

# Military and Strategic Affairs

Volume 3 | No. 2 | November 2011

**Responding to the Need for International Legitimacy:  
Strengthening the IDF Strike Force**

Yuval Bazak

**Force Deployment Planning  
in the IDF General Staff**

Gabi Siboni

**A Troubled Geostrategic Marriage:  
US-Pakistan Relations**

Dan Barak, Einav Yogev, and Yoram Schweitzer

**Fighting against Irregular Forces:  
Afghanistan as a Test Case**

Tal Tovy

**Critical Infrastructure Protection against Cyber Threats**

Lior Tabansky



המכון למחקרי ביטחון לאומי

THE INSTITUTE FOR NATIONAL SECURITY STUDIES

INCORPORATING THE JAFFEE  
CENTER FOR STRATEGIC STUDIES



TEL AVIV UNIVERSITY  
אוניברסיטת תל-אביב



# Military and Strategic Affairs

Volume 3 | No. 2 | November 2011

---

## CONTENTS

**Responding to the Need for International Legitimacy:  
Strengthening the IDF Strike Force | 3**

Yuval Bazak

**Force Deployment Planning  
in the IDF General Staff | 19**

Gabi Siboni

**A Troubled Geostrategic Marriage:  
US-Pakistan Relations | 33**

Dan Barak, Einav Yogeve, and Yoram Schweitzer

**Fighting against Irregular Forces:  
Afghanistan as a Test Case | 49**

Tal Tov

**Critical Infrastructure Protection against Cyber Threats | 61**

Lior Tabansky

## **Military and Strategic Affairs**

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

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

---

### **Editor in Chief**

Oded Eran

### **Editor**

Gabi Siboni

### **Editorial Board**

Yehuda Ben Meir, Meir Elran, Oded Eran, Moshe Grundman, Ephraim Kam,  
Anat Kurz, Emily B. Landau, Judith Rosen, Yoram Schweitzer, Giora Segal,  
Zaki Shalom, Gabi Siboni

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

### **The Institute for National Security Studies (INSS)**

40 Haim Levanon • POB 39950 • Tel Aviv 61398 • Israel  
Tel: +972-3-640-0400 • Fax: +972-3-744-7590 • E-mail: [info@inss.org.il](mailto: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](http://www.inss.org.il)

# Responding to the Need for International Legitimacy: Strengthening the IDF Strike Force

Yuval Bazak

## Introduction

The takeover of the Turkish ship *MV Mavi Marmara*, which prompted massive condemnation of Israel, demonstrated clearly the widening gap between how the IDF operates and how its actions are viewed by international public opinion. The IDF appears to have operated in accordance with international law in the face of explicit provocation intended to help a known terrorist organization under the guise of providing it with humanitarian assistance. The justification for the action was obvious, as was the manner in which the IDF acted, both in terms of the mode of action and in terms of the operational level, including the conduct of the fighters whose lives were in danger once they boarded the ship. Therefore, the world's harsh condemnation of Israel was nothing short of hypocrisy.

The *Mavi Marmara* episode did not occur in a vacuum. It was a direct continuation of a campaign waged against Israel in recent years, a campaign whose battles are conducted in the conventional realms – on land, in the air, and at sea – but whose objectives are directed at a different dimension entirely.

The *Mavi Marmara* phenomenon is an element in the asymmetry that characterizes “the new confrontations” between Israel and its enemies. Maj. Gen. (ret.) Giora Romm has called this phenomenon, which characterized the Second Lebanon War, “the rival strategies of Hizbollah and the IDF.” He claims that while the IDF aimed to utilