidly.

The purpose of this essay is to present the multifaceted nature of the challenge posed by sharing. It begins by presenting the current state of affairs and related problems, followed by an analysis of the practical aspects of sharing implementation, including reference to the theoretical background of trust among bodies. The following section lists the organizational gains and challenges, describing the business opportunities, aspects of the law, regulation and privacy. The paper concludes by offering several insights.

Most of the examples in the essay are from the United States, where sharing initiatives, standardization efforts, government and intelligence agencies actions, and legislative processes are open and at the heart of public debate.

From Compartmentalization to Sharing

The cyber threat is a sophisticated, complex dimension of crime and warfare that has developed in recent years in scope and severity. In terms of the scope of the threat, organizations must now defend not only their computer networks and information systems but also the range of endpoints available to users, such as smartphones and tablets, as well as infrastructure systems, including electricity and air conditioning. They must do so continuously while also making sure they can provide service anywhere, anytime, as expected of an organization of this era.

In terms of the severity of the threat, attacks are becoming harder to identify and locate, as they also include undocumented attack vectors that are unknown to the manufacturers of security solutions. This is true of zero day attacks;[1] the fact that hackers share information continuously and in real time creates a situation in which any weak point exposed in the system or malware can be replicated and used as means to perpetrate an attack almost instantaneously, regardless of location. A recent study of the topic conducted by the RAND Corporation[2] provides an analysis of the way in which cyberspace black markets are built, functioning like ecosystems with clear infrastructure and modules.

These developments create a paradigm shift towards joint efforts at fighting cybercrime, and as a result, many organizations are changing their approach to security; in most organizations, except for those subordinate to regulation and military and/or government systems, the approach to information security management was characterized by total separation from other organizations, both in terms of the technology of their information and security systems and in terms of sharing information about cyber events and security. Information about an attack or an attempted attack and the results of its analysis were kept within the organization, classified and distributed to a very limited intra-organizational list. Revealing information to a third party was perceived as a risk, a move liable to result in damage to its reputation, legal exposure and other complications.

Recently, this trend has reversed. Many organizations and authorities have abandoned the compartmentalization strategy[3] in favor of information

sharing. Through sharing cyber information among organizations, the way hackers do on the attacking side, security measures created in a certain organization to deal with a particular threat can be used by other organizations as an inoculation or at least as information that will heighten their alertness to that particular threat.

The high costs incurred by organizations–in terms of time, manpower and technology–required to provide an effective security protection generate an organizational interest in sharing information and passing some of the costs on to a third party. A study carried out in the United States[4] analyzed the connection between sharing cyber information and the costs of organizational cyber security. It found that companies sharing information spent less on security systems to reach the same level of protection attained by companies that did not share information, meaning that companies can save on direct costs as a result of information sharing. This includes, for example, proactive intelligence gathering and input about weaknesses and expected attacks, inoculations to attacks that occurred in other organizations, use of professionals to help analyze security events, and more.

Another reason for the change in organizational approach to information sharing is the direct and indirect business value in meeting standards and regulations. In certain critical sectors, like finance, healthcare, energy and communications, even private organizations are required to allow state supervision. Most regulations demand information sharing between the organization and some oversight body when it comes to cyber events or attempted attacks. In addition to the obligations, the regulations may have direct and indirect value: a financial organization subject to the Basel III regulation[5]–a standard relating to financial institutions requiring transparency on security events vis-à-vis the regulatory body–enjoys the direct benefit of improved capital allocation for the credit it extends, creating a greater profit margin. An example of indirect benefit may be found in an organization providing services that can make a bid on a government tender that requires bidders to meet the ISO-27032 standard,[6] which also entails information sharing.

Technological Principles in Information Sharing

Secure information sharing among organizations is, in many ways, a technological and operational challenge, from goal and policy articulation

to implementation and use. The methods required to meet the challenge must balance many different components: the ability to support a very large range of organizations and easily add them to the sharing endeavor (scalability); the ability to make use of information after establishing correlation and analyzing it in close to real time so as to produce maximal benefit (usability); and a system of controls to ensure the existence of the "CIA" principles: confidentiality, integrity, availability.[7] The steps towards constructing a system of sharing must include, among other things, goal articulation and participant definition, the privileges and obligations of the participating organizations, technological architecture, trust and oversight model, and work processes.

Information sharing among different entities requires the creation of a system of trust in order to ensure that the information is correct, complete, beneficial and useful. Trust is the basis for all the practical models and examples discussed in this essay. When it comes to trust, the sphere of discussion and solutions ranges from a product's components such as a computer, through the incorporation of various products into a system, to the trust between different systems in different organizations, such as, for example, internet commerce. Standards institutions, such as the Trusted Computing Group,[8] deal with many aspects of the topic, but cyber information sharing is a challenge for which the existing models have not yet provided a complete answer, hence the need for separate debate and the establishment of standards on this point precisely.

When building infrastructure for information sharing, there are three possible models.[9] The first is the "hub and spoke" model in which a central site receives information from the end organizations, fuses it to accommodate different needs and then disseminates it.[10] The hub serves as a clearance center protecting privacy and the intellectual property of all the participating organizations; its use is made possible in part by the accelerated technological development in the field of big data. This allows the processing and analysis of tremendous amounts of information and is a basic building block in constructing the ability to fuse information from different sources. The drawbacks of this model are primarily the consequences from its centralization: the challenge of size, dependence on a central site, delays in processing and disseminating the information.

The second model is the post-to-all architecture in which information is directly distributed among the participating organizations. Since the data

distributed is raw, this model requires infrastructure for analysis in every organization. The third model incorporates aspects of the first and second, striving to take advantage of the relative strengths of each. However, it is relatively complex and expensive to implement.

Technologically speaking, realizing the goal of sharing must take into account protecting an organization's assets and privacy in two ways: first, control of the information being shared based on the participants' goals, and a standardized agreed-upon format. Some of the definitions are meant to conceal the true sources of the information–as in the field of intelligence gathering– so that unnecessary details do not leak outside the organization. The second way entails limiting access to the information, and includes control of its distribution, where it is sent and who sees it, and must be based on a standardized sharing protocol.

Another fundamental choice that must be made is between the automated sharing model and the manual sharing model. Manual sharing means that an authorized party within the organization with access to the sharing system sends and receives information, and controls access to the information. The manual model has a prominent drawback: the human factor creates a bottleneck, especially when the organization is under attack. Other drawbacks include human error and difficulty of managing constant updates.

Automated sharing forces one to decide on a uniform, normalized format, a system of sensors in the organization that will gather and disseminate information, a monitoring system for local reception of warnings, and meticulous realization of controls designed to prevent unwanted distribution of sensitive information. This method overcomes the limitations of manual sharing, but it requires organizations to confront attack scenarios in which the automated sharing system is exposed, such as database poisoning.[11]

Some cyber information sharing standardization activities are already taking place. The most advanced, which has also been adopted by the US Department of Defense, involves a format called the Structured Threat Information eXpression (STIX™).[12] This format defines the structure of a database in which information relating to a user and/or traffic is proactively sent from the organization to an external entity or from an external entity to the organization while containing a range of structured details about a security event. Another relevant standardization for automating sharing is called Trust Automated eXchange of Indicator Information (TAXII™),[13] and it contains the structure of messages and network protocols supporting

the transmission of STIX-type messages among different entities. There are several other peripheral protocols under a wider architecture called Cyber Observable Expression (CyBOX),[14] supported by the US Department of Defense as part of the effort to automate sharing.

It seems that most theoretical models suggested by academics[15] and the practical models suggested by various research institutions[16] are based on automated realization, trust, and a "hub and spoke" sharing architecture. The standardization efforts referred to above suit the spirit of the academic and practical models, so that it seems that, technologically, there is a consensus over the right way to construct such a system. And, indeed, significant parties, such as the US Department of Defense, are working to advance projects based on this outline.[17] Nonetheless, the road to realizing effective information sharing remains long because of the multiple technological, commercial, operational, legal, and (some would claim) moral challenges faced by the sharing initiative members.

Benefits and Risks in Information Sharing

The value of sharing differs depending on the interests of the parties involved. In the case of commercial enterprises, sharing allows a heightened level of security and a reduction in response time in case of an attack, or inoculation against a possible attack in the future by means of receiving warnings and help in identifying, analyzing and confronting attacks. An experiment carried out by a South Korean research team supports this assessment.[18] Sharing also facilitates a reduction in the cost of security thanks to at least partial outsourcing of the analysis and response to a third party. Furthermore, the organization can benefit from regulatory relief as the result of increased transparency and meeting reporting obligations and other conditions.

In the case of the vendors and solutions and services providers, this is a new, technologically-oriented market segment with great growth potential that can distinguish them by creating sustainable, competitive advantages. One of the primary services this sector can offer is identification of possible attack patterns and the distribution of inoculations and warnings to organizations on the basis of fusing information about attacks and attackers gathered from the organizations themselves.

In the case of governments, it is in the interest of regulatory bodies and government and intelligence agencies to encourage sharing because

they increase the organizations' transparency, receive a broad situation assessment of the availability of services and credibility of the information, undertake analysis across different networks and organizations to identify patterns of attacks that have taken place or might take place, and allow for the possibility of a rapid response while disseminating the information to other organizations for the purpose of inoculating them. A state-sponsored body has the ability to construct and maintain a high level of technological capability for its personnel, and to cooperate with organizations in terms of human and technological resources. Sharing is an obvious national interest, allowing the government to fight the national cyberwar and strike at cybercrime in the most effective way possible as well as control the availability of critical national, public and private infrastructures. An example of the realization of regulation with a similar orientation in a different field may be found in regulations on the emission of industrial pollutants, which in some countries require industries, continuously and online, to monitor and report data on air quality in chimneys and other sources of pollution.[19]

Despite the advantages listed above, there are several risks directly related to cyber information sharing among organizations. An analysis of these risks must occur in the setting of an organizational risk management strategy and include the probability of every risk, its effects, the controls required to keep it in check, and the ways to reduce it. For example, the way to reduce the risk of legal exposure to lawsuits for revealing personal or commercial information is by means of laws and guidelines providing legal protection by the government or regulatory body. Another example is the risk of loss of organizational information assets as the result of uncontrolled sharing. That risk can be reduced by using a built-in, standardized sharing format that does not include sensitive information, as well as other checks such as instructions, regulations or legislation that will force the organization to remove personal or commercial data from the information meant to be shared before sending it.

Business Opportunities

The development of cyberspace threats and changes in organizational attitudes towards sharing are a business opportunity for the manufacturers of technological solutions, integration companies and service providers

that can leverage their base of products, knowledge and services to create added value in the context of the sharing challenge.

One example relates to the challenges posed by innovative attack technologies, such as the Advanced Persistent Threat (known as APT),[20] or taking advantage of undetected or untreated security breaches. Both of these attack mechanisms reduce the effectiveness of the traditional security measures[21] but can, to a certain extent, be addressed by an inter-organizational security sharing service. Such sharing could facilitate the identification of an anomaly in the cloud and comparison with organizational events not only with regard to its conduct within the organization but also to that within similar organizations, thus enhancing the identification mechanism and reducing the risk that harmless traffic will accidentally be identified as malicious (known as "false positive"). In addition, after the identification of an attack or attacker in a given organization, the components or the inoculation can be distributed to other organizations and thereby prevent similar attacks.

Several security systems manufacturers provide solutions to cyber information sharing based on a decentralized infrastructure of information gathering, using a system of probes, which may at times also serve as honeypot traps for attackers. These are installed in organizations and end clients or at central internet nodes belonging to the manufacturer. This infrastructure gathers information on attacks and attackers in real time, in cross-referencing geographical location and attack, and distributes it as a service to the organizations involved in sharing. The system serves as a share-based database on attackers and/or attacks in the cloud and may sometimes include a component that filters and blocks potential attacks on the basis of the information being dynamically updated.

In the case of cloud-based communications and storage service providers, sharing is an opportunity to reduce the rate of client dropout by means of providing the added value of another layer of protection.[22] The nature of a shared cloud allows the provider to improve the security policy for all the other hosted organizations in order to prevent its recurrence after identifying and stopping an attack in one organization.

Another business opportunity directly related to sharing initiatives is the construction of a solution for gathering, analyzing and distributing cyber information at the national or market sector levels. Several integration companies in the world have a comprehensive solution for creating a

situation assessment, analyzing events, distributing inoculations, training simulators, and other components, at the scale of military and large public systems. Moreover, there are solution manufacturers in the field of monitoring and in-depth analysis of traffic (deep packet inspection), allowing telecommunication service providers to selectively share information with the legal authorities so that the latter may listen in on telephone and internet networks for the sake of identifying threats. Some of these companies also provide the solution component responsible for information analysis based on smart logic, containing analysis of a tremendous amount of information gathered from various sources, study of anomalies, and correlations among the events.

One may assume that the wave of technological innovation in the world of security solutions will continue because of the need to adapt security systems to existing and emerging cyber threats. Furthermore, one may assume that the idea of sharing–taking on greater prominence in the security policies of key organizations–will continue to present business opportunities to commercial entities operating in the field.

Regulation and Privacy

There are fields in which the regulatory body and/or the law already require sharing information about cyber threats and cyber events, and it would seem that this trend is on the rise given governments' need to establish a national security system to fight cybercrime and maintain transparency regarding cyber-related events in public companies and strategic market sectors, such as communications, finance and healthcare. Moreover, various regulators, such as Basel III and ISO-27032, encourage sharing information between organizations and the authorities, both by means of guidelines and by offering economic benefits and relief to participating organizations. A paper analyzing the trade-off in financial institutions between investing in information security and sharing cyber information[23] concluded that the benefits of sharing among organizations increase in correlation with their interdependency, and the more sharing there is among such institutions the smaller their investment in information security. In many market segments (such as finances and telecommunications) the links between the organizations are critical to their everyday functioning, and an attack on one organization could propagate and damage the functioning of other

organizations in the same sector. Examples are financial transactions between different banks and phone calls between different service providers.

Similar organizations also share similar challenges, some of which may be unique to their sector. For example, healthcare organizations share the unique challenge of confronting cyber attacks aimed at medical equipment. Cooperation among such organizations on the gathering of intelligence or hardening procedure for such equipment will save on the investment each of the organizations has to make on its own.

Several nations have iterated their intention to establish systems for gathering cyber information, including the incorporation of government bodies and private/public bodies of national importance.[24] The essence of this move is to create a comprehensive cyber situation assessment, providing the ability to respond to attacks with highly trained personnel, and immediately disseminate inoculations or information about the attack to all subordinate organizations. As noted, the technological base for creating such a system may require legislation, and requires cyber information sharing among organizations and the establishment of a center for fusing information and applying defense mechanisms to secure organizational assets and privacy. The British government has established a sharing initiative called the Cyber Security Information Sharing Partnership (CISP) as part of its national program for coping with cyberspace challenges.[25] The partnership already includes more than 250 key organizations as well as the legal authorities, and its purpose is to improve the ability to cope with cybercrime and cyberterrorism. Since the beginning of the 21st century, the United States has instituted sharing initiatives named Information Sharing and Analysis Centers (ISAC) in sectors such as healthcare, finance and more. Most of these initiatives are owned and financed by the participating organizations, but recently they have benefitted from technological and even financial support from the US Department of Defense, thus acknowledging the government's interest. Examples of involvement include providing access to the United States Computer Emergency Readiness Team (US-CERT)[26] and establishing a master initiative designed to unite all the inter-organizational information in the United States into a single system.[27]

It is obvious that fighting cybercrime and cyberterrorism, which by their very nature cross geographical and political borders, can succeed only through technological and legal cooperation among nations. One such initiative is the program for research cooperation in the field of

cyberspace initiated by NATO and the EU.[28] Another initiative is the sharing infrastructure being built at NATO, in which the information will be automated on the basis of STIX in order to allow sharing among various organizations in NATO member nations.[29] Legally, the Convention on Cybercrime (also known as the Budapest Convention) was formulated and signed with an eye to coordinate the various legislative systems of the EU member nations, improve joint investigative methods, and increase cooperation in dealing with computer crime.

A paper surveying international cooperation in protecting critical infrastructures against cyberattacks[30] reinforces the hypothesis that the chances of an information sharing system succeeding increase if the participating entities have similar interests and cultural and political outlooks. Information sharing among different entities is naturally challenging in terms of maintaining secrecy because it requires a definition of the limits on sharing and controls that can distinguish between private or intra-organizational information and information that may be shared.

Over the years, governments have received tacit cooperation, which is sometimes enforced through legislation, from infrastructure and service providers, as well as application vendors, both for the purpose of national security and for the purpose of fighting cybercrime. This phenomenon received much attention recently, especially after *The Guardian* revealed, on the basis of Edward Snowden's leaks, the US National Security Agency surveillance of computer traffic of leading US companies in the context of its PRISM program.[31] The newspaper also revealed that the NSA-equivalent British intelligence organization GCHQ, monitors the internet traffic on Britain's fiber optic network,[32] and that MI5, Britain's security service agency, intends to deploy technological measures to enable filtering key words and specific data in all information traffic in the country.[33]

The exposure of the surveillance programs in the United States raised the issue of privacy and limiting the power of the government as well as the possibility of imposing legal sanctions against the parties that share their information. So far, the United States Supreme Court has rejected lawsuits against local telecom giants and confirmed the legality of submitting information regarding Internet and telephone use to legal and intelligence agencies.[34] Still, the possibility of lawsuits against an organization that shares information is an obstacle to sharing that the government would like to remove.

Since the end of 2011, legislation on cyber information sharing has been advanced.[35] The purpose of the proposed law is to allow private and public companies, in the context of cyberwar, to share information in real time with the government, law enforcement and intelligence agencies without risking lawsuits for violating secrecy or privacy. The bill passed in the House of Representatives, went through a round of adjustments in the Intelligence Affairs Committee,[36] and is still in the process of legislation in the Senate. Its opponents claim that it violates the Fourth Amendment to the Constitution,[37] which defines parameters for search and seizure of citizens' personal information, such as warrants or reasonable grounds. According to opponents of the bill, the new legislation would allow intelligence agencies to receive personal or commercial information from infrastructure and content providers without the checks delineated in the Fourth Amendment. Groups dealing with the problems inherent in the bill[38] are trying to enlist public support to oppose and prevent it from becoming a law, by running a campaign in the social media and on the internet in the United States.

The tension between supporters and opponents of cyber information sharing legislation is not unique to this area, but touches on the entire issue of privacy in the interface between the state and its citizens and the involvement of Big Brother. An example of a similar conflict may be found in the Smart City initiative in Britain, which includes covering cities with cameras and face recognition software.

Concluding Insights

Trends in the contemporary development of the cyber threat phenomenon include using attack methodologies focused on specific targets rather than being randomized, crossing geographical and legal borders, taking advantage of unidentified vulnerabilities, and using bits of malicious, modular code in cyberspace. The attackers maintain a flourishing, structured community with internal order and a supporting system of financing, allowing easy and rapid sharing of attack information. It seems that the realization of the community model on the defensive side and transitioning from a paradigm of isolated organizations to an information sharing initiative will lead to better results. In a broader view, one of the most significant resources coming into being in the 21st century is the wisdom of crowds.

One can see examples of crowdsourcing in many fields and, in this sense, cyberspace is no exception.

The transition to models of sharing is supported by the congruence of interests of most of the market forces involved, including regulatory bodies, governments, law and intelligence agencies, solution manufacturers and service providers, and even the organizations themselves. The value of sharing with external elements is, among other things, a product of the isolated organization's inability to fight its cyberwars on its own. Sharing contributes not only to significantly strengthening the security system and its survivability, but also to the organization's business success as it saves on investment, is granted preferential treatment by the regulatory bodies, and more.

The architecture of the solution and developing standards will, in the future, make it possible to create a technological structure connecting organizations while keeping their assets separate. They will also support links among separate sharing systems that can connect one another into a hierarchic structure of information, such as sharing within a market segment that will interface into cooperation at the national level.

Some of the success of the entire standardization process depends on support from the market forces. In this case, it seems that elements in the US administration, especially the Department of Defense, are determined to promote the process. Nonetheless, we still don't see effective large-scale information sharing because of the many challenges, not necessarily technological, and at times because of the conservative approach of organizational decision makers.

As the field comes of age, we may first expect to see sharing among similar organizations in the same sector and, later on, the implementation of information sharing on a larger scale. Shared interests, similar organizational cultures, and inter-organizational dependencies increase the chances of success of the initiative and reduce its risks.

Two of the prominent obstacles to sharing are the organizations' concern that if systems are linked, sensitive internal information may be exposed to the competition, and that they may receive incorrect cyber information because of the poisoning of a shared database, which might damage service provision. One can significantly reduce the risks inherent in both by technological means and standardized processes and protocols implemented both on premise and in the central sharing entity.

The greater challenge is faced by organizations whose business is essentially linked to cyberspace, such as security solutions, software products and services manufacturers, and the large project and integration bodies in the field. The question remains: is it possible to formulate a worthwhile working model among these manufacturers so that they will share cyber information, even though security and cyberspace are part of the field in which they compete? Such a model must include both elements of competition and of cooperation (coopetition) in a way that would provide advantages to each of the partners over time.

The disagreement between supporters and opponents of information sharing will continue. Given that, and given all the aspects of the topic discussed in this essay, the question that must be asked is this: is there a different paradigm in the world of information technology that would allow dealing with current and future cyber challenges without the need for sharing, or is there no choice but to join forces in the battle and rapidly adopt uniform standards for a sharing infrastructure? Either way, such an infrastructure must maintain a balance between individual rights and the state's ability to defend its infrastructures, assets and citizens.

Notes

1 A zero day attack exploits a security breach in the attack target's component that is unknown to the component's manufacturer or anyone else other than the attacker, or one that is known to the manufacturer but for which it has yet to distribute a patch.

2 One study conducted in the past year by the RAND Corporation analyzes the way in which cyberspace black markets are constructed and operate, surveys historical trends, and provides forecasts for the future. Researchers at the institute conducted in-depth interviews with experts who are officially and unofficially involved in these markets, including academics, security researchers, journalists, security providers, and law enforcement personnel. The report concluded that the black markets in cyberspace are a multi-billion dollar industry with solid infrastructures and a clear social and organizational structure. L. Ablon, M.C. Libicki and A.A. Golay, *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

3 The approach supporting compartmentalization of cyber information is described in many sources as part of an organization's preparation for a cyber event. An example is the preparation model suggested by SANS, taken

from a course dealing with the topic. E. Skoudis, ed., "Security 504: Hacker Techniques, Exploits & Incident Handling," *SANS Institute* (2006).

4 L.A. Gordon, M.P. Loeb and W. Lucyshyn, "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting & Public Policy* 22, no. 6 (2003): 461-85.

5 Basel III is a regulation in the field of finance that includes a chapter requiring financial organizations to share cyber information as part of their operational risks. For more information: *Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems*, http://www.bis.org/publ/bcbs189.pdf.

6 A standard which includes guidelines on cybersecurity, and the demand that organizations share information. "ISO/IEC 27032:2012−Information Technology−Security Techniques−Guidelines for Cybersecurity," July 16, 2012, http://www.iso.org/iso/catalogue_detail?csnumber=44375.

7 The three fundamental elements of CIA represent the classic basic principles of cybersecurity: confidentiality−protecting the contents from being read by unauthorized personnel; integrity−protecting the contents from alteration by unauthorized personnel; and availability−keeping the information and systems available.

8 TCG website, http://www.trustedcomputinggroup.org/.

9 "Cyber Information-sharing Models: An Overview," MITRE, October 2012, http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

10 Information fusion is a process designed to link and cross-reference data, information and knowledge in order to find correlations for the purpose of improving the ability to locate and identify entities about which information is being gathered, and for the purpose of assessing a situation and ranking risks. In addition, an assessment of the outputs quality is made and demands are created for information sources, as an integral part of the fusion process for the sake of improving the outputs.

11 Database poisoning using false information is liable to obstruct the organization's activity, internally or vis-à-vis outside bodies (denial of service). The advantage of an automated system of sharing is also its greatest disadvantage, and it is more prone to such poisoning than a manual sharing system because it does not include human monitoring in real time.

12 S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," February 2014, http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.

13 M. Davidson, C. Schmidt, "TAXII Overview," version 1.1, January 2014, http://taxii.mitre.org/specifications/version1.1/TAXII_Overview.pdf.

14 "CybOX−Cyber Observable eXpression−A Structured Language for Cyber Observables," 2014, http://cybox.mitre.org/.

15 An example of a fundamental architecture of sharing relating to the issue of trust in the context of academic research is an architecture called PEI proposed by Krishnan and colleagues. It includes three required layers:

the policy layer, which sets out the goals of sharing and the articulation of objectives; the enforcement layer, which includes the basic solution architecture; and the implementation layer, which entails delving into the technological level of the details of sharing. R. Krishnan, R. Sandhu, and K. Ranganathan, *PEI Models towards Scalable, Usable and High-Assurance Information Sharing* (New York: ACM, 2007), pp. 145-50.

16 The federally-financed MITRE research institute delineates the stages and decisions that must be made as part of a process of constructing a sharing model. Those decisions include the sharing architecture, the model of trust among the participants, automation of sharing, operations and participants. V.B. Bakis, "Cyber Partnership Blueprint: An Outline," MITRE, October 2013, http://www.mitre.org/sites/default/files/publications/Bakis_Partnership_Blueprint_Outline_0.pdf; The Bipartisan Policy Center has come up with a model in which a central body serves as a clearance center for shared information of critical infrastructure institutions in the United States. "Cyber Security Task Force: Public-Private Information Sharing," Bipartisan Policy Center (BPC), July 2012, http://bipartisanpolicy.org/library/cybersecurity-task-force-public-private-information-sharing/.

17 A. Merchant-Dest, "How the Department of Defense and the Department of Homeland Security are Taking Steps toward Information Sharing," *Federal Blue Print*, March 2014, http://federalblueprint.com/latest-news/department-defense-department-homeland-security-taking-steps-toward-information-sharing/.

18 The South Korean research team's experiment proves that sharing information among different parties (zones) shortens response time to attacks and raises the level of security. V. B. Chang, D. Kim, H. Kim, J. Na, and T. Chung, "Active Security Management Based on Secure Zone Cooperation," *Future Generation Computer System* 20, no. 2 (2004): 283.

19 The Israeli Ministry for Environmental Protection, "Procedures and Guidelines on Emissions of Industrial Pollutants." http://www.sviva.gov.il/subjectsEnv/SvivaAir/Industry/Pages/Regulations.aspx.

20 APT is a collection of cyber attack tools and methods aimed at a specific target and controlled by professional hackers, and which can therefore be developed and operated in a way that makes it very difficult to identify using standard security measures.

21 These two attack technologies reduce the effectiveness of the traditional security mechanisms whose main function is to identify clear patterns of attack. They require behavior based reference in order to identify the threat and a transition from developing signature based security products to behavior based anomaly detection products. Two of the main challenges in the latter is the need to create an organizational behavioral baseline that documents the normal behavior of the organization and its computer systems in order to identify anomalies, and the risk to disruption of legitimate transactions because of false positives.

22 Also called Managed Security Service Provider (MSSP).

23 K. Hausken, "Information Sharing among Firms and Cyber Attacks," *J. Account Public Policy* 26, no. 6 (2007): 639-88.

24 An example of a nation's strategy in constructing a national cyber system may be found in a document of the Finnish government that includes visions and principles in building a cross-organizational cyber system and a list of concrete recommendations to make it happen. *Finland Cyber Security Strategy*, Secretariat of the Security Committee, 2013, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

25 The British government's national program for confronting cyber threats. *The National Cyber Security Strategy, Our Forward Plans–December 2013*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf.

26 The US-CERT–United States Computer Emergency Readiness Team website, http://www.us-cert.gov.

27 The Information Analysis and Sharing Centers website– the National Councils of ISACs, http://www.isaccouncil.org/memberisacs.html.

28 *The Multinational Cyber Defense Capability Development (MNCD2) Program*, http://mncd2.ncia.nato.int/Pages/default.aspx.

29 *The Cyber Security Data Exchange and Collaboration Infrastructure (CDXI*); L. Dandurand, *Cyber Security Information Exchange*, http://www.rsaconference.com/writable/presentations/file_upload/sect-t08-cyber-security-information-exchange.pdf.

30 L. Tabanski, "International Cooperation in Critical Infrastructure Protection against Cyber Threats," *Atlantic Voices* 2, no. 9 (2012), http://sectech.tau.ac.il/node/114.

31 Electronic surveillance program carried out by the NSA, starting in 2007, to gather information for the purpose of intelligence from infrastructure, software and contents providers (Google, Yahoo, Microsoft, Apple, Skype, AOL). This activity was revealed through Edward Snowden's leaks to *The Guardian* in 2013.

32 E. MacAskill, J. Borger, N. Hopkins, N. Davies, and J. Ball, "How does GCHQ's Internet Surveillance Work?" *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

33 Monitoring technology allowing the filtering of key words in internet traffic is called "deep packet inspection."

34 The United States Supreme Court rejected a lawsuit against the giant telecom companies Verizon, Sprint and AT&T, and confirmed the legality of transferring information from emails and phone conversation to the NSA. B. Kendall, "High Court Lets Telecom Firms Wiretap Immunity Stand," *Wall Street Journal*, October 9, 2012,

http://online.wsj.com/news/articles/SB10000872396390444024204578046312896501562.

35 The Permanent Select Committee on Intelligence, 2013, *Cyber Intelligence Sharing and Protection Act of 2013*, http://intelligence.house.gov/bill/cyber-intelligence-sharing-and-protection-act-2013.

36 The modified bill after the changes is called: "Cybersecurity Information Sharing Act of 2014." Continuous updating on the status of the legislation may be found at the Library of Congress, http://thomas.loc.gov/home/thomas.php.

37 The Fourth Amendment reads as follows: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

38 Two of the institutions active on the topic are the Electronic Frontier Foundation (EFF) and Fight for the Future. Both are running a campaign called "CISPA Is Back" to gather citizens' signatures on a petition against the legislation. http://www.cispaisback.org.

Yemen: A Mirror to the Future of the Arab Spring

Sami Kronenfeld and Yoel Guzansky

Ethnic, political, and religious rifts make Yemen one of the most complex arenas in the Middle East, even more so following the eruption of the Arab Spring, which in November 2011 ended the 33-year regime of President Ali Abdullah Saleh. The disintegration of the delicate political balance Saleh created has brought Yemen to the brink of an abyss with competing elites, ethnic revolts, separatists, external intervention and fundamentalist terrorism threatening to divide the country while hindering the new regime's attempts to build a new political order and establish stability. Currently, the future of Yemen is still unclear, but the developments and processes it is undergoing may provide us with insights about possible scenarios in other Middle Eastern countries in the post-Arab Spring era.

Key words: Yemen, al-Qaeda in the Arabian Peninsula (AQAP), Ansar al-Shariah, Houthis, Ali Abdullah Saleh, Arab Spring, Iran, National Dialogue Conference

Yemen, the poorest of the Arab nations, is in many ways a microcosm in which the tensions, challenges and hopes typical of the entire Arab world are amassed. Competing elites, international intervention, ethnic violence, tribalism, Shiite-Sunni tensions, fundamentalism and terrorism are all part of Yemen's intensive and chaotic reality, as it rapidly changes and develops. Yemen's complex situation allows an *in vivo* examination of processes such as the transition of power, reconstruction of security forces, federalization, national reconciliation, and the fight against al-Qaeda affiliates, all of which we can expect to be replicated in Syria, Iraq, Libya and elsewhere.

Sami Kronenfeld earned his MA in International Relations at the Hebrew University in Jerusalem. Yoel Guzansky is a research fellow at the Institute for National Security Studies.

Saleh's Arrangement and the Arab Spring

Poverty, violence, lack of personal security and government corruption were some of Yemen's hallmarks prior to the onset of the Arab Spring. The inability to create effective sovereignty and internal stability is, to a large extent, inherent in Yemen's reality, as it suffers from ethnic, religious and cultural heterogeneity, enmities among regions and provinces, and tribal structures carrying traditional hierarchies over into the 21st century. Over the years, these problems were exacerbated by the actions of President Ali Abdullah Saleh, who during his 33-year rule cultivated and preserved a divided and conflicted political system in order to fashion himself as the only element capable of holding the country together.[1]

Saleh's regime relied on balancing the country's various power groups and elites. In order to ensure loyalty and enlist support, Saleh created a network of government patronage and economic benefits, preserving the delicate balance in the security forces and the distribution of power among the tribes; tribal leaders who promoted the regime's interests received significant benefits. Saleh even managed to bribe the opposition and cause it to change sides. He sought to placate the public, most of which was marginalized and kept outside political discourse and economic centers, along with his allies in the international community by means of extensive use of the democracy rhetoric, though this was no more than a cover for a regime sullied by a combination of terror and corruption.[2]

While Saleh's arrangement managed to preserve Yemen's political unity and create the appearance of stability for many years, the exclusion of large segments of the population from the political and economic systems eventually led to the regime's collapse. In January 2011, tens of thousands of young Yemenis took to city streets, calling to overthrow Saleh and establish a true democracy. The protesters, inspired by demonstrations in Tunisia and Egypt and motivated by a profound sense of discrimination and hopelessness, called for justice, equality and opening the political and economic power centers, which until then were only accessible to the traditional elites. The protests grew more vigorous, and any attempt by Saleh to placate the masses with promises of reforms failed.

The protests in Yemen quickly generated chaos and violence throughout the country, as entire military units have even deserted and joined the protesters. In June 2011, an RPG was fired at the presidential compound. The missile killed four of the president's men, and Saleh himself was seriously wounded, and was forced to leave Yemen for medical treatment in Saudi

Arabia. In November 2011, under Saudi and US pressure, Saleh signed an agreement that regulated the ceding of authority to Vice President Abed Rabbuh Mansur Hadi, forcing the government to hold new elections within two years. The agreement also entailed a commitment on the part of the international community to provide Yemen with political and economic aid during the transition period. The signing of the agreement created hopes for positive change; however, most of them have yet to be realized.

Yemen outranks Iraq and Afghanistan on the list of failing nations.[3] The violence and chaos in the nation have spread while elements interested in weakening the country, or even in its dissolution, whether external or internal, are hard at work–sometimes in concert–to attain their goals. Nonetheless, 2014 has seen some developments that may signal the beginning of political stabilization, including the end of the National Dialogue process and the decision to turn Yemen into a federative nation.

In the Aftermath of the Arab Spring: Searching for Stability

The transition government and the international community's efforts to preserve Yemen's unity and strengthen the legitimacy of its institutions and sovereignty were, to a great extent, channeled into the National Dialogue Conference. The conference, which met for the first time in March 2013 supported and encouraged by the Gulf states, the United States, the United Nations and the World Bank, consisted of 565 representatives from every political party and faction in Yemen. Emphasis was given to the inclusion of young people, who were at the heart of the popular protests, as well as the inclusion of women and minorities. Conference participants received a wide mandate to deliberate the core issues such as the nature of the regime, civil rights, the structure of the security forces, and the formulation of a constitution, in order to fashion a new Yemen and neutralize the loci of conflict and instability through dialogue and consensus.[4]

The beginning of the talks was accompanied by optimism, though it was not long before many of the protest leaders came to realize that the old elites were seizing control of the talks, many of which were held with notable lack of transparency. Over a ten-month period, the conference lost most of public support and trust, and many started questioning the legitimacy of its actions and decisions.[5] The conference's legitimacy was dealt a harsh blow when, four days before its end, the head of the Houthi delegation was assassinated.[6] This was the second assassination of a member of the

Houthi delegation, and it led to the group's withdrawal from the conference and doubts as to the legitimacy of resolutions reached in the conference.[7]

While the talks were plagued by many difficulties, it seems that the conference's resolutions, made public on January 25, 2014, will affect Yemen's stability and unity. The most critical decision refers to turning Yemen into a federal republic composed of several provinces with local parliaments and extensive autonomous authority. The federal regime will be headed by a president, and elections for national institutions will be held on the basis of relative representation for each of the provinces. The number of provinces and their borders were determined by a sub-committee headed by the president. It decided that, pending ratification by referendum, Yemen will be divided into six provinces. The capital city of Sana'a will be autonomous and not belong to any of the six provinces, while the southern port city of Aden will be given special status as an economic city.[8] Other than the decision on establishing a federation, the National Dialogue Conference also appointed a committee to formulate a constitution. This committee shall work for three months after which it will present a new constitution for a national referendum. Should the constitution be approved, general elections to all national and provincial institutions will be held within one year. Furthermore, President Hadi's term in office was extended by one year to allow him to promote and oversee the implementation of the National Dialogue Conference's recommendations.[9] These reforms, seeking to generate stability, are receiving widespread international support as well as the support of large segments of the Yemeni political system and public. But the road to this elusive stability is still long, and significant challenges, both domestic and external, threaten to bring about further deterioration.

Domestic Challenges: Multidimensional Splits

The Competing Elites

One of the key elements threatening the success of the reforms and Yemen's political stability is the struggle among the country's elites, a struggle that became more extreme and even violent after the fall of Saleh's regime. The Yemeni political system consists of a wide gamut of players and power groups competing amongst themselves for control of the political, security and economic power centers, in what they largely view as a zero-sum game. The dominant figure in these struggles is the ousted president, Ali Abdullah Saleh, who received a full pardon in the transition of power

and managed to retain much of his influence and control even after he left the presidential palace. Saleh and his family have many loyalists in key government and army positions including from the time Saleh had served as head of Yemen's ruling party (of which President Hadi is also a member). In addition, Saleh controls a multi-branched network of contacts in the bureaucratic frameworks, religious institutions and tribal leaderships.

Saleh and his loyalists are doing everything in their power to undermine the reforms and show that a stable Yemen is impossible without them. Dozens of army units loyal to Saleh have rebelled against their new commanders,[10] and when Hadi sought to dismiss the air force commander, Saleh's half-brother shut down Sana'a's international airport.[11] Saleh is also seen by many as being behind a wave of terrorism and assassinations that, since 2011, have cost the lives of many government and army personnel (some even say that he secretly supports the Houthis' rebellion in the north).[12] Saleh's subversive activities led the UN to impose personal sanctions (Resolution 2140) against persons attempting to damage the Yemeni reform program. While the resolution did not specify names, it was largely aimed at Saleh and his people.[13] At present, the threat of sanctions does not seem to moderate Saleh's subversive activities. In June 2014, members of the presidential guard surrounded a mosque belonging to Saleh in southern Sana'a, claiming that it was being used to hide weapons and that a tunnel had been dug leading to the interior of the presidential palace, to facilitate a violent seizure of the center of Yemen's governance.[14]

Saleh's main opponents in the struggle for power are his former allies who broke with him and are now seeking to consolidate their power and influence in the new Yemen. One important group is the al-Ahmar family, heading the Hashid federation, a large, powerful tribal coalition. The family has thousands of fighters at its disposal as well as a great deal of wealth, and it is working assiduously to solidify its power. Another influential figure is General Ali Muhsen, the former commander of the 1st Army and a key official in Saleh's regime. Although dismissed from his post by President Hadi, he still commands the loyalty of many powerful army personnel and wields considerable influence. Another player is al-Islah, Yemen's second largest political party and what passed for the official opposition to Saleh's regime (in fact, its leaders were coopted by Saleh and cooperated with him behind the scenes). The party, made up of a coalition of the Muslim Brotherhood, tribal elements (including the al-Ahmar family) and salafi

movements, is currently the president's main coalition partner, working hard to expand its influence in the power centers of both the army and the government.

Amidst all of these is the residing president, who was initially viewed as weak, though over time he has managed to establish his power and influence in the political system and the army. The additional year in office granted by the National Dialogue Conference positions him as the key person in forming the political structure of the Yemeni federation-in-the-making.[15] These players, all of whom cooperated with and were a part of the power structure of the old regime, are currently aggressively attempting to preserve and strengthen their power and influence in Yemen. It is unclear to what extent they care about the interests of the country and its people.

The center of gravity of the competing elites lies in the security forces. Even in Saleh's time, Yemen's army and security forces were never a homogeneous, professional institution, but rather a fragmented gathering of competing units serving as tools for political struggles between the various power groups. In the last years of Saleh's regime, the main split in the security forces has been between those supporting Ahmed Ali Saleh, the commander of the Republic Guard and the former president's son who was being cultivated as his heir, and the supporters of Ali Muhsen. This rivalry became even more contentious during the protests, almost culminating in a dangerous clash between the Republican Guard and 1st Army forces. Each side recruited thousands of soldiers and tried to entrench its relative power.[16]

Though the split within the security forces did not end in widespread military clashes, the politicization of the army has been a constant threat against any attempt at reform and political change. Therefore, when he came to power, Hadi began to neutralize the power loci in the security forces and establish a professional, unified army subject to the civil government. Hadi succeeded in exploiting the rivalries among the various army factions: making use of existing rounds of promotions, he transferred officers with rival political loyalties away from positions of command and influence. The height of the move was the dissolution of the Republican Guard and the 1st Army and assimilating those personnel in the ranks of other army units while dismissing Ahmed Ali Saleh and Ali Muhsen from their posts. The president also established new units and recruited thousands of soldiers to undermine the old elites.[17]

Hadi has focused most of his effort on minimizing his predecessor's influence. While he has gained some success doing so, it has also cost him dearly in terms of the Yemeni army's operational capabilities. The Republican Guard and the 1st Army were Yemen's military elite. They controlled the best equipment and included both the special forces and the anti-terrorism units, some of which received U.S. training. Their dissolution and replacement by new recruits means that Yemen is currently finding it hard to confront the terrorists and guerrilla organizations threatening the various parts of the country, including Sana'a.[18]

At present, it seems that the struggle among Yemen's elites and power groups is far from over. While Hadi has succeeded in weakening Saleh's loyalists, his rivals accuse him of following in his predecessor's footsteps, trying to wrest control of the army by inserting his loyalists into key command positions and recruiting soldiers primarily from among the ranks of al-Islah, his political ally.[19] Furthermore, there are those within his own party who claim that, in his attempt to weaken Saleh, he is handing Yemen over to al-Islah.[20]

Economic Weakness

In addition to the lack of political stability, Yemen is also suffering from deep-seated economic hardships. Saleh's tenure in office and the benefits he gave his supporters all but drained Yemen of its resources. Oil, the country's only natural resource and the source of most of its income, dwindles fast. In the absence of an alternate program for economic development, Saleh was, in the last years of his regime, forced to rely on financial aid from Saudi Arabia and the United States. Yemen is the most populated nation in the Arabian Peninsula and also the poorest country in the Arab world, with about half of its population living on less than two USD a day. Since the beginning of the protests in early 2011, the economic situation in Yemen has only deteriorated. Oil and gas exports received a lethal blow (drilling installations have become a favorite target for terrorist organizations),[21] and the economy has sustained other serious losses. Unemployment in Yemen hit new heights: according to several indices, it is past the 50-percent mark. Unemployment can be expected to worsen as hundreds of thousands of Yemenis working abroad may face deportation as a result of reforms in the Saudi Arabian labor market.[22] In addition, water has become a rare commodity; hunger is on the rise, as is the fear of contagious diseases.[23]

The political upheavals Yemen has experienced have also damaged the delicate tribal fabric that is so important to economic stability, and in several cases touched off armed confrontations between tribes over control of the country's dwindling resources. Economic considerations are liable to become a serious obstacle to the federalization program. In the north as well as the south, many claim that the proposed borders impinge on their economic rights and were intentionally designed to weaken them in order to maintain the dominance of Sana'a.

Insurgence from the North and the South

Yemen's stability and integrity are also–perhaps primarily–threatened by the national and self-determination ambitions of separatists in the north and south of the country. In the north, Yemen is facing a widespread Shiite revolt led by the Houthis (named after the al-Houthi family) concentrated in Sa'da province. The spark that ignited the armed struggle in 2004 was the killing of Hussein al-Houthi (the regime sought his arrest, in part for his links to Shiite communities in Lebanon and Iran).[24]

By 2009, the conflict had become full blown, to the point that Yemen embarked on a scorched earth operation against rebel cells in the north. The fighting spilled over into Saudi Arabia as the rebels crossed the border, capturing several villages and killing Saudi soldiers. The Houthi attack on its territory pulled the Saudi army into the fighting. In early November 2009, while the Yemeni army was fighting rebels in the south, the Saudis attacked from the north in a classical Pincer Move. For three months, the Saudis, equipped with the very best weapons the West could offer, worked to quell the uprising deep in Yemeni territory. In 2010, as the result of international pressure, the warring sides signed a ceasefire agreement.

The Houthi rebellion was reignited in 2011 when the rebels–some 7,000 according to various estimates–exploited the chaos, generated by the protests and the transfer of many army units from Sa'da province to Sana'a, to seize control of large tracts of land along the Saudi border. The Houthis reinvented themselves and turned their ideological, religious movement into a classical guerrilla movement seeking to establish autonomous Shiite rule in the northern provinces. The intensity of their operations rapidly generated a counter-response by Sunni tribes led by the al-Ahmar family and by salafist groups.[25] The attack on the city of Damaj, a Salafi center in the Sa'da province, by Houthi rebels in November 2013 led to the expansion

of the fighting and escalated the situation in northwest Yemen to ethnic warfare. During the fighting, the Zaidi Shiites had great success on the battlefield, conquering Salafist and tribal strongholds (including the city of origin of the al-Ahmar family), extended their area of influence, and managed to get to within 40 kilometers of the capital city.[26]

In February 2014, the sides agreed to a ceasefire; two of the warring parties agreed to withdraw to their original territories and approved the deployment of the army to maintain order in the region.[27] Nonetheless, it seems that the instability and tension in the north of Yemen have not been resolved. Elements among the Houthis have expressed fierce opposition to the division into provinces as outlined by the regime. The Houthis say that their region, Sa'da, has been included in a province that has no significant natural resources and no access to the sea. The Houthis view this as an intentional attempt on the part of the central government to damage their ability to develop economically and undermine their power.[28] It seems that the planned federative division already contains the seeds of the next round of violence. The first indicators have appeared in February when a Houthi force attacked an army position; 24 people were killed in the incident.[29]

Other than the ethnic conflict in the north, Yemen's stability and unity are also threatened from the south. Since the early 1990s, the unification between the south and north has been a source of friction and instability. The dominance of the north in the united Yemen created a sense of disenfranchisement among the southerners. In 1994, these feelings led to a civil war: the armies of the south and the north, which have never been integrated into a single army, clashed on the battlefield. After several months of fighting, the north held the upper hand, and many leaders of the south fled the country. The defeat in the civil war did not, however, put an end to the aspirations for independence of the south, and over the years the tensions between the two parts of the country only intensified. Southern groups regularly rebelled against what they viewed as political and economic discrimination and exclusion by the regime, and Saleh retaliated by using the security forces against the southern separatists. In 2006, the tensions between the sides escalated further when the Southern Liberation Movement was established. The movement was a loose confederation of different political and social movements seeking to expand the authority of the local government, perhaps even complete separation from the north. The establishment of the movement was a catalyst for an outburst

of demonstrations and protests in the south that were forcibly suppressed by the security forces; ultimately, the movement failed, largely due to internal power struggles.[30]

The fall of Saleh's regime and the struggles within the security forces and elites in Sana'a have reignited the south's attempts to separate. The latter has taken advantage of the revolutionary wave, and increasing numbers of southerners–even those who didn't necessarily seek to undermine the unity of Yemen but rather sought to rectify the prevalent situation–have expressed their support for the separatist movement that, unlike the Houthis' struggle, has not been violent. Since 2011, the movement has been conducting what resembles an intifada using peaceful means to arouse international support for southern independence. In May 2013, on the day Sana'a marked the 23rd anniversary of the unification of Yemen, the movement's leaders organized a huge demonstration in Aden, the historical capital of southern Yemen. According to the organizers, one million people from all the southern provinces attended the demonstration and called for separation from the north. The popularity of the separatist notion in the public had begun to trickle into the south's political elite, and many of its leaders have begun supporting the separatist idea.[31]

The southern separatist ambitions were a key factor in the decision of the National Dialogue Conference to turn Yemen into a federation. While representatives from the south agreed to the concept, their demand was that Yemen be divided into two parts–the south and the north. This demand was obviously rejected by the north as it was concerned that such a division would be the first step to a split into two nations. The conference determined that Yemen would be divided into six provinces, and that the historical south would constitute two of them. Although southern representatives went along with this proposal, it seems that many in the south are opposed, worried that the four northern provinces will act in concert against southern interests. In addition, some have claimed that the division of the south into two was meant to weaken it; the division artificially separates the population and economic centers in the southwest from the oil resources and mines in the southeast. Southern leaders, including the former president of South Yemen, Salim al-Beidh, have declared that the south will not be able to accept the plan in its current format, and that one cannot rule out the possibility of a violent reaction on the part of more extremist separatists.[32] While neither the Houthis nor the southern elites

showed opposition in principle to the idea of a federation, their opposition to the proposed division into provinces approved by the National Dialogue Conference could hinder the implementation of the federation plan and quickly lead Yemen back to chaos and bloodshed.

External Challenges: A Playground for Regional and Global Struggles

Other than the destabilizing influence of internal fragmentation, the vacuum left by the fall of the Saleh regime allowed external elements that had been active in Yemen in the past to expand their influence on events in the country and steer Yemen's future direction. Today Yemen is a key arena in regional struggles, the expansion of global jihad, and the US war on terrorism.

Iran's involvement in the Yemeni arena is not a new development; evidence of Tehran's involvement goes back to Saleh's regime. While in the past this involvement was perceived by the US administration as a marginal phenomenon that entailed weapon shipments to Shiite groups in Yemen, today it seems that Iran's involvement there is of strategic significance and is expanding as the central government weakens. In April 2012, former US Ambassador Gerald M. Feierstein declared that "we do see Iran trying to increase its presence here, in ways that we believe are unhelpful to Yemen's stability and security."[33] Similar sentiments were expressed by Assistant Secretary of State for Near Eastern Affairs Jeffrey Feltman after a meeting with President Hadi.[34] The vehement US rhetoric went hand in hand with an increase in cooperation between Yemeni and US security forces on preventing and foiling Iranian weapon shipments to Yemen.[35]

The pressure on Iranian activity in Yemen increased through 2012. In July of that year, Yemen's Interior Ministry announced that an Iranian spy ring, apparently based in Sana'a, had been discovered and that an officer in the Iranian Revolutionary Guards was arrested on suspicion of having been its leader. In addition, a Yemeni court sentenced crew members of a vessel found with an arms shipment by the Yemeni Coast Guard and the US Navy in a joint operation and in January 2013 to prison terms ranging from 3 to 10 years, on charges of collaboration with Iran and weapons smuggling.[36] President Hadi made a public demand that Iran stop interfering in his country's domestic affairs, saying that Iran would "pay the price"

should it continue to do so. "We will expose them to the world," said the president, adding, "They will fail in Yemen."[37]

For Iran, involvement in Yemen is an important front in the "cold war" it is conducting with Saudi Arabia over hegemony, influence, and prestige. Iran makes extensive use of Shiite communities to surround Saudi Arabia with instability (Yemen thus joining Iraq and Bahrain). Its influence among the various factions operating in Yemen provides Iran with a presence on the ground on the southwestern border of the Saudi kingdom it can use as political pressure against Riyadh, and as means to harass Saudi Arabia at its pleasure. A steady foothold on Yemen's western coast would give Iran access to the Red Sea, a fact that could help it continue its regular arms supply to its local allies and maintain a contiguous presence near the Bab el-Mandeb Straits offering access to the Suez Canal and the Mediterranean. In addition, its involvement in Yemen allows Iran to demonstrate its regional might and the reach of its military influence.

Iran's locus of involvement in Yemen is the military support for the Houthi rebels. This support, similar to Iran's involvement in Iraq and the Levant, is effected through the Revolutionary Guards' Quds Force and, according to various reports, with the help of Hizbollah.[38] The Quds Force concentrates on creating proxies to promote Iran's interests in their regions. Iranian arms shipments intended for the Houthis (assault rifles, explosives, anti-tank weapons, and large amounts of cash, usually transferred by sea) are not significant in and of themselves compared to the weapons already flooding Yemen, especially the north, but they do allow Tehran to buy influence in Yemen and challenge Saudi Arabia's hegemony in the peninsula.

Not only does Iran assist the Houthis, but it also operates to strengthen its influence on other Yemeni factions, including the southern separatist movement and, according to the Saudis, on groups affiliated with al-Qaeda.[39] The Yemeni regime claims that Iran even tried to undermine the National Dialogue Conference. In May 2013, the Iranian ambassador to Sana'a met with head of the political branch of the Houthi movement; sources in Yemen say that this was not the first meeting between the two and that during the meeting the Iranian ambassador tried to persuade the Houthis to withdraw from the conference.[40] In addition, Hizbollah and Iran support and finance the activities of the former president of South Yemen, Salim al-Beidh, operating from Beirut and constantly promoting

the south's secession from the union.[41] By withdrawing from the Yemeni arena, Iran may quell some of the Saudi concerns and create the basis for a certain détente between the sides. This, however, would not seem to be the path Iran is choosing; Iranian involvement in Yemen continues to this day. At the end of March 2013, President Hadi accused the Islamic Republic of deep-rooted involvement in the various conflicts besetting Yemen and of supporting both the Houthi insurgents and the southern separatists.[42]

Al-Qaeda and the Threat of Radical Islam

Since 2009, and with added momentum since the beginning of 2011, al-Qaeda in the Arabian Peninsula (AQAP) and its affiliate, the Ansar al-Shariah militias have become key players in the Yemeni arena, exerting strategic influence. The Yemeni branch of al-Qaeda consists mostly of Yemenis and Saudi Arabians who found refuge in Yemen, but is augmented by men who have participated in armed conflicts in Iraq and Syria, fighters from Afghanistan, and former Guantanamo detainees. According to Washington, the organization is the most dangerous of al-Qaeda's affiliates.[43] In 2012, John Brennan, former counterterrorism advisor to President Obama and current Director of the CIA, said that AQAP is al-Qaeda's most active cell and that this represented a very serious problem for Yemen.[44] The organization's extensive international activities include an attempt on the life of Muhammad Bin Naif, the Saudi Minister of the Interior, the attempt to detonate a US airliner in the skies of Detroit on Christmas 2009, the attack on the Japanese oil tanker in the Straits of Hormuz,[45] and another attempt to blow up a US plane, thwarted by Saudi intelligence, in April 2012.[46] An analysis of AQAP's behavioral pattern since the 2011 revolution shows that the organization possesses both strategic and tactical flexibility and is capable of effectively adapting itself to opportunities and pressures on the ground and rapidly adjusting to changes in the volatile Yemeni environment. Over the past two years, the organization's ability to move efficiently and quickly along the axis from classical terrorist group to guerrilla and insurgency group seeking to hold and control territories and populations has been especially prominent.

When the political crisis in early 2011 led to the Yemeni army's focus on events in Sana'a and many military units streamed to the country's capital, the organization quickly exploited the vacuum created in the country's periphery and managed–through the use of violent raids, suicide attacks

and assassinations–to seize control of several areas in the southern part of the country, including Shabwah, Abin and Zinjibar. The organization's power and audaciousness reached a peak in April 2012 when, in an attack described as the most sweeping in the organization's history in Yemen, it captured a military base, its personnel and arms, including artillery, cannons, and tanks. Hundreds of Yemeni soldiers were killed in the attack that was only part of the organization's attempt to seize control of the Lawdar District controlling access to other key locations such as Hadramaut, Bida and Aden.[47]

As the organization grew more entrenched in southern Yemen, it initiated a strategic process of transitioning from classical terrorism to an attempt to gain a permanent hold on the area and promote a governing system in the spirit of the Shariah. This operative change was accompanied by a conceptual change regarding the treatment of the population under the organization's control. Organization members, and especially the Ansar al-Shariah members, showed relative flexibility and moderation in applying Shariah law. They began functioning as the local administration, supported and allied themselves with tribal leaders, instituted a system of settling inter-tribal conflicts, and even provided services such as defense, water, food, basic healthcare and religious schools. This was meant to generate tribal and local community support and exploit the resentment towards the central government in Sana'a. Nonetheless, within a short period of time and as the organization's control of the area deepened, al-Qaeda members reverted to their traditional behavior and began enforcing their fundamentalist Islamic values aggressively and cruelly. This caused thousands of local resident to flee the al-Qaeda controlled areas and establish so-called popular committees[48] that sought to fill the governmental and security vacuum left by the state and to protect the population against al-Qaeda.[49]

Al-Qaeda's hold on parts of southern Yemen continued until May 2012, when Hadi ordered a comprehensive military attack against al-Qaeda's strongholds. More than 20,000 regular soldiers, supported by mercenary militias from the southern tribes, participated in the operation. US advisors were involved in planning the attack, while the Saudi regime provided a significant part of the financing. Ground forces received extensive aerial support; while the president attributed this support to the Yemeni air force alone, the backroom talk was of extensive US unmanned aerial vehicles' involvement. The operation lasted about two months. Many al-Qaeda

activists were killed and the organization was driven out of the areas it had controlled, pulling back to its natural hiding spots in the center of the country.[50] As a result, the organization reverted to its classical mode of terrorist activity before 2011. Its members embarked on a serious campaign of deadly attacks and assassinations aimed at senior figures in Yemen's security and intelligence communities, army units operating in the area, and tribal and community leaders cooperating with the regime. The organization succeeded in rebuilding its force and set up an extensive network of terrorist cells, acquired advanced technological capabilities, and created effective intelligence gathering infrastructures to provide support for its attacks. The organization also expanded its involvement in criminal activities to finance the reconstruction of its force. Its members take part in robberies, extortion, blackmail, smuggling, and abducting foreign citizens.[51]

The weakened state of Yemen's security forces–the result of reforms and structural changes–has provided al-Qaeda with breathing room and maneuvering space. It seems that they are not afraid of attacking government institutions even in the regime's home court. Its operatives blew up a bus transporting soldiers, attacked the Defense Ministry officess in the heart of Sana'a, and broke into detention facilities in order to liberate their comrades. These attacks were especially bold and indicated highly developed tactical skills: they included complex operations that combined the use of powerful explosives and assaults by commando units.[52] The organization swung back into action in southern cities and carried out several successful raids in Hadramaut and Bida. It seems that it is trying to reestablish itself within the population and discontinue its cooperation with the regime and security forces. Two years after it was dealt a serious blow, and despite the ongoing pressure exerted by the security services and the extensive US assassinations in Saudi Arabia, AQAP's determination and operational flexibility have contributed to its rising power.

Conclusion

Yemen, one of the most complicated of the Middle Eastern arenas, is currently undergoing an intensive process of reconstruction with no clear indication of when and how it will end. An analysis of the process may provide some insight as to possible processes and scenarios elsewhere in the Middle East in the post-Arab Spring reality. Yemen's location in the periphery of the Middle East has to some extent marginalized it in the context of the

international strategic discourse. This could be a missed chance because, as has been said before, the route taken by Yemen since the beginning of the Arab Spring allows an examination and understanding of key processes taking place–or likely to take place –in other Arab countries as well.

First, the Gulf States, the United States and other elements in the international community played a role in arranging for Saleh to step down from the presidency and the transition of authority to the interim government. An analysis of this involvement could provide important insight as to the effectiveness of international arbitration in resolving the political and military crises rocking the nations of the Middle East. Developments in Yemen show that the combination of intensive mediation on the part of Arab elements, such as the Gulf Cooperation Council, the Arab League and Arab nations, on the one hand, and pressure on the part of the superpowers and the international community on the other, could serve as a catalyst to setting a process of political arrangement in motion. However, external intervention can by no means serve as a guarantee for the success of such a process or the stabilization of a country and its political system. The experience and lessons learned from the intervention in Yemen may also generate insight relevant to the effect and limits of international intervention in Syria, though the international constellation around the Syrian arena is more complex since the involvement of players such as Russia and Iran creates a split in the international community.

Second, an analysis of the Yemeni political system since Saleh stepped down also provides insight about the challenges created by the redistribution of the loci of power among the various elites. Developments in Yemen indicate that a formal change in government is not enough to bring about stability because the influence of the old elite is tied to informal connections and loyalties that prevent real reforms and change. In addition, one can generate many insights from an analysis of the Yemeni national dialogue and the reorganization of the security services in terms of the reconstruction undergone by the nations that experienced the Arab Spring.

Third, an examination of the conduct of al-Qaeda in Yemen sheds light on the strategic changes taking place within the global jihad movements in the course of the Arab Spring. The main change we can point to is al-Qaeda's shift in focus from classical terrorism to an attempt to establish a long-term hold on regions where the weakening of the regime has created a governmental vacuum. AQAP is a pioneer in this trend; it had even

published an official document of recommendations to other al-Qaeda affiliates in which it suggest a comprehensive strategy for action for seizing control of a territory and holding onto it.[53]

The Yemeni arena has much to teach us about the dangers posed by al-Qaeda and the effectiveness of counterterrorism strategies, such as comprehensive military attacks or assassination campaigns using drones. Nonetheless, the dynamics reviewed in this paper indicate that, even at its weakest, the state is still the most dominant and powerful element in its territory and that the radicalization in the attempts of subversive forces to damage its sovereignty can only be expected to be met with determined, forceful countermeasures.

Finally, Yemen–after the unification of the emirates–is the first Arab nation expected to take the federal route, a process that may be repeated in other countries as well, such as Syria, Libya and Iraq. Keeping an eye on the implementation and development of the federal process in Yemen may provide important insight on the effectiveness of this political configuration for creating governing stability and preventing widespread violence.

Notes

1 Ginny Hill, Peter Salisbury, Léonie Northedge, and Jane Kinninmont, "Yemen: Corruption, Capital Flight and Global Drivers of Conflict," *Chatham House* (September 2013): 8-9.

2 W. Andrew Terrill, "The Conflicts in Yemen and US National Security," *Strategic Studies Institute*, January 1, 2011.

3 The Failed States Index 2013, *The Fund for Peace*, 2013, http://ffp.statesindex.org/rankings-2013-sortable.

4 "Yemen Begins New National Talks," *al-Jazeera*, June 8, 2013, http://www.aljazeera.com/news/middleeast/2013/06/201368153532856750.html.

5 Mustafa Ahmad Nuaaman, "Opinion: Yemenis Have Grown Tired of the National Dialogue," *Asharq al-Awsat*, August 19, 2013, http://www.middle-east-online.com/english/?id=61877; Fawaz Traboulsi, "Yemeni Revolution Enters Third Year," *al-Monitor*, February 20, 2013, http://www.al-monitor.com/pulse/politics/2013/02/yemeni-revolution-third-year.html; Sama'a Hamdani, "Yemen's National Dialogue behind Closed Doors," Atlantic Council, June 17, 2013, http://www.atlanticcouncil.org/blogs/menasource/yemens-national-dialogue-behind-closed-doors.

6 Hamdan al-Rahbi, "Yemen: Hadi announces conclusion of national dialogue," *Asharq Al-Awsat*, January 22, 2014, http://www.aawsat.net/2014/01/article55327827.

7 "Yemeni Houthi Representative in National Dialogue Killed−Source," *Reuters*, November 22, 2013, http://uk.reuters.com/article/2013/11/22/uk-yemen-assasination-idUKBRE9AL0UZ20131122.
8 "Regions' Committee Transforms Yemen into Six-Region Federation," *NDC*, February 10, 2014, http://www.ndc.ye/news.aspx?id=3051.
9 Faisal Darem, "Yemen national dialogue conference concludes," *al-Shorfa*, January 24, 2014, http://al-shorfa.com/en_GB/articles/meii/features/2014/01/24/feature-02.
10 Sasha Gordon, "Mutiny in the Yemeni Military," AEI Critical Threats Project, July 10, 2013, http://www.criticalthreats.org/yemen/gordon-mutiny-yemeni-military-july-10-2013.
11 "Yemen President Orders Military Trial for Saleh's Rebelling Half-Brother," *The National*, April 16, 2012.
12 Robert F. Worth, "Even Out of Office, a Wielder of Great Power in Yemen," *New York Times*, January 31, 2014, http://www.nytimes.com/2014/02/01/world/middleeast/even-out-of-office-a-wielder-of-great-power-in-yemen.html?_r=0.
13 Abubakr al-Shamahi, "Sanctioning You-Know-Who," *a-Sharq al-Awsat*, March 5, 2014, http://www.aawsat.net/2014/03/article55329693.
14 "Yemen Troops Encircle Ex-President Mosque amid Coup Fears," *Gulf News*, June 15, 2014, http://gulfnews.com/news/gulf/yemen/yemen-troops-encircle-ex-president-mosque-amid-coup-fears-1.1347533.
15 Thomas Juneau, "Yemen and the Arab Spring: Elite Struggles, State Collapse and Regional Security," *Orbis* 57, no. 3 (2013): 408−23.
16 Crisis Group, "Yemen's Military-Security Reform: Seeds of New Conflict?" *Middle East Report* 139 (2013): 10-13; Michael Knights, "The Military Role in Yemen's Protests: Civil-Military Relations in the Tribal Republic," *Journal of Strategic Studies* 36, no. 2 (2013): 276-82.
17 Sasha Gordon, "A New Wave of Military Restructuring Decrees in Yemen," AEI Critical Threats Project, April 11, 2013, http://www.criticalthreats.org/yemen/gordon-new-wave-military-restructuring-decrees-yemen-april-11-2012.
18 "Yemen Blasts Security Forces," *Middle East Newsline*, February 18, 2014.
19 Crisis Group, p. 20.
20 Hill, Salisbury, Northedge, and Kinninmont, "Yemen: Corruption, Capital Flight and Global Drivers of Conflict," p. 28.
21 "Al Qaeda Linked Group Blows up Gas Pipeline East of Yemen," *al-Arabiya*, April 27, 2012.
22 David Arnold, "Saudi Deportation Policies Impact Yemen," *Voice of America*, August 15, 2013.
23 "Hunger in Yemen: Disaster Approaching," *The Economist*, April 21, 2012.
24 Inbal Nissim-Lubaton, "The Youth Rebellion and the Challenges of the Failing Yemeni State," in *The Persian Gulf and Arabian Peninsula: Culture and*

Nations in Transition, eds. U. Rabi and S. Yannai (Tel Aviv: Moshe Dayan Center for Middle Eastern and African Studies, 2014).

25 Hill, Salisbury, Northedge, and Kinninmont, "Yemen: Corruption, Capital Flight and Global Drivers of Conflict," p. 12.

26 Hammoud Mounassar, "Yemen Houthi Rebels Overrun Tribal Strongholds," *Arab News*, February 2, 2014, http://www.arabnews.com/news/519316; Mohamed Vall, "The Rise of Yemen's Houthis," *al-Jazeera*, February 12, 2014, http://blogs.aljazeera.com/blog/middle-east/rise-yemens-houthis.

27 Arafat Madabish, "Yemen: Hashid and Houthis Agree Ceasefire," *Asharq al-Awsat*, February 5, 2014, http://www.aawsat.net/2014/02/article55328540.

28 "Yemen rebels oppose six-region federation," *al-Jazeera*, February 11, 2014, http://www.aljazeera.com/video/middleeast/2014/02/yemen-rebels-oppose-six-region-federation-2014211101417410323.html

29 "Yemen: Houthis, Army Exchange Accusations over al-Jawf Violence," *Asharq al-Awsat*, March 1, 2014. http://www.aawsat.net/2014/03/article55329536.

30 Hill, Salisbury, Northedge, and Kinninmont, "Yemen: Corruption, Capital Flight and Global Drivers of Conflict," p. 12; Peter Salisbury, "Yemen's Southern Intifada," *Foreign Policy*, March 13, 2013.

31 Haytham Mouzahem, "South Yemen Activists Push for Independence," *al-Monitor*, May 31, 2013. http://www.al-monitor.com/pulse/originals/2013/05/south-yemen-movement-al-qaeda-threat-exaggeration.html.

32 Yara Bayoumy, "Yemen's Federal Plan a Bold Idea, But Many Hurdles Remain," *Reuters*, February 23, 2014. http://www.reuters.com/article/2014/02/23/us-yemen-politics-analysis-idUSBREA1M05720140223; Joseph A. Kechichian, "Yemen in Transition - and in Turmoil," *al-Jazeera*, February 6, 2014, http://www.aljazeera.com/indepth/opinion/2014/02/yemen-transition-turmoil-2014264255740696.html

33 "Iran Continues to Mess Up in Yemen," *Arab News*, April 18, 2012, http://www.arabnews.com/node/411280.

34 "Political Unrest in Yemen," *al-Arabiya*, March 30, 2012, http://english.alarabiya.net/views/2012/03/30/204180.html.

35 Eric Schmitt and Robert F. Worth, "With Arms for Yemen Rebels, Iran Seeks Wider Mideast Role," *New York Times*, March 15, 2012, http://www.nytimes.com/2012/03/15/world/middleeast/aiding-yemen-rebels-iran-seeks-wider-mideast-role.html?pagewanted=all.

36 "Yemen Jails Crew over Arms Shipment from Iran," *The Daily Star*, November 12, 2013, http://www.dailystar.com.lb/News/Middle-East/2013/Nov-12/237611-yemen-jails-crew-over-arms-shipment-from-iran.ashx#ixzz2vYKgYL5C.

37 "Yemen President Warns Iran to Stop Meddling," Washington Examiner, July 18, 2012, http://www.washingtonexaminer.com/yemen-president-warns-iran-to-stop-meddling/article/2502548.

38 Michael Segall, "Iran Targets Yemen," *Jerusalem Issue Brief* 12, no.9 (2012).

39 Muaad al-Maqtari, "Saudi Arabia Accuses Iran of Supporting Ansar al-Sharia in Yemen," *Yemen Times*, April 30, 2012, http://www.yementimes.com/en/1568/news/781/Saudi-Arabia%C2%A0accuses%C2%A0Iran-of-supporting-Ansar-Al-Sharia-in%C2%A0Yemen.htm.

40 Haytham Mouzahem, "Iran's Angle in Yemen," *al-Monitor*, May 14, 2013, http://www.al-monitor.com/pulse/originals/2013/05/iran-angle-yemen-relations.html.

41 Raghida Dergham, "Foreign Minister Criticizes Hezbollah, Iran Roles in Yemen," *al-Monitor*, May 14, 2013, http://www.al-monitor.com/pulse/politics/2013/10/yemen-foreign-minister-interview-iran-hezbollah.html.

42 "Yemen's President Accuses Iran of Meddling," *al-Arabiya News*, March 31, 2014, http://english.alarabiya.net/en/News/middle-east/2014/03/31/Yemen-s-president-accuses-Iran-of-meddling.html.

43 Kareem Fahim, "Militants and Politics Bedevil Yemen's New Leader," *New York Times*, April 23, 2012, http://www.nytimes.com/2012/04/23/world/middleeast/militants-and-politics-bedevil-yemens-new-president.html.

44 "The United States: We Will Remove the al-Qaeda Cancer from Yemen,"*Maariv- NRG Online*, May 8, 2012.

45 Attack on Tanker Perpetrated by Abdullah Azzam Brigades, Identified with AQAP.

46 Scott Shane and Eric Schmitt, "Qaeda Plot to Attack Plane Foiled, US Officials Say," *New York Times*, May 7, 2012, http://www.nytimes.com/2012/05/08/world/middleeast/us-says-terrorist-plot-to-attack-plane-foiled.html.

47 "222 Dead in Qaeda Battle for Yemen's Loder," Asharq al-Awsat, April 14, 2012, http://www.aawsat.net/2012/04/article55242439.

48 Yaser al-Yafei, "Yemen: Popular Committees Take Control," *al-Akhbar English*, April 19, 2012, http://english.al-akhbar.com/node/6353.

49 Daniel Green, "Al-Qaeda's Soft-Power Strategy in Yemen," *Policy Watch* (January, 2013): 2-3.

50 Terrill, "The Conflicts in Yemen and US National Security," pp. 46-50.

51 Daniel Green, "Al-Qaeda's Resiliency in Yemen," *Policy Watch*, (January 23, 2013): pp 1-2; Terrill, "The Conflicts in Yemen and US National Security," pp 50-52; Farea al-Muslimi, "Yemen Plagued by Assassinations," *al-Monitor*, October 18, 2013, http://www.al-monitor.com/pulse/originals/2013/10/assassinations-plague-yemen.html; "Armed Men Attack Yemen Police Headquarters, Wounding Seven," *Reuters*, December 31, 2013, http://www.reuters.com/article/2013/12/31/us-yemen-blasts-idUSBRE9BU00G20131231.

52 Shaul Shay," Yemen under Attack," *BESA Center Perspectives* no. 226, December 12, 2013, http://besacenter.org/wp-content/uploads/2013/12/perspectives226.pdf; "Inmates Flee after Prison Blast in Yemen," *IOL News*, February 14, 2014,

http://www.iol.co.za/news/world/inmates-flee-after-prison-blast-in-yemen-1.1647179#.UxiLT2xWHVI;
Hakim Almasmari, "Blast Targets Bus Carrying Soldiers in Yemen," *CNN*, August 26, 2013,
http://edition.cnn.com/2013/08/25/world/meast/yemen-blast.

53 Daniel Green, "Al-Qaeda's Shadow Government in Yemen," *Policy Watch*, December 12, 2013.

Managing Intellectual Property in the Defense Establishment: Opportunities and Risks

Shmuel Even and Yesha Sivan

In Israel, there is a consensus on the value of all knowledge generated in the defense establishment and its contribution to the economy. But in the State Comptroller's report of March 2014, the management of intellectual property (IP) at the Ministry of Defense was described as an ongoing fiasco, with the blame ascribed to both the Ministry of Defense and the Ministry of Finance. This essay seeks to contribute to the discourse on remedying the flaws and suggest some organizing principles in the management of IP, while considering both the needs of the defense establishment and those of the Israeli economy. The essay proposes that the IDF manage the IP under its purview as part of the organization's knowledge management, but not engage in financial IP transactions; a specially designated company should be established in the Ministry of Defense that would be responsible for this. At present, the chances of such a move succeeding seem low, but even if it results only in an improvement of the management of technological knowledge in the defense establishment, it would constitute an achievement. Knowing that the idea of commercializing knowledge has been seriously and thoroughly examined is important in and of itself.

Key words: knowledge management, commercialization of knowledge, defense establishment, Ministry of Defense (MoD), Israel Defense Forces (IDF), State Comptroller, defense budget, Israeli economy, high-tech, cyberspace

Dr. Shmuel Even is a Senior Research Associate at INSS.
Prof. Yesha Sivan is the Director of the Coller Institute of Venture at the Management Faculty at Tel Aviv University.
The essay was written as part of the INSS Economics and National Security Research Program, supported by the Joseph and Jeanette Neubauer Foundation.

Introduction

Many technologies serving humankind started out as developments for the military, including the microwave, radio, digital camera, internet, GPS, and more.[1] All of these have vast economic value. The Israeli defense establishment (Ministry of Defense, IDF, etc.) develops and improves technologies that subsequently enter the civilian sector, but the knowledge travels from the defense establishment to the economy in an unsupervised, unmanaged way, without any compensation.

The fundamental question at stake is this: should a state deal with the management and commercialization of knowledge developed in its institutions in general and its defense establishment in particular? The analysis in this essay can help formulate an opinion on the matter. The essay's starting point is the State Comptroller's March 2014 report, according to which the Minsitry of Defense (MoD) should manage its intellectual proprety (IP) in order to capitalize on it, or at least make a serious attempt to do so. The results would then either lead to a codification of the issue or to its being removed from the national agenda. Therefore, the essay will attempt to outline how best to meet this challenge while minimizing risks and maximizing opportunities.

The discussion on the management of IP in the defense establishment requires an understanding of several concepts:

a. *Knowledge management* refers to the entire system of development, follow up, control and oversight in the context of the creation of internal knowledge (within the defense establishment), receipt of external knowledge (from outside the establishment), and transfer of the knowledge, including the distinction between existing knowledge and knowledge that has yet to be developed.
a. *Intellectual property* is the general term for the rights to intangible goods and resources resulting from thought processes. IP includes inventions, technologies, work processes, patents, and any sort of information or knowledge having commercial potential (henceforth "information"). The rights of IP are protected by means of patents, copyrights, confidentiality clauses, and so on.
a. *IP management* is the systematic management of knowledge defined as IP or likely to become such, including its production, registration, classification and commercialization. Management touches on knowledge created within the system and on the ways its commercialization affects

the organization (in our case, the defense establishment), the people in it, and even global and Israeli companies.

a. *Commercialization of IP* is the range of actions involved in generating an economic return on IP. This may include the process of turning IP into something with commercial potential and then trading with it. Trade in IP can involve selling the rights to the IP or the products developed on its basis, or receiving royalties.

The Current State of Affairs

The Problem According to the State Comptroller's Report

In March 2014, the Israeli State Comptroller issued a report on the management of IP at the Ministry of Defense. The report states that the MoD's lack of management of IP is an ongoing fiasco and that "the MoD has, for many years, neglected the handling of Israel's defense IP assets under its purview and owned by the IDF."[2] According to the report, the MoD has no policy, suitable directives[3] or central body handling the issue. As a result, the MoD does a poor job of managing, following up on, and supervising the assets of the IP developed on its watch or with its financing, including the military industries, and even following up on its subsequent uses. For example, the IDF has no current data on the quantity, type, and value of IP assets in its possession.

The State Comptroller's report indicates that from 2004 until 2012 nine different teams tackled the issue. All of them pointed to the many flaws in the management of IP at the MoD and formulated recommendations to deal with the issue and improve the situation. However, the ministry's conduct was characterized by "foot-dragging and a lack of resolve." The major flaws were lack of policy on managing the wealth of IP assets in the ministry and how to realize them economically, while not receiving any compensation for transferring ministry knowledge to third parties. "These failings cause real damage both to the ministry's ability to manage its IP and its ability to realize the economic potential inherent in its IP. The MoD must address these failings without delay."[4]

The report also noted that the Israeli Accountant General, as the executor of the Ministry of Finance responsible for handling the nation's assets including intangible ones, failed to fulfill his obligation. The report indicated his neglect when it comes to regulating IP in the Ministry of Defense, supervising the IP assets at the ministry's disposal and the use

that is made of them. Interestingly, the Accountant General stated that the ministry's IP assets have great inherent economic potential, and therefore recommended to institutionalize the field of IP in the Ministry of Defense.[5]

The Israeli State Comptroller's Office noted in the 2013 Annual Report (March 2014) that MoD Director General Maj. Gen. (res.) Dan Harel instructed that steps be taken to remedy the significant failings that emerged during the review.

Completing the assessment of what is happening in the government sector is the seminal study issued in April 2014 by the Haifa Center for Law and Technology at the University of Haifa, which examined the current state of affairs of the policy on the commercialization of government sponsored R&D in general. The study's findings also indicated the lack of a consistent policy on patent registration of products of research funded by the government and their commercialization. "This state of affairs does not serve the goals of government sponsored R&D and is at odds with the principles of good governance." The study's conclusions reveal that although it would be unwise to dictate a single policy for all forms of IP sharing, development and commercialization of government knowledge, it is necessary to create a unifying framework for defining the decision makers' and policy framers' considerations on these issues. The study therefore suggests a framework for defining and identifying the relevant concerns regarding the commercialization of products resulting from government sponsored R&D by means of patents.[6]

The Knowledge Created in the Defense Establishment and its Importance to the Economy

Managing knowledge in Israel's defense establishment represents a unique instance of knowledge management in public institutions. The knowledge created in the defense establishment is the result of the formulation of new ideas, development, manufacturing, generation of lab data, experiments, operational use, lesson learning, training and instruction, and more. The many challenges and the access to creative manpower render Israel's defense establishment unique. These advantages greatly affect the development of the Israeli economy, especially in the high-tech sector. The derived added value will increase as the need for new and innovative technologies surges. Israel's prominent position in the global cyber market is an excellent example of untapped IP assets.

The act of creating knowledge with commercial potential in the defense establishment occurs in several bodies: those in charge of planning and managing R&D in the MoD, the IDF, and the security industries, both government owned (Israel Aircraft Industries, Rafael, and Israel Military Industries) and private or semi-private ones acting on the government's behalf (Elbit Systems, mPrest Systems and others), research institutions and in academic settings where R&D is conducted for the Ministry of Defense. In addition, the Administration for the Development of Weapons and Technological Infrastructures is a joint body belonging to the MoD and the IDF. Quite a few projects were initiated by the army's branches and corps, following which they were executed by the defense industries. The engineers in the defense establishment characterize, provide advice and ensure that the weapons developed and manufactured meet the demands with a profound understanding of operational needs.[7]

Furthermore, IDF units create IP assets in fields such as technological developments for the sake of intelligence gathering and cyberspace; weapons, securing and fortification development; warfare doctrines; experimental data; and more. The State Comptroller's report also stated that an officer in Unit 8200 reported that the unit is brimming with IP assets that could be traded to the defense industries, but that there is no suitable mechanism for making it happen: "there is no strategic mechanism defining what may be released and what must be released."[8]

The knowledge created in the defense establishment feeds the economy by contributing to the GNP, investments, and employment. The high-tech sector directly employs close to 9.5 percent of the country's workforce and is a critical source for the GNP, income from taxes and exports. One must remember that increasing exports of Israeli goods and services is a prerequisite of growth, because Israel's own market is small and its economy is export oriented. This dependence forces Israel to maintain a high level of competitiveness and adapt itself to structural changes in the global market. Because Israel has no competitive advantage in terms of a cheap workforce, this is possible only if Israel remains a leader in the high-tech sector.

Many technological companies have been established in Israel by or via former members of technological units in the defense establishment, in part because of the knowledge base and experience they gained during their army service. The financial press has pointed to former members of

military intelligence's Unit 8200 as being involved in the founding of some internationally leading tech companies: Check Point Software Technologies Ltd., which deals with information security, valued at $13.8 billion on the NASDAQ (November 2014); Verint Systems Inc., which deals with information gathering, retention and analysis for business intelligence, valued at $3.5 billion on the NASDAQ; NICE Systems Ltd., which specializes in telephone voice recording, data security and surveillance, valued at $2.8 billion on the NASDAQ; and more. The technological and operational knowledge emanating from the IDF also represents a critical resource for Israeli security companies. In 2013, Israel signed contracts for selling weapons and security equipment estimated at $6.5 billion.[9]

The defense establishment is proud of its contribution to the economy. In December 2013, Maj. Gen. Orna Barbivai, then- head of the IDF's Manpower Directorate, said that, "if one takes a broad, national, systemic view, it is easy to see how the IDF and other security services are the engine pulling the country's economic growth and that its manpower is a competitive edge by any standard...One can see the correlation between the advanced startups, in Israel and abroad, and their roots in the army."[10] In January 2011, then- Maj. Gen. Ami Shafran, head of the IDF's Teleprocessing Branch, said that "the IDF represents a key technological hothouse for the high-tech sector...One of the products of this technological hothouse is the human capital that assimilates into Israeli R&D, higher education and industry." According to Shafran, "from a market point of view, spending on developing technological human capital in the IDF in the field of teleprocessing, whose designation is primarily security, also represents an investment yielding significant economic returns for the economy and a central part of Israeli exports."[11]

One could say that the defense establishment–because of investments, authority given to young people, and operational demands–has, in recent decades, served as a significant catalyst for the founding of new Israeli companies and has created a competitive edge for Israel on the global market. However, global trends in R&D and the founding of new companies are generating new challenges.[12] Global competition and the need to be the first to hit the global market mean an accelerated rate of development and the need for rapid availability of international contacts and capital. Entrepreneurs are therefore eager to reach investors and strategic contacts to finance the developments that can take them into new markets and issue

the companies on global stock markets as soon as possible. This gives rise to a question: will inventions whose origins lie in centers of knowledge in Israel, including the defense establishment, continue to create the same value for the Israeli economy in the future, or will they quickly find their way to international companies?

IP Movement from the Defense Establishment to the Business World

The IP generated by the defense establishment currently makes its way to the outside world via personal and institutional routes.

The Personal Route–Via Alumni

IP developed in the defense establishment technological units moves into the free market via the people who served in them. Officially, the Ministry of Defense's policy does not allow the transfer of information this way, but in practice this is not supervised by the ministry, as many companies employ former members of the MoD departments. However, as far as anyone knows, no concrete information has been published on the transfer of specific IP from the defense establishment, and no one has made any kind of assessment of the value of the IP that has moved into the free market via the personal route. It should also be noted that given the current state of affairs, it is difficult to isolate the contribution of protectable IP from the professional knowledge and experience accrued by graduates of the defense establishment and from the added value the IP accrues in the civilian business setting. The defense establishment is losing potential income from this IP, as noted by the State Comptroller, but as long as it is used in Israeli companies the local economy and the state are at least benefiting greatly, albeit indirectly. This is not the case when IP is realized in its early stages within foreign companies abroad.

The Institutional Route–the Military Industries

These are cases in which an idea, definition, performance testing and sometimes even development funding and manufacturing all happen within the defense establishment, whereupon the industries may use the information and products also on behalf of other clients. Sometimes, the MoD receives royalties for this use, should its rights be specifically noted in the work orders for projects that the military industries carry out as contractors.

It should be noted that the transfer of knowledge from the companies used (through sub-contractors or previous employees) is supposed to be handled in the setting of the commercial company interested in protecting the IP even if the information is affiliated with the defense establishment. When this happens in companies fully owned by the government, the state receives full compensation for the IP because the defense establishment and these companies have one single stockholder–the government. But when it happens in defense industries not owned by the government, the defense establishment is liable to lose potential income. The growing use made by the defense establishment of external companies is another reason for following up on what happens to the IP developed in the defense establishment or with its funding.

Institutionalizing the Management Of IP in the Defense Establishment–Opportunities and Risks

In changing the current situation by institutionalizing the management of IP of the defense establishment and commercializing it, as required by the State Comptroller's report, there are both opportunities and risks for the defense establishment and for the economy, as is demonstrated below.

Opportunities for the Defense Establishment in Managing IP

a. *Contribution to the improvement of knowledge and organizational memory management.* Documenting and managing IP is a necessary component in improving the defense establishment's ability to attain its goals long before touching upon the issue of commercializing knowledge. Insufficient retention of technological knowledge in the defense establishment arouses some troubling questions: are time and resources being wasted in certain units as they redevelop technological products already developed in the past? Do certain units promote technological abilities already developed or being developed in other units due to a lack of central control of technological information? These questions are particularly pertinent for units in the IDF and the intelligence community. Compared to the IDF, the defense industries have an advantage in knowledge preservation because they make institutionalized efforts to retain accumulated knowledge over a long period of time by a cadre of permanent employees who do not end their service after three years or are transferred from one position to another, as is customary in the

army. Nonetheless, even with regard to these companies, the question arises: is there sufficient documentation of knowledge and is there a sharing of knowledge among government owned companies?

b. *Economic compensation for the defense establishment.* According to the State Comptroller, "maximizing the economic potential in IP assets may provide the MoD with many added financial resources that could significantly increase the state's budget sources in general and that of the MoD in particular."[13] At stake is the compensation expected from the system's income resulting from the commercialization of IP through products such as various types of communications devices, command and control systems, information security products, optics, drones, satellites, voice processing, picture processing, and so on.[14] Additional income would be generated by means of equipment sale, rendering services, real estate, etc.

c. *Contribution to retaining personnel in technological units.* Currently, given the lack of management of IP, the possibility of extracting IP without compensation is liable to tempt the most outstanding personnel in the system to leave as soon as they can. In addition, if the IDF gives up on copyrights, its employees or those serving in it are discriminated against, compared to their cohorts who leave the system and use the knowledge for their own gain. By contrast, if there is informed management, the possibility that personnel serving in the technological units become partners in the creation of IP on the forefront of global technology could maintain a high level of motivation to enlist in these units and perhaps also reduce the numbers leaving the army during high-tech booms around the world. Furthermore, the possibility of recruiting new workers not subject to long service in the defense establishment–for example, 3-6 year stints–to be part of the system of knowledge development and experimentation as part of their own professional development should be examined. This would encourage knowledge to flow in the opposite direction: from outside the system inwards.

d. *Contribution to the defense establishment's operational capabilities.* It is only reasonable to assume that in various units there are ideas that remain unrealized because of limited resources or lack of economic feasibility, especially if the unit would be the product's only customer. By means of an orderly transfer of IP to businesses, it would be possible to develop more ideas at lower cost, thereby increasing the number

of products that IDF units could purchase from the industries. For example, it may be that somewhere in the IDF there is an idea for a new explosives detection device or one for conducting underground surveys. Orderly work with a business for joint development could allow the development of products for marketing to meet both the needs of the defense establishment and the global market.

e. *Preventing operational harm.* Increasing command and control would reduce the rate of unsupervised leakage of classified IP leaving the system liable to fall into hostile hands.
f. *Protecting the IDF's ability to use technology.* Situations are liable to arise in which IP originating in the defense establishment is patented by a civilian entity, which could limit the defense establishment and defense industries' ability to use it.
g. *Improving the governance of national resources.* Meeting directives and procedures as noted in the State Comptroller's report.

Risks to the Defense Establishment in Managing IP

a. *Risk of becoming overly preoccupied with IP for civilian needs.* At times, this could skew the priorities of the units away from dealing with the most important security needs.
b. *Risk of financial loss.* The way to turn an idea into protected IP can be long and costly. Furthermore, conflicts about ownership of the IP that could lead to costly legal battles are liable to erupt. This could also damage the defense establishment's image. In any case, maximizing the income of information developed in the defense establishment is complex, and it is best not to develop higher than realistic expectations of the financial gains this route can represent. For example, if compensation takes the form of stocks the state receives from the sale of IP, it could deplete the funds raised by the company.[15]
c. *Risk to human resources.* Strengthening the interface between civilian industries and the defense establishment is liable to increase the temptations for many talented personnel to leave the defense establishment, especially during high-tech booms. In addition, over-supervision of knowledge is liable to deter experts from working in the defense establishment.
d. *Risk of establishing a mechanism that will only perpetuate itself.* One of the dangers is the establishment of a body that will fulfill its bureaucratic

objective but lack sufficient motivation to maximize the value of the knowledge because it will be part of the defense establishment structure whose performance is not tested on the basis of the results of knowledge commercialization.

e. *Growing risk of exposing sensitive information.* The management of IP, the sharing of knowledge, and the establishment of knowledge bases are inherently liable to increase this risk, especially when more information is exposed to more people who will want to make use of it on global markets.

Opportunities for the Economy in Managing IP in the Defense Establishment

a. *Improving the flow of information to the market.* It is reasonable to assume that the defense establishment currently suffers from loss of information because it never makes it to the market. For example, in March 2014, Brig. Gen. (res.) Prof. Chaim Eshed, chair of the military space committee in the National Council for R&D, said: "in cyber, we are breaking new ground...This is the field in which we've dealt for more than 20 years, even if we didn't always call it cyber. Still, the defense establishment has greatly invested in turning military technologies into dual-purpose technologies that can be marketed in the civilian world, but we're not there yet."[16]

b. *Giving priority to the use of IP to benefit Israel.* Globalization encourages routes in which IP moves directly abroad (also with the help of defense establishment alumni) without contributing to the Israeli economy. This route offers Israeli entrepreneurs the opportunity to work in places where there is access to capital, large markets and higher standards of living and working. In some cases, tempting offers come to Israeli entrepreneurs directly from abroad. In addition, many global companies, by means of their development centers in Israel, keep a watchful eye on new ideas emerging from Israel. This makes it possible for foreign companies and nations to enjoy the profits of IP developed with resources belonging to the State of Israel. Control of IP developed by the nation would allow it to give priority to using this IP for the good of the country and its economy (more on this below).

c. *Institutionalizing the flow of information.* This would protect companies and other knowledge users from claims and lawsuits, and increase market equality in receiving information. The more uses there are for

the information, the more knowledge will expand, thereby multiplying the number of new opportunities in the encounter among entrepreneurs, consumers, financing and science.

d. *Greater social equality.* The issue of economic inequality in Israeli society is at the heart of public discourse. Generally speaking, no one disputes the right of personnel exiting the public sector to maximize the knowledge and skills they acquired for creating economic wealth once they enter the private sector. However, in the future it will become more difficult to ignore the question of whether or not the public is entitled to this wealth, with so much IP originating with the defense establishment.

Risks to the economy in managing IP in the defense establishment

Damage to the Flow of Information

The State Comptroller's report does not relate to the question of how to ensure that the great economic potential inherent in IP assets of the MoD and the IDF will in fact be maximized on behalf of the Israeli economy. If the defense establishment keeps its IP to itself (a risk liable to arise from an extreme interpretation of the State Comptroller's report) as the result of rigid procedures and directives and without establishing a mechanism for the transfer and application of information, the damage to both the economy and the defense establishment is liable to be significant, because several technological developments with value to the defense industry, the super-technology industries, and the Israeli GNP in general could be prevented. Therefore meticulous registration of intangible assets and their safekeeping must occur in tandem with a solution for the application of the information. It is likely that the current state of affairs, in which information is transferred without compensation to the defense industries and the economy through personnel that served in technological units and are now working on the free market, is preferable to the state compared to a situation in which rigid procedures will prevent its use altogether.

Factors Liable to Turn this Risk into a Reality

a. *The establishment of a rigid bureaucratic mechanism within the Ministry of Defense.* For example, for the defense establishment, which is not oriented by nature towards economic profits, it is very easy to delay and even prevent the release of information to the free market on the

basis of its being classified or restricted. Furthermore, in the fast-paced world of accelerated technological developments, such delays may decrease attractiveness of the IP created in the defense establishment and its competitive edge on the global market.

b. *Failed intra-system cooperation.* It is clear that the subject under discussion is not likely to head the agenda of any commanding officer and may even be viewed as a nuisance. Former defense establishment personnel can bypass the system's ownership of the IP by making certain alterations. In extreme cases, there is a risk that some personnel within the defense establishment will prefer to keep certain knowledge with commercial potential to themselves rather than register it with the defense establishment in the first place.

Interim Summary

Proper IP management in the defense establishment can maximize opportunities and minimize risks. The following are suggested steps that can be taken to this effect.

First, regulation is needed for the sake of controlling and supervising the information. This stage should begin with an orderly registration of information. Second, it is necessary to institutionalize the sharing of information and knowledge within the system. Third, it is possible to begin to commercialize the knowledge. This stage must involve detailed planning, establishment of a mechanism, a survey and a pilot program before full-scale commercialization begins. These three stages require prior planning and risk management, mainly in order to prevent a situation in which information produced by the defense establishment that can be released, is not. The following section examines possible solutions for the commercialization of knowledge.

Existing Models of Commercialization of Knowledge

Assuming that the defense establishment is interested in the orderly application of the IP generated under its aegis, the following section will review the main models for realizing this goal.

Venture Capital Funds

These are bodies that raise money from investors (limited partners) for risky ventures such as startups. The many companies controlled by the

fund reduce the risk involved when an investor invests in a single company. The sources of IP in ventures capital funds vary; some funds invest in ideas at the very beginning, while others come in at a more advanced stage. The capital is usually foreign: 90 percent of the capital currently raised for the Israeli high-tech sector comes from foreign investors.[17] As a result of the dramatic increase in raising venture capital for the Israeli market at the end of the 1990s, the defense establishment had the idea to use the assets to develop dual-purpose (civilian and security) technologies originating in the technological units of the IDF, and thereby help finance R&D in the security sector.[18] This idea was never implemented and became less attractive after the high-tech bubble burst globally at the start of the new millenium. From time to time, funds and private companies specializing in the commercialization of dual-purpose technologies originating in the defense establishment are founded.

Technological Incubators and Accelerators ("Hothouses")

These are settings designed to turn innovative technological ideas into startups and get them to the point where they can raise funds on their own. The hothouse provides new projects that are still in their early stages, with support such as an infrastructure for R&D, technological and business support, connections to investors and strategic partners, help in putting together suitable teams and administrative services for the company, etc. The technological hothouse program run by the chief scientist of the Ministry of the Economy allocates a certain budget to the projects that have been approved for participation; 85 percent of the funds are provided by the state as a grant to be paid back in the form of royalties on sales, and the entrepreneurs hold 15 percent of the stock of the company to be established thanks to the hothouse without having to invest any of their own money in the venture.[19]

Investment Companies

This is a general term for companies specializing in acquiring subsidiaries and working to upgrade them. The company's profits come from the subsidiary's dividends and from the income derived from the sale of the upgraded companies. Investors in an investment company are the company's shareholders. RDC Ltd.,[20] for example, applies the idea of cooperation between the security and civilian sectors. This company is owned jointly

by Rafael Industries and Discount Investments. It is designed to combine technological IP from Rafael and receive capital and business knowhow from Discount Investments for the sake of establishing subsidiaries. The most successful of RDC's projects is Given Imaging Ltd., which manufactures and markets diagnostic products–pills with tiny cameras inside for the visualization and detection of disorders in the gastrointestinal tract. At the end of 2013, Given Imaging Ltd. was sold to the Covidian Group for $820 million.[21]

Companies for the Commercialization of Knowledge at Universities, Research Institutes and Hospitals

These companies promote commercial applications based on inventions by researchers working in the organization, such as Ramot Ltd. at Tel Aviv University, Hadassit Ltd. at Hadassah Hosptial, Yisum Ltd. at the Hebrew University, and so on.[22] Isorad Ltd. is a government company manufacturing and commercializing developments made at the Soreq Nuclear Research Center. This company, for example, is involved in the development of nuclear catheters and other developments in the field of nuclear medicine.[23]

The 8200 EISP Program

This is a non-profit organization established in 2010 by an NGO formed by Military Intelligence Unit 8200 alumni on behalf of the community. Its objective is to use the knowledge and experience of its members to help young entrepreneurs, not necessarily from Unit 8200, succeed in new ventures. By April 2014, 60 entrepreneurs in three rounds have participated in the program. Among the projects participating in the program were a company in the field of interactive advertising and a company in the field of information security.[24]

The US Army IP Model

The US Army grants licenses to civilian companies to use patents under its registration. The army views this as a way to expand the use of various inventions that came about under its aegis. The license may be for non-exclusive, partially-exclusive or exclusive use, based on the army's considerations for any given invention. In any case, the US administration retains the nation's rights to use the military's inventions for its own needs.

Royalties are determined through negotiations and relate to the size of the potential market, exclusivity, and the need to develop additional technologies. The army's research labs may provide technological assistance for further development.[25] Obviously, when exclusivity is not granted, the particular IP becomes less attractive.

The Intellectual Ventures (IV) Model

Intellectual Ventures is a company based on the principle of knowledge sharing. One of the company's approaches is developing ideas while taking advantage of a network of some 4,000 inventors around the world. Inventors respond to a call for proposals, IV chooses the ideas for commercialization and finances the creation of patents. The inventors are eligible for some of the profits should IV sell its assets.[26]

Principles for Handling the Management and Commercialization of IP in the Defense establishment

Given the situation and the various models presented above and in light of an analysis of the risks and opportunities, we now propose some principles for the management of IP in the purpose of commercialization.

At the opposite ends of the security spectrum are two types of organizations that must be treated very differently:

a. *Security companies.* These commercial companies are supposed to manage their IP as any company doing business these days, including documentation, confidentiality and patent registration, under government guidance and supervision. The MoD and the Ministry of Finance must ensure that government owned companies use up-to-date procedures that protect the state's rights in general and particularly when they sign contracts. The best scenario would be the establishment of a knowledge sharing mechanism that would connect all government owned companies to increase efficiency and maximize the advantage of size. When it comes to non-government companies or providers to government owned companies, it is important to make sure that there is a contractual and follow-up system in place, so that IP developed with defense establishment funds remains under defense establishment ownership and supervision, even if those non-government companies use it on behalf of other customers.

b. *Military units*. In general, it is best that they do not focus on the business side of things but rather on the security purpose of their developments and on transferring the information that could be applied to commercial uses. The responsibility of the commanding officers would be to document the information created in the unit, use the information for the unit's needs, share the information with other units in the defense establishment for its security needs, preserve information security (so far, these are all tasks that serve the military's needs), and only then transfer the information regarding business needs to the body in the MoD authorized to deal with its commercialization. It should be noted that the task of preventing the leakage of information out of the unit based on information security considerations also serves the function of supervising the IP developed in the unit.

Most of the dealings with the commercialization of IP originated in IDF units would therefore occur within the MoD itself, but cooperation with the units is a prerequisite.

A Prerequisite is the Internal Management and Control of the IP

The defense establishment must engage in the registration, protection and regularization of ownership before patent registration. To that end, the defense establishment must undertake activities of a legal and organizational nature: procedures, directives, guidance, explanation, enforcement and supervision. The MoD must take steps to ensure that unreleased information does not leak into the market in an unsupervised way and that the flow of information takes place only via an authorized body. In any case, it is essential to ensure that application of this principle is in tandem with the regularization of the release of IP to the market so at to avoid a bottleneck in the defense establishment.

Taking a Broad View

Handling this complex issue requires the integration of representatives from different fields. It is best to put together a steering committee that would include representatives from the Ministry of Defense, the technological units in the IDF, the military industries, the Ministry of Finance, the Chief Scientist in the Ministry of the Economy, and the Patents Authority in the Ministry of Justice. Subordinate to this committee, there would be two groups charged with the essential components of the process: one

dedicated to gathering information from IDF units, sorting it, and releasing it for commercialization, and one dedicated to preparing the information for its commercialization and its actual commercialization.

Gathering and Sorting of IP and its Release for Commercial Use

This requires a professional body in the Ministry of Defense. It must be intimately familiar with the technologies in the defense establishment and be able to envision their civilian applications. It would be responsible for the active gathering, intake and preservation of information from the technological units. It is important that this body have expertise both in the technological side and in marketing, including an understanding of the needs of the civilian market, on the one hand, and the capabilities of the defense establishment, on the other. To this end the body would have to seek the help of consultants from the business world.

After gathering, sorting, and organizing the information, a committee will authorize the release of technologies from the defense, while undertaking a cost-benefit analysis. The committee would include representatives from the groups involved in the steering committee. The IP released for commercialization would appear in the Ministry of Defense's database.

The Realization of the IP for the Needs of the Civilian Market

Another body, such as a designated government company, would be established to realize the IP designated for the non-government business market. The company would be fully government owned or owned in partnership with the business sector. Initially, full government ownership is preferable given the complexity of founding and running a jointly owned company. In either situation, control would remain in the hands of the MoD and management would be handled by business professionals. The Ministry of Defense's representatives on the steering committee would be members of the company's board of directions, ensuring they were committed to its success. The Chief Scientist of the Ministry of the Economy would be involved in its establishment. It is best that this company be founded only after the professional body in the MoD has gathered 20-30 ideas from the units.

The designated company would handle the following: retrieving information from the database; documenting and researching the applicability of the IP for the business sector; protecting the preparation

of the information for commercialization (e.g., protecting the information with patents); and the commercialization of the information.

Commercialization of the Information for the Civilian Sector

This would occur via the designated company at least in the direct sales routes.

Direct Sales Route

The designated company would sell the rights to the knowledge to commercial companies, both military and civilian, under normal business terms, such as a lump sum payment, royalties,[27] and stocks with an anti-dilution mechanism. Conditions for limited use may be set: a prohibition on transferring the technology to another party, and commitment to use the IP within a set period of time. There may also be priorities in the selling of IP, such as giving preference to establishing and developing companies in Israel or foreign companies that are providers of security products to Israel or contribute directly to the development of Israel's economy, etc.

The Hothouse Route

This route's purpose would be to sell the IP at the stage where it is already applied at the small business level. This route, which is infinitely more complex, could make a significant contribution in other fields as well, such as the development of knowledge and management of manpower (more on this below). The designated company would stay in close contact with existing hothouses and/or establish a startup hothouse of its own. One could also consider the founding of startups whose knowledge base is classified, provided the final products are not restricted or would be channeled into use only within the defense establishment. Some of the projects could be developed in hothouses already active while others could be developed close to the technological units.

This interaction is likely to provide the defense establishment two additional advantages: on the technological side, the units would be able to test the applicability of the ideas to existing needs, and on the side of maintaining technological manpower, the project would represent an alternative to technological personnel who, in any case, want to leave the army without completely cutting themselves off from the system. In other words, in certain cases, the IDF would allow people to leave the units and develop their ideas in the hothouse. Because only a fraction of the projects

can be expected to succeed, as is the norm in the venture capital sector, the defense establishment would be able to reintegrate hothouse personnel. Alternately, personnel from the technological units would be able to work in the hothouse for a certain period of time as part of an extended service program, similar to personnel granted time to study at the university. The risk in this is that the route could also accelerate the rate at which certain personnel leave or overemphasize hothouse-related efforts at the expense of security goals.

Conclusion

The defense establishment has IP that can be developed for commercial use in both the military and civilian sectors. Some IP leaves the system in a disorganized fashion or remains in the system and is never fully realized. Generally, the prevalent situation in the MoD and the findings of other studies point to the need for a comprehensive policy on the management of IP belonging to the government into which the security sector would be integrated.

Proper management of IP in the defense establishment would take full advantage of the opportunities and minimize the risks inherent in the field. In any case, it is important to avoid overly rigid government involvement, which might damage the economy. It is therefore necessary to ensure that there are routes via which it is possible to transmit the information to the market so that the market could make use of it. Given the risks inherent to the process, it is best to implement the process gradually and to begin by undertaking a pilot program.

Notes

1 Avi Eliyahu, "Military Inventions that Make our Lives Better," *PZM*, September 4, 2012, http://www.mako.co.il/pzm-magazine/Article-bb7009e7e378931006.htm.
2 State Comptroller, *Annual Report*, 2013, www.mevaker.gov.il
3 The report notes several MoD directives relating to IP that are apparently ill-suited to the task or insufficiently applied.
4 *Annual Report*, p. 131.
5 Ibid., p. 127.
6 Niva Elkin-Koren and Sharon Bar-Ziv, *The Policy on Managing IP in the Government Sponsored R&D Sector* (Haifa: University of Haifa, April 2014).
7 Eliezer Ben Harosh, Amir Rapaport, and Alex Blechman, "Is This Why I Studied Engineering?" *Ma'arachot* (April 2014).

8 *Annual Report*, p. 138.
9 Nili Cohen, "The Scope of Israeli Weapons' Export Had Decreased in 2013; Sales to African Countries Have Doubled." *Haaretz*, October 7, 2014, http://www.haaretz.co.il/news/politics/.premium-1.2453337.
10 The IDF's radio station website, http://www.idf.il/1133-20098-HE/Dover.aspx.
11 Meir Orbach, "In Cyberwarfare, the IDF Is Target No. 1 for Every Terrorist Organization," *Calcalist*, January 12, 2011, http://www.calcalist.co.il/internet/articles/0,7340,L-3480421,00.html.
12 Yesha Sivan, "The Venture Ecosystem Framework: Messy, Fast, and Global," *Venture Findings* (Tel Aviv: Coller Institute of Venture at Tel Aviv University, 2014), pp. 6-18.
13 *Annual Report*, p. 122.
14 Avriel Bar-Yoseph and David Arbel, "Financing Security R&D with Venture Capital Funds," *Ma'arachot* 385 (2002).
15 Evyatar Matanya, "Security R&D Financed by Venture Capital?" *Maarachot* 388 (2003).
16 Avi Blizovsky and Chaim Eshed, "We Must Link Cyber, Space, Nanotechnology and Robotics," *People and Computers*, March 26, 2014, http://www.pc.co.il/it-news/151094.
17 Asaf Gilad, "Pitango: No Venture Capital Funds Lose Money," *Calcalist*, October 9, 2013, http://www.calcalist.co.il/internet/articles/0,7340,L-3613920,00.html.
18 Bar-Yoseph and Arbel, "Financing Security R&D with Venture Capital Funds."
19 The Technological Hothouse Authority website, http://www.moital.gov.il/NR/exeres/2E873A83-AEF5-4B38-8DCF-2CD9687E6958.htm.
20 Rafael Development Corporation.
21 Bloomberg, "Iron Dome in Your Living Room: Israeli Startups Drinking From the IDF's Well," *TheMarker*, August 13, 2014, http://www.themarker.com/wallstreet/1.2404659.
22 For details on the activities and income of these companies, v. the survey made by the Central Bureau of Statistics, "Knowledge Commercialization Companies in Israel: 2012-2013" (press release of August 26, 2014). The survey noted that Israel rates highly by all measures (after standardization): the number of discoveries to inventions, patent applications, number of licensing agreements, number of startups founded, and income from IP and royalties.
23 2010 report on government companies.
24 Ro'ee Goldberg, "The Hothouse Effect," *Globes*, April 30, 2014, http://www.eisp.org.il.
25 U.S. Army Research Laboratory (ARL), http://www.arl.army.mil/www/default.cfm?page=15.

26 V. the IV website: http://www.intellectualventures.com.

27 There is already a Ministry of Defense directive on collecting royalties that belong to it from exporters that, in the course of developing or manufacturing, make use of ministry property.

And What If We Did Not Deter Hizbollah?

Yagil Henkin

The consensus in Israel is that Hizbollah was deterred as a result of the Second Lebanon War, that because of the damage sustained by the group and its supporters, it refrained from fighting against Israel, and that quiet that has reigned on the northern border was a result of the war. In fact, most of the arguments supposedly proving that Hizbollah was deterred are less clear-cut than they appear. The majority of Hizbollah's actions, both before and after the war, can be explained by other factors—domestic Lebanese and international—over which Israel has a very limited degree of control or influence. It is thus necessary to carefully examine the assumption of deterrence, and in particular, to avoid complacency based on this assumption.

Key words: Israel, Lebanon, Hizbollah, Nasrallah, deterrence, Syria, Iran

Was Hizbollah Deterred?

On August 1, 2006, in the midst of the Second Lebanon War, then-Prime Minister Ehud Olmert stated that

> Those who fired the missiles will not hurry to create friction which will instigate confrontation, since they know the price paid by them, the country in which they reside, the population whose support is the source of their strength, and everything around them.[1]

Since then, Olmert's assertion was reinforced by his political supporters and opponents alike,[2] as well as army officials.[3] Another layer was provided by the "Dahiya Doctrine," which states, in the words of then-Commander of the Northern Command Gabi Eisenkot in 2008, "the possibility of harm

Dr. Yagil Henkin is a military historian and a lecturer in the IDF Command and General Staff College.

to the population is the main restraint on Nasrallah and the reason for the quiet."[4] Because the northern border has been quiet since 2006, Olmert called the Second Lebanon War, seven years after the fact, "the most successful" of Israel's wars.[5]

In fact, there are different interpretations of Hizbollah's behavior that do not rely on the assumption that it was deterred by the war. It can also be argued that the results of the war actually served the organization's purposes and that since then it had refrained from a confrontation for internal or domestic Lebanese reasons, not because it was deterred by Israel. Such an interpretation indicates the possibility that the claim about deterrence is incorrect or that deterrence is not the only factor, although it does not prove the opposite, of course. Nevertheless, it requires that Israel examine its basic assumptions about Hizbollah and its behavior.

A Few Words on Deterrence

There have been many theoretical discussions on the issue of deterrence; as one scholar puts it: "When it comes to deterrence, there are more questions than answers."[6] Deterrence can be defined as a threat (explicit or implicit) to use force intended to avoid the need to use it. Otherwise, the threat can be made in order to create a situation in which it will be clear to the enemy that the benefit of using force will be outweighed by the damage it will suffer as a result. In Israel, the term is also employed for using force in a limited fashion (for example, retaliatory acts) in order to cause the enemy to refrain from using force.

Deterrence is not dichotomous; it is a broad spectrum of possibilities. One's actions may deter the enemy from acting in a certain way, but not another. For example, Israel's crushing victory in the Six Day War (1967) did not cause Egypt to refrain from launching the War of Attrition, and within a mere three weeks, firing was resumed along the Suez Canal. However, the victory did deter Egypt from attempting to engage in an all-out war. Even in the Yom Kippur War (1973), Egypt's objectives were relatively limited.[7] In other words, the correct question is not "*did* Israel deter Egypt?" but "*from what* did Israel deter Egypt?"

Similarly, it is reasonable to assume that the quiet on the Golan Heights since 1975 indicates that Syria was deterred from launching an all-out war, even if it was deterred from targeting Israel through Lebanese elements. Another example is the behavior of the United States and the Soviet Union

during the Cold War: Each deterred the other from launching an all-out war, but this did not prevent them from attempting to harm each other in indirect ways, through wars by proxy such as in Vietnam and Afghanistan.

In Israel, Hizbollah leader Hassan Nasrallah's avoidance of public appearances since the Second Lebanon War is seen as proof of deterrence. Dan Haloutz, Chief of Staff during the war, stated in 2010 that killing senior terrorists provides "another layer of deterrence. There is a reason that Nasrallah is sitting in his bunker."[8] In 2011, in response to threats from Nasrallah, Prime Minister Benjamin Netanyahu commented that "the man hiding in the bunker should stay in the bunker."[9] Yet Nasrallah's personal fear of assassination does not mean that Hizbollah as an organization has been deterred from acting against Israel. To give a different example, concern over the personal fate of Prime Ministers since the assassination of Yitzhak Rabin, reflected in a tremendous amount of security, has not prevented any of them from expressing willingness to make even more far-reaching political concessions than those which prompted Rabin's assassination.

Deterrence always depends on context and on cost-benefit considerations. It will cease working the moment the enemy thinks that the benefit of an attack exceeds the risk (or merely makes an error in calculation). For example, a lock that deters a burglar in a student apartment will not deter a break-in at the estate of a multimillionaire. When the benefit outweighs the risk, deterrence is weaker and requires more sophisticated means of protection.[10]

Successful deterrence is not necessarily a threat to exact the highest price. Thus, for example, it is a known fact that soldiers are more afraid of blindness or the loss of sexual potency than death, and therefore a German S-mine, which exploded at waist level, was a potent deterrent for even the bravest of soldiers.

Many theories of deterrence apply only to countries, and their relevance to groups such as Hizbollah, a non-state actor (even if it is integrated into one).[11] For example, an invasion is almost always a threat for states, but from the perspective of a non-state organization, an invasion could actually be an opportunity to draw the enemy into a conflict on favorable terms. However, since almost all organizations and movements have assets as well as a vested interest in self-preservation, the difference between states and non-state actors on the issue of deterrence is largely a practical one. The difficulty in finding *what* deters a non-state adversary does not mean

that *nothing* will deter it. Nevertheless, it is important not to assume that measures considered effective in deterring states will work against a non-state enemy.

Who Will Deter Whom?

At the beginning of the Second Lebanon War, Prime Minister Ehud Olmert stated that "Israel will not agree to live in the shadow of the threat of missiles or rockets against its residents ... Israel will not be held hostage."[12] However, the threat of missiles has only increased since the war. In June 2007, after a volley of rockets was fired at Israel, associates of Olmert declared that the responsible party "is interested in dragging Israel into a response."[13] Following a rocket salvo fired at Kiryat Shmona in 2013, a senior officer in the Northern Command noted that the rockets were intended to draw Israel into a response against Hizbollah.[14]

Statements made by Hizbollah after the Second Lebanon War are often perceived as proof of deterrence, but in fact, the organization was making similar statements even before the war. After rockets were fired at Israel in 2007, Lebanon's Minister of Labor, who was Hizbollah's representative in the Lebanese government, declared that "we have no connection to this ... we refuse to accept the attempt by the enemy to take advantage of the attacks to turn the aggression against Lebanon."[15] Four years earlier, in June 2003, Hizbollah made a similar statement after rockets were fired at an Israeli ship: "we are opposed to this action, which is inexcusable and was not planned in advance."[16]

Israel did not believe that Hizbollah was responsible for either instance of rocket fire, but only in 2007 did it interpret the remark as an indication of deterrence. It should be noted that even in the most serious terrorist attack on the northern border before the war, near Kibbutz Metzuba in 2002, Hizbollah used Palestinians in order to conceal its involvement and avoided taking responsibility.[17]

In addition, perception of threats as indicative of deterrence goes both ways. If Nasrallah's threats and Hizbollah's statements reflect weakness and are a consequence of Israeli deterrence, as many Israelis tend to assume, then Israel's threats against the organization may indicate that Israel is weak and has been deterred by Hizbollah as well.[18]

One Sentence, If at All

The assumption that Hizbollah was deterred in the Second Lebanon War relies largely on one quotation from Secretary General Hassan Nasrallah, in an interview in August 2006, immediately after the end of the war. In the interview, Nasrallah claimed that "no one expected, not even a one percent chance" that Hizbollah's abduction of Israeli soldiers would lead to war. "If I had known that the kidnapping would lead to such a result, we would never have carried it out."[19]

It is very problematic to base a theory of deterrence on this one comment by Nasrallah. Hizbollah's Secretary General is an expert propagandist who does not hesitate to lie when necessary.[20] Furthermore, this sentence is only a small part of a long interview given to a Christian television station, intended to reassure the target audience, many of whom are traditionally among Hizbollah's opponents. In the same interview, Nasrallah claimed that "anyone who says that the two abductees are the reason for the war is mistaken ... we surprised Israel with the timing ... Israel would have declared war at the end of September or beginning of October with or without a pretext." In other words, Nasrallah claims that Hizbollah would not have carried out the abduction if it had believed that it would lead to war, though it would have broken out in any case, and that in retrospect, it was good that the kidnapping was carried out because it forced Israel to attack before it was ready.

Nasrallah's logic is reminiscent of the story of the man who, when asked to return a pot he had borrowed from his neighbor, replied: "firstly, I already returned it to you in one piece. Secondly, when I borrowed it, it was broken. And thirdly, I never borrowed a pot from you."

Nasrallah had no qualms about telling bald-faced lies in that interview, including claims that Hizbollah had never used weapons against Lebanese citizens and that it had never taken Lebanese hostages. Nor was he averse to making promises he had no intention of keeping, such as saying that the Lebanese army could disarm anyone who was armed in southern Lebanon. Therefore, it is by no means certain that the only sentence that can be interpreted as admission of error, which Nasrallah apparently iterated only once, actually represents his opinion. On the other hand, one month before that interview, Nasrallah made the claim that Israel had planned the war in advance and that the abduction had only helped Lebanon, and he also repeated this claim in the following years.[21]

During the Second Lebanon War, Nasrallah explained that just as—in his view—Hizbollah had defeated Israel during Operation Grapes of Wrath in 1996, thereby preventing it from achieving its objectives, the same thing would happen this time as well: "when the resistance survives ... when Lebanon faces the cruelest military force [or the military superpower] with determination and does not agree to humiliating terms ... when we are not defeated militarily, that is victory."[22] We should consider the possibility that Nasrallah *really* believes this claim, which he repeated a number of times after the war.[23]

Between Hamas and Hizbollah

Hizbollah is not just Nasrallah, and we can assume that the organization is not terrified of Israel, as Israel would have wished. Even if Hizbollah was deterred in the Second Lebanon War, it is likely that the events in the Gaza Strip in recent years are eroding this deterrence. After Operations Cast Lead and Pillar of Defense; following the "trickle" of rockets fired from Gaza at Israeli communities and the limited IDF response to the rocket fire from Lebanon (for which Hizbollah did not claim responsibility); and even after the extensive but limited destruction in Operation Protective Edge, it is difficult to believe that Hizbollah still thinks that Israel would respond uncontrollably to any action it took when it has not done so in Gaza. Furthermore, in October 2012, a senior IDF officer expressed the opinion that a Hizbollah attack abroad would be a casus belli, yet the Hizbollah attack on Israeli tourists in Burgas, Bulgaria a few months prior to that statement did not elicit such a response.[24] Hence, Hizbollah can make an assessment, at least for now, that sporadic firing of rockets at Israel will not lead to a third Lebanon war, and that even if this war were to take place, it would be subject to all the restrictions on the use of force that were in effect in the Gaza Strip.

It is commonly believed that the Second Lebanon War harmed public support for Hizbollah, and in particular, the support of the Shiite community in Lebanon, which is the organization's power base. These assumptions are strengthened by Shiite leaders' statements.[25] For example, Subhi Tufayli, the first Secretary General of Hizbollah, stated in November 2006 that "Israel had no preliminary plan for a war in Lebanon... Iran had an interest in causing turmoil." He even hinted that Nasrallah was interested in a civil war in Lebanon.[26] These were not necessarily new ideas. As early as 2003,

Tufayli stated that "the Iranian leadership was, and still is, responsible for all of Hizbollah's decisions" and claimed that the organization was Israel's "border patrol."[27]

However, the assumption that the damage caused in the Second Lebanon War pushed the Shiite community to "understand" its results and pressure Hizbollah is problematic. Immediately after the war, some 70 percent of the Shiites in Lebanon believed that Hizbollah was the victor (compared to less than half of the Druze or Christians and about one-third of the Sunnis).[28] In public opinion polls in Lebanon during the four years following the war, Hizbollah won the support of an overwhelming majority of Shiites, generally more than 85 percent, and sometimes as high as 94 percent.[29] Furthermore, in the 2009 Lebanese elections, although the bloc to which Hizbollah belonged was weakened, Hizbollah's candidates won the election in every district in which a Hizbollah candidate participated, including in southern Lebanon, which had suffered grave damage during the war.[30]

If it was not deterrence that brought quiet to the Israeli-Lebanese border, how can we explain the fact that Hizbollah refrains from firing rockets? An answer can be found by comparing the organization's method of operation between the IDF withdrawal from Lebanon in 2000 and the Second Lebanon War, and between the end of the war and the present.

2000-2006: The "Resistance" Seeks Direction

Hizbollah, in Nasrallah's words, is an organization with many aspects: "political, jihadi, administrative, and social."[31] His deputy, Sheikh Naim Qassem, declared that the group's "primary objective is the struggle [jihad] against the Zionist enemy" but that "the clever and sagacious political jihad can and should be the buttress and pillar of this *jihadi* movement."[32]

Though it is a Shiite organization, Hizbollah is also influenced by Lebanon's domestic politics; for years Nasrallah was careful to emphasize that he is the defender of all Lebanese citizens, not seeking to impose his religious beliefs. In 1992, the organization even decided to participate in Lebanese politics (with the approval of Iran's spiritual leader, Ayatollah Khamenei), and since then, it has collaborated with Christian leaders and made efforts to win the hearts of Christian Lebanese citizens.[33] This does not indicate a change in Hizbollah's ideology, but rather, pragmatism in its actions and its path, and possibly also in its timetable and priorities.

Theoretically, Hizbollah's military strength contravenes the Taif Agreement of 1989, which ended Lebanon's civil war and provided for disarming all militias in the country. When the IDF was present in the security zone, Hizbollah (with the support of the Syrians, who at that time maintained de facto control of Lebanon, and the Lebanese government itself) justified the existence of its military wing by citing the need to oppose the Israeli occupation. An Israeli withdrawal, therefore, was supposed to lead to the disarming of Hizbollah. Sheikh Fadlallah, Hizbollah's spiritual leader, stated in 1995 that there would apparently be no place in Lebanon for the Islamic resistance once the land was liberated from the Israeli occupation.[34] In 1997, Nasrallah declared that "when the Zionist enemy withdraws from the occupied territories, we will not be responsible for security. We have a state and it will use its security forces in these territories."[35]

These commitments were tested after the Israeli withdrawal from Lebanon in May 2000, when many Lebanese (including then-Prime Minister Rafiq al-Hariri) believed that Lebanon must direct its resources to internal reconstruction and that Hizbollah's military role had ended.[36] In April 2001, the editor of Hariri's newspaper claimed that the organization's actions were not helpful to Lebanon, and another Lebanese commentator called on Syria and Hizbollah not to fight their battle with Israel from Lebanese soil.[37]

Militating against this position was the clear fact that Hizbollah was the only Arab force to succeed in causing Israel to withdraw without an agreement and without receiving anything in return. The prestige this conferred on Hizbollah made it unlikely that the organization would be disarmed, even in the eyes of old adversaries such as Nabih Beri, head of the Shiite organization Amal.[38] However, an ongoing state of calm on the northern border could have convinced many Lebanese at that time that in fact, Hizbollah's role had ended. Contrary to the hopes of officials in Israel,[39] Hizbollah found other pretexts for continuing the fighting. It announced that it would continue until all Lebanese lands (that is, the Shab'a Farms) and Lebanese prisoners held by Israel are liberated.[40] In July 2001, Nasrallah even declared that "our struggle with the Zionist enemy is not a border conflict between two countries, but a confrontation with an entity whose aim is [the destruction of] our survival and future." While in the short term, there was little chance of achieving the "liberation of Palestine," this "requires neither nuclear weapons nor a strategic balance ... although there may be something of a dream here, there is also something

of reality."[41] This reality requires maintaining Hizbollah's power and continuing clashes with Israel as perpetual justification for preserving its military force. The past few years have emphasized this need, since the status of the Shiites in Lebanon, who were traditionally far from the centers of power and suffered from discrimination, had been largely based on Hizbollah's weapons arsenal.[42]

Despite Syrian support[43] and considerable Lebanese support for Hizbollah on the issue of the Shab'a Farms, the expulsion of the Israeli occupying forces from an uninhabited area of twenty-five square kilometers was a rather weak justification for the existence of a private army. In fact, the Shab'a Farms issue is rather marginal for Hizbollah. Until 2002, the organization attacked IDF outposts on Har Dov almost every month.[44] However, after that, it slowed down the pace of attacks, and when it came under pressure on the issue within Lebanon, a conflict on that point was not enough to justify maintaining its military power.

In September 2004, the UN Security Council passed resolution 1559, which included a call to disarm all the militias in Lebanon. This resolution created pressure on both Syria (with growing calls for its withdrawal from Lebanon) and Hizbollah, which ultimately led to the assassination of Prime Minister Hariri shortly after his resignation from office. The murder proved to be a double-edged sword. It caused internal and external pressure that led to the withdrawal of Syrian troops from Lebanon, in spite of demonstrations by Hizbollah supporters who supported the presence of Syrian forces and opposed disarming the organization. Many people in Lebanon, from Druze community leader Walid Jumblatt to Sunni Muslims, feared that Hizbollah was serving the interests of Iran and Syria rather than Lebanon, and that the weapons in its possession conferred dangerous power on the Shiite community and could lead to a new arms race. It was actually a pro-Syrian Lebanese commentator whose definition was quite precise: "Hizbollah's rifle is ultimately Shiite."[45] On the other hand, Hizbollah supporters claimed that the desire to disarm the organization was "treason" that served "only the interests of Israel." Elias Saba, a veteran Lebanese politician, claimed that "the role of the resistance ... is necessary [even] after the liberation of the land and the prisoners [... since] how can we ensure that Israel will not reconquer the land?" Nasrallah attempted to calm the heated atmosphere by stating that "no one will succeed in bringing this weapon into the domestic arena."[46]

In July 2005, Hizbollah joined the Lebanese government for the first time. One of its representatives, Minister of Water and Energy Muhammad Fneish, stated that the Lebanese "have no reason to fear" Hizbollah's weapons and that "if joining the government and the Parliament is a national duty, so is defending the country."[47] The message was clear: Hizbollah would use its weapons only against Israel, but it would not consent to the demand to disarm. And in fact, in January 2006, then-Lebanese Prime Minister Fuad Seniora promised that he would treat Hizbollah as a "national liberation group" and not as a "militia," which removed the burden of resolution 1559 from Hizbollah.[48]

It is therefore not surprising that Hizbollah escalated its operations on the northern border in 2005 and 2006. Abducting Israelis in order to bring about the release of Lebanese prisoners held by Israel was within the Lebanese consensus. It showed that Hizbollah was acting for all of Lebanon; it strengthened its position, which had been harmed by internal Lebanese disputes; reduced the fear that it would turn its weapons inward; and decreased the pressure to disarm it.

Despite all this, many Israelis saw the situation in Lebanon as unprecedentedly quiet, or alternatively, as a balance of terror intended to prevent an Israeli attack. "Never has there been quiet on the northern border such as the quiet that has existed since IDF soldiers have been guarding on the eastern side of the border," wrote Yigal Tzhor of the Labor Party and the Berl Katzenelson Foundation, on the fifth anniversary of the IDF withdrawal from the security zone.[49] One year earlier, journalist and researcher Daniel Sobelman wrote:

> From the beginning of 2003, stability was maintained on the Israeli-Lebanese border despite several upheavals [...] such as the war in Iraq, the Israel Air Force (IAF) attack in Syria, military operations inside Lebanon that were attributed to Israeli intelligence, destruction of Hizbollah anti-aircraft batteries by Israel, and the killing of Hamas leader Ahmed Yassin and his successor, Abd al-Aziz Rantisi.[50]

Only one week before the outbreak of the Second Lebanon War, *Haaretz* correspondent Aluf Benn wrote that "a Nasrallah was needed in the Gaza Strip." While he hates Israel, unlike the leaders of Hamas, who kidnapped Gilad Shalit and launch rockets, Nasrallah "has authority and responsibility, and therefore, his behavior is rational and reasonably predictable. In the

present conditions, this is the best that there is. Hizbollah is preserving quiet in the Galilee more than the pro-Israel South Lebanese Army did."[51]

From 2006 Onward: Domestic Politics or Deterrence?

One could argue that Hizbollah (almost) ceased to operate against Israel after the Second Lebanon War because it was no longer necessary and because it was dealing with other things which Israel had a very limited ability to influence. To many in Lebanon and even in the West,[52] the fact that the war took place is proof that it was deliberate; in other words, the fact that Israel invaded Lebanon proved that it had planned in advance to do so. This is not a new idea: as early as 1972, Fadlallah stated that Israel was interested in invading Lebanon irrespective of the actions of the Palestinian organizations. To many people, the fact that Israel remained in parts of Lebanon after Operation Peace for Galilee (1982) was confirmation of his claim.[53] In October 2006, 84 percent of the Lebanese believed that the war had been planned in advance by the United States and Israel in order to reshape the region, and 78 percent thought that it would have broken out regardless of Hizbollah's actions.[54] The similarity between these statistics and the claims by Nasrallah reinforce the assumption that he was not going to voice his regret for the abduction of Israeli soldiers but rather he intended to claim that it was only an excuse for Israel to undertake a planned invasion of Lebanon.[55] After the war, Hizbollah needed to "maintain" an active conflict with Israel less than it had in the past. The war and the destruction left in its wake clearly demonstrated the danger from Israel and the need for Hizbollah to grow stronger in order to prevent a similar war in the future. In August 2013, Nasrallah even declared that because of Hizbollah's great strength, "the era of Israeli tourism on the Lebanese border has ended forever."[56]

Since the war, the denominational issue has continued to determine the attitudes of the various Lebanese groups to Hizbollah: the Shiites are enthusiastic supporters, the Sunnis have reservations, the Druze and Christians are suspicious and fearful.[57] However, a poll from October 2006 showed that only about one-fourth of the Lebanese wished to disarm Hizbollah, about one-half wished to incorporate it into the Lebanese army, and more than one-third (among them the vast majority of the Shiites) supported maintaining Hizbollah as an armed independent entity.[58] The non-Shiites apparently perceived Hizbollah as Lebanon's most effective

protector, but they feared that it would use its armed power internally. Even at a low point in its popularity, in February 2007, only 20 percent supported forcibly disarming the organization, and 48.6 percent (among them, surprisingly, most of the Sunnis and Orthodox Christians) were in favor of allowing it to keep its arms, at least until the liberation of the Shebaa Farms or an Israeli-Lebanese agreement.[59]

It is possible that the protracted negotiations for the return of the bodies of abducted IDF soldiers Eldad Regev and Ehud Goldwasser, which ended in mid-2008, also contributed to Hizbollah's lack of interest in heating up the sector again: the achievement of returning the Lebanese prisoners through diplomatic means was sufficient to justify avoidance of any action that could have harmed the deal.

At the same time, Hizbollah apparently believed that the war provided an opportunity to increase its political influence in Lebanon, and given the disparities in support for the group between the Shiites and other communities it may have estimated that the time was right for a more "Shiite" and less "Lebanese" line of politics. Hizbollah officials made increasingly blunt statements on this subject, to the point of explicitly supporting a Shiite country. Furthermore, in November 2006, all Shiite representatives resigned from the government, which caused paralysis (for constitutional reasons) following the proposal to establish an international tribunal to try Hariri's murderers and Hizbollah's desire to bring additional representatives into the government. A few days later, Shiite and pro-Syrian elements began a series of mass anti-government protests, and Nasrallah even declared (and in fact threatened) that Hizbollah's supporters should not fear "a new civil war."[60] The Lebanese police estimated that at the height of the demonstrations, Hizbollah brought some 800,000 people to the streets, about one-fifth of the country's population.[61] The group also worked to prevent the establishment of an anti-Syrian government, which could have acted to disarm it and perhaps even reached tacit agreements with Israel.[62] In addition, members of the March 14 Alliance, who opposed the Syrians and Hizbollah, continued to die under mysterious circumstances, including Minister of Industry Pierre Gemayal, whose funeral turned into a large-scale anti-Syrian (and implicitly, anti-Hizbollah) demonstration.

At the same time, Hizbollah continued its military buildup, even daring to demand that the Lebanese army return a truck of ammunition it had confiscated. (There was great support for the demand among the Shiites,

while the other ethnic groups, especially the Druze, took the opposite position.)[63] In November 2007, Hizbollah claimed it had held a large military exercise in southern Lebanon, thus making clear that it was in fact ignoring Security Council resolution 1701 and that there was no power in the country that could force it to disarm.[64] It continued to position itself as the defender of Lebanon against Israel, and as usual, employed various pretexts to maintain its military power.[65]

At the same time, Hizbollah continued to cross Lebanese political boundaries: In January 2008, seven people were killed in exchanges of fire between Hizbollah operatives and the Lebanese police. In May of that year, in a protest over the government's disabling of Hizbollah's communications network and the dismissal of the official in charge of security at the Beirut airport, who was close to Hizbollah, fighting broke out throughout Lebanon and the organization used artillery and rockets while the army stood by. The Doha Agreement, signed on May 21, 2008, stated that the opposition would receive eleven (out of thirty) minister positions in the Lebanese government, therefore awarding Hizbollah veto power. Its communications network continued to operate, and even the official in charge of security at the Beirut airport got his position back. Several days later, Chief of Staff General Michel Suleiman was appointed president of Lebanon, and almost immediately, he praised the "resistance" and took a pro-Syrian stance.[66]

"During the winter of 2007 and the spring of 2008," writes the American journalist and researcher Thanassis Cambanis, "it wasn't Israel but moderate Arabs who posed a serious existential threat to Hezbollah."[67] In other words, it may be that Hizbollah refrained from firing at Israel not because it had been deterred from doing so but because at that point, it had other more pressing matters to attend to. Israel's Prime Minister at the time, Ehud Olmert, claimed in July 2008 that since the Second Lebanon War, and because of its results, "Hizbollah is clearly reluctant to confront us militarily in the area of southern Lebanon. It is busy trying to rebuild its political position."[68] Given the events of spring 2008, it may be that it was not "clearly reluctant" but that it took advantage of its success, not to rebuild its position but to strengthen it.

Nasrallah's assurances that Hizbollah's weapons are "Lebanese" and that they would be directed only against Israel turned out to be empty. While the organization's position among the Shiites grew stronger, its political opponents and the other communities in Lebanon began to fear

and oppose it even more than they had prior to 2008.[69] If Hizbollah intended to strive toward an Islamic state in Lebanon,[70] the attempt was made too soon. Evidence of this came a year later, in the 2009 elections, when the strength of the Hizbollah camp was reduced, even if the organization itself won all the seats for which it ran candidates.[71] In a Hizbollah manifesto from November 2009, the call to establish an Islamic state, which was central to its previous platform in 1985, was omitted.[72] However, the group remained a member of the government, received veto power, and received the important position of Minister of Communications. The new Lebanese cabinet once again confirmed that Hizbollah was a "resistance" movement and not a militia that had to be disarmed.[73] The organization continued to enjoy tremendous support from the Shiites, and even among the general public, it had a small majority of supporters.[74] In southern Lebanon, control by the opposition in general and Hizbollah in particular remained absolute.[75] Some believed that Hizbollah was not interested in too large a victory in the elections because it was convenient to be a member of the government that could veto its actions, yet not be perceived as the responsible party.[76]

What has been written until this point is sufficient to show that Hizbollah's actions were not influenced only or perhaps even primarily by fear of Israel. Its involvement in recent years in the civil war in Syria and the fighting against Sunni organizations demonstrates this well. There are those who argue that Hizbollah is nothing but a servant of Syria or Iran, that the question whether to act against Israel would be settled primarily by them and would not be dependent on deterrence in Lebanon. [77] According to Shimon Shapira, "one of the main reasons for the quiet on the northern border is that at this time, Iran has no interest in heating up the sector. Hizbollah's missile force was intended to create deterrence against Israel in order to prevent an Israeli attack on Iran."[78] In another context, Subhi Tufayli claimed that the only reason for Hizbollah's intervention in Syria was that Iran forced it to intervene.[79]

Buildup and Deterrence

After the Second Lebanon War, Hizbollah began to rebuild its strength and repair the damage sustained. Within two years, the organization had tripled its weapons stockpile to some 40,000 missiles and rockets, some of them heavier and with a longer range than those it previously possessed,[80] and turned villages into fortified compounds. In July 2010, Israel mapped

the ammunition storage facilities, fortifications, and headquarters built by Hizbollah in the town of al-Hiyam in southern Lebanon.[81] In September of that year, an ammunition storage facility belonging to the organization in al-Shahabiya in southern Lebanon exploded. The IDF spokesperson reported that documentation of the explosion was "a fact that embarrassed Hizbollah,"[82] but it turned out that the embarrassment was rather limited (if at all). When an explosion took place in Tair Harfa about two years later, Hizbollah members openly blocked off the area and, according to reports, even prevented UNIFIL personnel from approaching it.[83] Israel, for its part, did not openly attack Hizbollah for its renewed buildup, but rather approached the United Nations.[84]

Hizbollah's reluctance to confront Israel during its rebuilding effort could be interpreted not as fear of Israel or as a result of deterrence but as a tactical measure intended not to disturb the buildup. While Hizbollah refrained from direct and open action against Israel until 2013, it is believed that the group was responsible for several incidents on the Israeli-Lebanese border during those years. In January 2009, during Operation Cast Lead, four Katyushas were shot at the Galilee (two of them fell in Israeli territory). Israel held Hizbollah responsible, but the organization denied involvement.[85] In July of that year, a group of unarmed civilians infiltrated an abandoned IDF outpost on Mount Dov and hung the flags of Hizbollah and Lebanon. The IDF responded with threats but decided not to take action because the civilians were unarmed.[86] In October 2012, Hizbollah sent a drone over Israeli territory, which was shot down in the area of the Yatir Forest,[87] and in April of the following year, Israel shot down a drone believed to have been sent by Hizbollah, although the organization denied responsibility.[88] In contrast, when four IDF soldiers were wounded near the border with Lebanon in August 2013, Hizbollah (for the first time since the Second Lebanon War) claimed responsibility and said that it had ambushed IDF soldiers operating in Lebanese territory.[89] In April 2014, Nasrallah claimed responsibility for an explosive device used against IDF soldiers on Mount Dov.[90]

After the Second Lebanon War, Hizbollah increasingly resumed its international terrorist operations. In this context, some claim the group has been operating in Iraq since 2006[91] and that it planned large-scale terrorist attacks, particularly against Israeli targets in Cyprus, Egypt, Thailand, and Europe, with a nearly total lack of success, until 2012, when it carried out

an attack in Burgas, Bulgaria that killed six people, including five Israelis.[92] This is reminiscent of the actions of the Palestine Liberation Organization (PLO) after the ceasefire in 1981, when it believed it could act against Israel abroad without a response in Lebanon.

Of course, one could argue that Hizbollah's attempts to operate against Israel from locations other than the Lebanese border were the result of successful deterrence. However, it is possible that they stemmed from considerations of convenience and not deterrence. Even if it they were, in fact, a result of Israeli deterrence, they show its limitations. Thus, for example, in the 1990s, Hizbollah operated almost exclusively in the security zone in southern Lebanon, and it generally did not attempt to infiltrate Israel (in contrast to the Palestinian organizations). This was not a reflection of Israeli deterrence but of an understanding that targeting Israel in the security zone was no less effective than infiltrating into Israel, and much more convenient. An army's choice to attack at one point does not indicate that it is deterred from attacking in other places, but that it is seeking a more convenient point, which holds true for a terrorist organization as well.

Nasrallah himself has recently raised his profile. Although for the first five years after the Second Lebanon War, he appeared in public only twice (in January 2008 and December 2011), in the past two years, he has appeared in public at least four times (September 2012, August 2013, November 2013, and July 2014). His threats have not become more moderate. In 2011, he announced an operational plan to conquer the Galilee. In August 2012, Hizbollah reported a large exercise[93] and as befits a modern terrorist organization, even published an interactive presentation in broken English, ostensibly showing the next war, including occupation of northern Israel up to the Haifa-Afula-Bet She'an line.[94] Nasrallah also threatened to "turn the lives of millions of Israelis into hell" if Israel attacked Iran;[95] declared that the destruction of Israel is a Lebanese, Arab, and Muslim interest, and not just a Palestinian one;[96] and threatened to assassinate Israeli officials in revenge for the assassination of Hizbollah official Imad Mughniyeh.[97] In addition, he promised that "Israel would be punished" for killing another Hizbollah official, Hassan al-Lakis, in December 2013, even though a Sunni organization took responsibility (and some claimed that Hizbollah itself was responsible).[98]

The conventional interpretation in Israel tends to be that Hizbollah's relative inaction against Israel is a result of deterrence. If this is in fact the

case, there are several questions: Why did Hizbollah send drones over Israeli territory? Why did Nasrallah, for the first time in several years, claim responsibility for attacking IDF soldiers, precisely when his organization had become deeply entangled in the civil war in Syria? And why is he appearing in public more frequently than in the past and making equally impassioned speeches?

In late 2013, Hizbollah claimed that its "presence in Syria is for defending Lebanon, Syria, Palestine, and the resistance against all threats facing them."[99] Following Operation Protective Edge (during which it made its regular threats), the organization explained that the call to intervene during the operation in support of Hamas was not serious and not official.[100] This shows that the absence of Hizbollah operations against Israel is not a result of Israeli deterrence but of different priorities, and that the most important thing for the group today is to fight in Syria. It appears that at this point, the extremist Sunni groups operating in Syria are more threatening to Hizbollah than Israel.[101] A car bomb that exploded recently in one of Hizbollah's strongholds indicates that this hypothesis has a basis.[102] We should not conclude from the current situation that Hizbollah will not choose someday to defend Lebanon and the Palestinian cause more directly.

The Second Lebanon War serves as a vivid reminder that Lebanon needs Hizbollah in order to protect itself against Israel. The organization will maintain its hatred of Israel in the foreseeable future, but its priorities have changed since 2006, and not only because of the damage caused. If before the war, Hizbollah took advantage of clashes with Israel in order to gain support, today, it uses a supposed threat in order to achieve the same objective, but it does not see the need for extensive operations against Israel.[103] Furthermore, after the war, Hizbollah became much more involved and influential in the Lebanese government than it had been previously.

We should take into account that Hizbollah's increasing willingness to openly carry out (small) operations against Israel could mark its return to the concept that guided it before the Second Lebanon War. In any case, this appears to be on a slightly smaller and more careful scale—friction with Israel for the purpose of helping Hizbollah's standing within Lebanon. This is a gamble, and Hizbollah may be wrong yet again.

What about Mughniyeh?

The weak link in the assumption that Hizbollah has not been deterred is the fact that it has not responded directly to the assassination of Imad Mughniyeh or Hassan al-Lakis and did not come directly to the aid of Hamas in Operations Cast Lead or Protective Edge. However, Hizbollah actually did attempt to strike at Israeli targets in retaliation for Mughniyeh's killing. If the organization was planning large-scale reprisals, it is no wonder that it did not bother to fire rockets, and after those attempts failed, it is not surprising that it did not launch them: what type of organization shoots Katyushas in 2009 in response to a killing that took place in 2008?

The assumption of non-deterrence is undermined by Hizbollah's failure to launch missiles during Cast Lead and Protective Edge (in contrast to Operation Defensive Shield, when it fired hundreds of rockets and mortar shells and carried out a terrorist attack). If there is one thing that strengthens the theory of deterrence, this is it.[104] But in fact, even Hizbollah's behavior during Cast Lead and Protective Edge does not constitute definitive proof of deterrence, since its involvement in building up its strength and fighting in Syria, along with its meddling in Lebanese politics, may have made the timing of the two operations inconvenient: on the one hand, it had not yet completed preparations for another conflict, and on the other, it needed more time to correct the impression left by its use of weapons in the internal Lebanese arena.[105] If Hizbollah's buildup was also intended to deter Israel from acting against Iran, then perhaps from Iran's point of view, Cast Lead did not justify use of the organization. During Protective Edge, Hizbollah was entangled in Syria, more than at any time in the past.

Summary and Conclusions

This author hopes that Israel did, in fact, deter Hizbollah. However, the organization's behavior can be explained even without resorting to an assumption that it was deterred. What protects the Israeli-Lebanese border today may be not only the IDF's strength, but also Hizbollah's problems, its additional goals, and its other affairs. The organization will not reconcile itself to or accept Israel's existence, and if it is deprived of the existing reasons to fight Israel, it will likely find or invent others. However, it should be understood that Israel is not always Hizbollah's most pressing issue.

The question whether Hizbollah was deterred by Israel in the Second Lebanon War is not only theoretical. Israeli operational plans (against

Hizbollah or against other adversaries) that are based on the assumption that the devastation Lebanon suffered during that war is what led to the quiet and deterred Hizbollah could fail if it becomes clear that this was not the case.[106] At the same time, if Hizbollah's failure to act against Israel is influenced primarily by factors over which Israel has no control, then a belligerent action by the group may be closer than is commonly thought. Suffice it to mention that in early 1967, the Israeli military intelligence assessment was that war was not to be expected since the Egyptian army was entangled in Yemen, and that several months later, because of a chain of events that were largely not under Israel's control, the Six Day War broke out.

Finally, excessive faith in the power of deterrence could lead to complacency. Three months before the Yom Kippur War, Defense Minister Moshe Dayan believed that a major war was not to be expected in the coming decade. On the face of it, he had a basis for this assessment: the Egyptians appeared to have been deterred. They had failed to achieve their goals in the War of Attrition, and despite the Egyptian rearmament, it was never quieter on the Suez Canal—until the afternoon of October 6, 1973.

Notes

1 Prime Minister's Speech at the Commencement Ceremony of the 33rd National Security College Course in Glilot, August 1, 2006.

2 See, for example, Tzipi Livni, "The Real Revelation of the War," July 12, 2011, http://www.tzipilivni.co.il/?p=5105; and Dana Weiss, "Ya'alon on Operation in Gaza: There Were Political Considerations," Channel 2 News, November 24, 2012, http://www.mako.co.il/news-military/politics/Article-7bbe028bfe23b31004.htm.

3 See, for example, "OC Northern Command: Nasrallah is Placing All His Cards on Assad," *Walla*, October 12, 2013, http://home.walla.co.il/?w=/2689/2682933.

4 Alex Fishman and Ariella Ringel-Hoffman, "I Have Tremendous Power, I Will Make No Excuses," *Yediot Ahronot*, October 3, 2008 ; see also "The Dahiyah Doctrine," Reut Institute, June 12, 2009, http://reut-institute.org/Publication.aspx?PublicationId=3672 .

5 Adi Hashmonai, "Olmert: Second Lebanon War—The Most Successful of Wars," *Maariv- NRG Online*, July 17, 2013, http://www.nrg.co.il/online/1/ART2/491/157.html .

6 Adam Lowther, "Introduction: The Evolution of Deterrence," in *Thinking about Deterrence–Enduring Questions in a Time of Rising Powers, Rogue Regimes*

and Terrorism, ed. A. Lowther (Maxwell Air Force Base: Air University Press, 2011), p. 5.

7 Danny Asher, "Breaking the Concept," *Ma'arachot* (2003).

8 Yehoshua Breiner, "Haloutz: Nasrallah in Bunker Thanks to Assassinations," *Walla*, February 23, 2010, http://news.walla.co.il/?w=/2689/1646554.

9 Barak Ravid, "Prime Minister Benjamin Netanyahu Responds to Nasrallah: Anyone Hiding in a Bunker Should Stay There," *Haaretz*, February 16, 2011, http://www.haaretz.co.il/news/politics/1.1162510.

10 The process of selection is influenced by considerations other than cost and benefit. See, for example, Dan Ariely, *The Honest Truth about Dishonesty: How We Lie to Everyone–Especially Ourselves* (New York: HarperCollins, 2012).

11 For a discussion on deterring non-state actors, see, for example, Adam Lowther, "Deterring Nonstate Actors," in *Thinking about Deterrence*, pp. 195-215; Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research," *Contemporary Security Policy* 31, no. 1 (2010).

12 Remarks by Prime Minister Olmert to the Knesset Plenum, *Ynet*, July 17, 2006, http://www.Ynet.co.il/articles/0,7340,L-3277334,00.html.

13 Ronny Sofer, "Olmert Associates: They Want to Drag Israel into a Response," *Ynet*, June 17, 2007, http://www.Ynet.co.il/articles/0,7340,L-3414045,00.html.

14 Yohai Ofer, "Assessment: Rockets in the North—To Draw IDF into Responding," *Ma'ariv- NRG Online*, January 1, 2014, http://www.nrg.co.il/online/1/ART2/535/865.html.

15 Ronen Manelis, "Between Lebanon and Gaza: Hizbollah in Operation Cast Lead," *Military and Strategic Affairs* 1, no. 1 (2009): 42.

16 Daniel Sobelman, "Four Years after the Withdrawal from Lebanon: Refining the Rules of the Game," *Strategic Assessment* 7, no. 2 (2004): 27.

17 "Portrait of Hizbollah as a Terrorist Organization," Meir Amit Intelligence and Terrorism Information Center, November 28, 2012, http://www.terrorism-info.org.il/Data/articles/Art_20436/H_158_12_1721977627.pdf.

18 In fact, there are those who claim that "the quiet is based primarily on mutual deterrence." Amos Harel, "In Next Conflict with Hizbollah, Iran and Syria May Not Remain on Sidelines," *Haaretz*, November 17, 2013.

19 *NewTV* (Lebanon), August 27, 2006.

20 For example, his remarks on the subject of Hizbollah's involvement in Syria; see Dana Khraiche, "Nasrallah Denies Hizbollah Members Fighting with Syrian Regime," *The Daily Star*, October 11, 2012, http://www.dailystar.com.lb/News/Politics/2012/Oct-11/191066-nasrallah-denies-Hizbollah-members-fighting-with-syrian-regime.ashx; "Syria: Hizbollah Role Grows as Rebels Gain," *UPI,* March 5, 2013, http://www.upi.com/Top_News/Special/2013/03/05/Syria-Hizbollah-role-grows-as-rebels-gain/UPI-94691362517331.

21 Ghassan Bin-Jiddu, "Interview with Hizbollah Secretary General Hasan Nasrallah," *Al-Jazeera,* July 20, 2006, http://www.globalresearch.ca/interview-with-Hizbollah-secretary-general-hasan-nasrallah/2790; Shimon Shapira, "Hizbollah Threatens to Strike Strategic Israeli Targets in Response to an Attack on Iran's Nuclear Facilities," Jerusalem Center for Public Affairs, September 25, 2012, http://jcpa.org/article/hizbullah-threatens-to-strike-strategic-israeli-targetsin-response-to-an-attack-on-irans-nuclear-facilities.

22 Interview with Nasrallah, July 20, 2006.

23 "Nasrallah: 'Israel Cannot Win Any Other War,'" *Republic News Agency*, November 24, 2012, http://www.irna.ir/en/News/80428275/Politic/Nasrallah__Israel_cannot_win_any_other_war.

24 "IDF Officer Warns of Repeat Lebanon War," *Reuters/Ynet*, October 29, 2012, http://www.Ynetnews.com/articles/0,7340,L-4298668,00.html.

25 "Internal Shiite Criticism: Hizbollah Did Not Ask Shiites Their Opinion on the War; Shiites Did Not Give Anyone Permission to Declare War in Their Name," Meir Amit Intelligence and Terrorism Information Center, August 28, 2006, http://www.terrorism-info.org.il/data/pdf/PDF_06_263_1.pdf.

26 Yohai Sela, "Subhi al-Tufayli against Hassan Nasrallah," *Middle East Magazine*, March 3, 2007, http://www.mideast.co.il/p-2_a-101/.

27 Ibid.; Joseph Alagha, *Hizbollah's Identity Construction* (Amsterdam: Amsterdam University Press, 2011), p. 223.

28 "Poll: Most Lebanese See War as Attempt to Remake Region," *The Daily Star*, October 13, 2006, http://www.dailystar.com.lb/News/Lebanon-News/2006/Oct-13/43301-poll-most-lebanese-see-war-as-attempt-to-remake-region.ashx.

29 Richard Wike, "Lebanon's Precarious Politics," Pew Research Global Attitudes Project, November 15, 2007, http://www.pewglobal.org/2007/11/15/lebanons-precarious-politics/; "Most Embrace a Role for Islam in Politics," Pew Research Center, December 2, 2010, http://www.pewglobal.org/files/2010/12/Pew-Global-Attitudes-Muslim-Report-FINAL-December-2-2010.pdf.

30 Chris Harnisch, "2009 Lebanese Parliamentary Elections," *Critical Threats,* June 12, 2009, http://www.criticalthreats.org/lebanon/2009-lebanese-parliamentary-elections.

31 Interview with Nasrallah, July 20, 2006.

32 Robert G. Rabil, "Hizbollah, the Islamic Association and Lebanon's Confessional System: al-Infitah and Lebanonization," *The Levantine Review* 1, no. 1 (2012): 57.

33 Judith Patrick Harik, *Hizbollah: The Changing Face of Terrorism* (London: I.B. Tauris, 2004), pp. 64-79.

34 Martin Kramer, *Fadlallah: The Compass of Hizbollah* (Tel Aviv: Moshe Dayan Center for Middle Eastern and African Studies, 1998); Fadlallah's official web site, http://www.bayynat.org.lb.

35 Yossi Beilin, *The Guide to Withdrawing from Lebanon* (Tel Aviv: Kibbutz Meuhad, 1998).
36 See, for example, Hariri's statement in 2001 about the differences in approach between him and Hizbollah; Daniel Sobelman, *New Rules of the Game: Israel and Hizbollah after the Withdrawal from Lebanon*, Memorandum 65 (Tel Aviv: Jaffee Center for Strategic Studies, 2003), p. 48.
37 Ibid., pp. 48-49; Zvi Barel, "Bashar's Political Radar," *Haaretz*, April 19, 2001, http://www.haaretz.co.il/misc/1.694978.
38 Eli Avidar, *The Abyss: What Really Separates Us from the Arab World* (Tel Aviv: Agam, 2011), pp. 72-73 .
39 For example, Beilin, *Guide to Withdrawal from Lebanon*.
40 Eitan Azani, *Hizbollah: The Story of the Party of God From Revolution to Institutionalization* (New York: Palgrave Macmillan, 2011), Ch. 7-9; Eitan Azani, "Hizbollah between the IDF Withdrawal from Lebanon and the Lebanese National Unity Government: Another Step on the Road to an Islamic Republic in Lebanon," Institute for Counter-Terrorism, Herzliya, 2007, http://lib.cet.ac.il/pages/item.asp?item=19001 .
41 Sobelman, *New Rules of the Game*, pp. 22-23.
42 Amal Saad-Ghorayeb, "Hizbollah's Arms and Shiite Empowerment," *The Daily Star* (Lebanon), August 22, 2005, http://www.dailystar.com.lb/Opinion/Commentary/2005/Aug-22/95333-hizbullahs-arms-and-shiite-empowerment.ashx; On the Shiites in Lebanon, see Fouad Ajami, *The Vanished Imam: Musa al Sadr and the Shia of Lebanon* (Tel Aviv: Am Oved, 2006) ; Avidar, *The Abyss*, pp. 165-87; Shimon Shapira, *Hizbollah between Iran and Lebanon* (Tel Aviv: Kibbutz Me'uhad, Fourth Printing, 2006).
43 Sobelman, *New Rules of the Game*, pp. 43-44.
44 Sobelman, "Four Years after the Withdrawal from Lebanon," p. 26.
45 Meir Amit Intelligence and Terrorism Information Center, "The Struggle to Disarm the Militias in Lebanon on the Basis of Resolution 1559," February 23, 2006, http://www.terrorism-info.org.il/data/pdf/PDF_18904_1.pdf.
46 Ibid.
47 Reuters, September 25, 2005.
48 Augustus Richard Norton, *Hizbollah: A Short History* (Princeton: Princeton University Press, 2007), pp. 131-32.
49 Yigal Tzhor, "The Disengagement from Lebanon," *Maariv- NRG Online*, May 26, 2005, http://www.nrg.co.il/online/1/ART/938/990.html.
50 Daniel Sobelman, "Four Years after the Withdrawal from Lebanon," p. 25.
51 Aluf Benn, "We Need a Nasrallah," *Haaretz*, June 7, 2006.
52 Seymour M. Hersh, "Watching Lebanon: Washington's Interests in Israel's War," *New Yorker* 21 (2006): 28-33.
53 Avidar, *The Abyss*, p. 181.
54 "Poll: Most Lebanese See War as Attempt to Remake Region," *The Daily Star*.
55 Ibid.
56 Army Radio, August 16, 2003.

57 In November 2007, only 7 percent of the Christians and 10 percent of the Sunnis had a positive opinion of Hizbollah; Wike, "Lebanon's Precarious Politics," *Pew Research Global Attitudes Project*.

58 Gallup Poll, November 20, 2006, http://www.gallup.com/poll/25501/few-lebanese-want-Hizbollah-militia-simply-disarmed.aspx. Druze were not included in the poll, but they constitute only about 6 percent of the population. An earlier poll showed that 51 percent favored disarming Hizbollah and 49 percent opposed it. *L'Orient Le Jour*, August 28, 2006, http://www.lorientlejour.com/article/538859/Sondage_Ipsos88__des_Libanais_revent_d%27un_Libana_l%27abri_des_conflits_regionaux_51__des_personnes_interrogees_souhaitentque_le_Hizbollah_delaisse_s.html; a closer examination shows that the wording of the question is similar to that of the question used in the Gallup poll on keeping weapons under any conditions. Therefore, it is possible that those opposed also included Hizbollah supporters who are prepared to disarm the organization at some time in the distant future.

59 "The Majority of Lebanese Support Holding a Referendum on Lebanon's Identity," *Information International s.a.l.*, December 2007, http://information-international.com/pdf/iipolls/2007/Pages%20from%20TheMonthly-issue65-DEC07-English.pdf; "A High Trust in Lebanese Army and Security Forces," *Information International s.a.l.*, March/April 2007, http://information-international.com/pdf/iipolls/2007/Pages%20from%20Ii%20Monthly_March07_issue57-English.pdf; among the Shiites, 91.6 percent supported Hizbollah's possession of weapons.

60 Yohai Sela, "The Political Crisis in Lebanon," Mideast Forum, November 16, 2006, http://the-mef.blogspot.co.il/2006/11/blog-post_16.html ; "Nasrallah and Aoun at the Top but with Fewer Supporters," *Information International s.a.l.*, http://information-international.com/pdf/iipolls/2007/Pages%20from%20Ii%20Monthly-April07%20Issue%2058_English.pdf.

61 "Hundreds of Thousands Protest in Beirut," *MSNBC*, December 1, 2006, http://www.nbcnews.com/id/15981439/#.Uu7Lj_l_uuk.

62 Thanassis Cambanis, *A Privilege to Die: Inside Hizbollah's Legions and Their Endless War against Israel* (New York: Free Press, 2011), pp. 199-212.

63 "Nasrallah: We Have a Right to Smuggle Weapons," *Haaretz/Walla*, February 17, 2007, http://news.walla.co.il/?w=/13/1059053.

64 Meir Amit Intelligence and Terrorism Information Center, November 8, 2007, http://www.terrorism-info.org.il/data/pdf/PDF_07_239_1.pdf.

65 Azani, "Hizbollah between the IDF Withdrawal from Lebanon and the Lebanese National Unity Government"; Amos Harel and Yoav Stern, "Hizbollah: We'll Take 'Concrete Steps' against IDF Flights in Lebanon," *Haaretz*, August 1, 2008, http://www.haaretz.co.il/misc/1.1340273.

66 News Agencies, May 7-18, 2008; William Harris, "Lebanon's Roller Coaster Ride," in *Lebanon: Liberation, Conflict, and Crisis*, ed. B. Rubin (New York: Palgrave Macmillan, 2009), pp. 78-79.

67 Cambanis, *A Privilege to Die*, p. 227.

68 Arik Bender, "Olmert: Nasrallah Has Lost His Self-Confidence," *Maariv-NRG Online*, July 28, 2008, http://www.nrg.co.il/online/1/ART1/765/961.html.

69 Guy Bechor, "Banished from the Sanctuary: On the Death of Muqawama and Where the Commentators Were Wrong," May 20, 2008, http://www.gplanet.co.il/prodetailsamewin.asp?pro_id=822; It appears that Bechor underestimates Hizbollah's influence within Lebanon. See also Alon Levin and Yuval Bustan, "The Great Victor: Nasrallah Fortifies His Political Position," *Focused Coverage*, June 2008, http://www.sikurmemukad.com/magazine/062008/nasrallah.html; Harris, "Lebanon's Roller Coaster Ride," pp. 79, 81.

70 For example, Azani, "Hizbollah between the IDF Withdrawal from Lebanon and the Lebanese National Unity Government."

71 Harnisch, "2009 Lebanese Parliamentary Elections."

72 Benedetta Berti, "The 'Rebirth' of Hizbollah: Analyzing the 2009 Manifesto," *Strategic Assessment* 12, no. 4 (2010): 85 ; Joseph Elie Alagh, *Hizbollah's Documents: From the 1985 Open Letter to the 2009 Manifesto* (Amsterdam: Amsterdam University Press, 2011), pp. 28-31, 39-55, 116-137.

73 "Lebanon Gives Hizbollah Right to Attack Israel," *al-Arabiya*, November 26, 2009, http://www.alarabiya.net/articles/2009/11/26/92423.html.

74 In 2010, 94 percent of the Shiites and 12 percent of the Sunnis supported Hizbollah. Among the Lebanese, 52 percent sided with Hizbollah and 46 percent opposed it. "Most Embrace a Role for Islam," Pew Research Center.

75 Harnisch, "2009 Lebanese Parliamentary Elections."

76 Paul Salem, "Why Hizbollah Doesn't Really Want to Win," *Foreign Policy*, June, 6, 2009, http://carnegie-mec.org/2009/06/06/why-Hizbollah-doesn-t-really-want-to-win/b3re.

77 It has been argued that Iran was furious with Hizbollah in 2006 because it "wasted Iran's most important military investment in Lebanon just because of ... two abducted soldiers." Quoted in Benjamin S. Lambeth, "Israel's Second Lebanon War Reconsidered," *Military and Strategic Affairs* 4, no. 3 (2012).

78 Lilach Shoval, "Hizbollah 2013: The Organization You Didn't Know," *Israel Hayom*, May 11, 2013, http://www.israelhayom.co.il/article/87789; Shimon Shapira, "Is Hizbollah Considering Withdrawing from Syria," Jerusalem Center for Public Affairs, February 5, 2014, http://jcpa.org.il/2014/02/%D7%94%D7%90%D7%9D-%D7%97%D7%99%D7%96%D7%91%D7%90%D7%9C%D7%9C%D7%94-%D7%A9%D7%95%D7%A7%D7%9C%D7%AA-%D7%9C%D7%A1%D7%92%D7%AA-%D7%9E%D7%-A1%D7%95%D7%A8%D7%99%D7%94/ .

79 "Former Hizbollah Leader Subhi Al-Tufayli: Iran Forcing Hizbollah to Participate in Syrian War," MEMRI, May 9, 2013, http://www.memri.org/report/en/0/0/0/0/0/0/7172.htm.

80 Idan Yosef, "Barak: 'Hizbollah Has 40,000 Missiles That Reach Dimona,'" *News1*, August 7, 2008, http://www.news1.co.il/Archive/001-D-170079-00.html?tag=05-18-30.

81 See, for example, Yehoshua Breiner, "IDF Official: Hizbollah Will Launch 600 Rockets Per Day," Walla, July 8, 2010, http://news.walla.co.il/?w=/2689/1704985.

82 "Hizbollah's Weapons Storage Facility Violation of UN Resolution," IDF Spokesman, September 4, 2010, http://www.idf.il/1133-8103-he/Dover.aspx.

83 AP, December 17, 2012; "Explosion Heard South of Ter Harfa Town ... as Usual Hizbollah Cordons off the Area," *Kataeb.org*, http://www.kataeb.org/en/news/details/396921/Explosion+heard+south+of+Ter+Harfa+town...+As+usual+Hizbollah+cordons+off+the+area.

84 "Israel Complains to UN about Rearming by Hizbollah," *Reuters*, December 20, 2012, http://www.reuters.com/article/2012/12/20/us-lebanon-un-israel-idUSBRE8BJ1D220121220.

85 Amir Buhbut, "IDF Responds with Artillery Fire at Lebanon," *Maariv- NRG Online*, January 8, 2009, http://www.nrg.co.il/online/1/ART1/837/333.html; Manelis, "Between Lebanon and Gaza," p. 42.

86 Uzi Baruch, "Lebanese Wave Hizbollah Flags at IDF Outpost," *Arutz Sheva*, July 18, 2009, http://www.inn.co.il/News/News.aspx/192000.

87 Sara Taha Moughnieh, "Sayyed Nasrallah: Drone is ours, it Won't Be the Last ...," *al-Manar TV*, October 11, 2012, http://almanar.com.lb/english/adetails.php?fromval=1&cid=23&frid=23&eid=71210.

88 Roi Kais and Yoav Zeitun, "Hizbollah Denial: We Did Not Send UAV to Israel," *Ynet*, April 26, 2013, http://www.Ynet.co.il/articles/0,7340,L-4372544,00.html.

89 "Nasrallah: Hizbollah Ambushed Israeli Troops," *Now Magazine*, August 14, 2013, https://now.mmedia.me/lb/en/archive/hezbollah-nasrallah-al-mayadeen-israel-labouneh.

90 "Nasrallah Claims Responsibility for Shab'a Farms Explosion," *As-Safir*, April 7, 2014, http://assafir.com/Article/345653/Archive.

91 Michael R. Gordon and Dexter Filkins, "Hizbollah Said to Help Shiite Army in Iraq," *New York Times*, November 28, 2006, http://www.nytimes.com/2006/11/28/world/middleeast/28military.html?_r=0; Michael Gordon, "Hizbollah Trains Iraqis in Iran, Officials Say," *New York Times*, May 5, 2008, http://www.nytimes.com/2008/05/05/world/middleeast/05iran.html?pagewanted=all.

92 "Portrait of Hizbollah," Meir Amit Intelligence and Terrorism Information Center; Jacky Khoury, "Hizbollah Terrorists in Egypt: We Planned to Avenge Mughniyeh's Death," *Maariv- NRG Online*, April 13, 2009, http://www.nrg.co.il/online/1/ART1/878/366.html ; Dexter Filkins, "The

Shadow Commander," *New Yorker* 30 (2013), http://www.newyorker.com/reporting/2013/09/30/130930fa_fact_filkins?currentPage=all.

93 Shimon Shapira, "Hizbollah's Operational Plan: Missiles on Tel Aviv and Occupation of the Galilee," Jerusalem Center for Public Affairs, November 2011, http://jcpa.org/article/hizbullah-discusses-its-operational-plan-for-war-with-israel-missile-fire-on-tel-aviv-and-conquest-of-the-galilee/; "Hizbollah Drill Prepares to 'Occupy the Galilee,'" *Jerusalem Post*, August 23, 2012, http://www.jpost.com/Middle-East/Hezbollah-drill-prepares-to-occupy-the-Galilee.

94 "Galilee–Where Resistance Confronts Enemy Next," *al-Ahed*, September 2012, http://english.alahednews.com.lb/uploaded1/essaysimages/big/2012/09/jalel_995x650%20_en.swf.

95 Shapira, "Hizbollah Threatens to Strike Strategic Israeli Targets."

96 "Hizbollah's Nasrallah Urges Elimination of Israel in Rare Public Speech," *Haaretz*, August 2, 2013, http://www.haaretz.com/news/diplomacy-defense/1.539502.

97 Amit Cohen, "Nasrallah: Revenge for Mughniyeh Will Be Assassination of Israeli Officials," *Maariv- NRG Online*, February 16, 2012, http://www.nrg.co.il/online/1/ART2/337/928.html.

98 Army Radio, December 20, 2013, http://glz.co.il/1064-32425-HE/Galatz.aspx; Itzik Shamli, "Hizbollah Assassinated al-Lakis because He Was Mossad Spy," *Nana10*, December 7, 2013, http://news.nana10.co.il/Article/?ArticleID=1022727.

99 Sara Taha Moughnieh, "Sayyed Nasrallah: We Won't Bargain Existence of Syria for Some Ministerial Posts," *al-Manar*, November 14, 2013, http://www.almanar.com.lb/english/adetails.php?fromval=1&cid=23&frid=23&eid=120790.

100 Roi Kais, "Nasrallah: I Supported Argentina in the World Cup," *Ynet*, August 14, 2014, http://www.ynet.co.il/articles/0,7340,L-4558596,00.html.

101 See, for example, Mordechai Kedar, "Hizbollah and the Syrian Bloodletting Account," *Makor Rishon*, July 14, 2013.

102 Subhi Tufayli feared that the situation would lead the Shiites into an alliance with Israel in the future. Pinhas Inbari, "Upheaval in the Arab World: The Israeli Interest," Jerusalem Center for Public Affairs, July 7, 2013, http://jcpa.org/researcher/pinhas-inbari/.

103 For example, in July 2013, Nasrallah emphasized Israel's belligerent intentions and the need for Hizbollah's power to stop it. Sara Taha Moughnieh, "Sayyed Nasrallah: Resistance Can't be Isolated, Enemy Eye on Galilee in any War," *al-Manar*, July 20, 2013, http://www.almanar.com.lb/english/adetails.php?eid=102629&frid=23&seccatid=14&cid=23&fromval=1#83065.

104 Reuven Erlich, "The Road to War: The Lebanese Arena from 2000-2006," Meir Amit Intelligence and Terrorism Information Center, October 7, 2007,

http://www.terrorism-info.org.il/data/pdf/PDF_07_194_1.pdf; Manelis, "Between Lebanon and Gaza."

105 Amir Kulick, "Hizbollah and the Palestinians: From Defensive Shield to Cast Lead—Its Influence Domestically," *Strategic Assessment* 11, no. 4 (2009), http://heb.inss.org.il/index.aspx?id=4354&articleid=727.

106 See the disagreement between Maj. Gen. (ret.) Giora Eiland and Brig. Gen. (ret.) Yossi Kupferwasser on the question whether Israel should have Lebanon or Hizbollah as a target in a future conflict. *Strategic Assessment* 11, no. 2 (2008), http://www.inss.org.il/uploadimages/Import/(FILE)1226472866.pdf; and http://www.inss.org.il/uploadimages/Import/(FILE)1226473077.pdf, respectively.

Call for Papers

The Institute for National Security Studies (INSS) at Tel Aviv University invites submission of articles for publication in *Military and Strategic Affairs*, a refereed journal published three times a year in English and Hebrew and edited by Gabi Siboni, Director of the Military and Strategic Affairs Program and Cyber Security Program at INSS.

Articles may relate to the following issues:

- Military and strategic thinking
- Lessons learned from military organizations throughout the world
- Military force developments on various subjects, including: human resources, weapon systems, doctrine, training, command, and organization
- Ethical and legal aspects of war and combat
- Military force deployment and operations
- Civil-military relations and decision making processes
- Security/military technology
- Cyber security and critical infrastructure protection
- Defense budgets
- Intelligence
- Terrorism

Submitted articles should not exceed 6000 words (including citations and footnotes), and should include an abstract of 120 words and a list of up to 10 keywords. Only original material that has not appeared in another publication or is under consideration for publication elsewhere may be submitted. Previous issues of the journal may be accessed on the INSS site at: http://www.inss.org.il/.

For further information, please contact:
Daniel Cohen
Coordinator, *Military & Strategic Affairs*
Cyber Security Program
Tel: +972-3-6400400/ext. 488
Cell: +972-50-5772338
danielc@inss.org.il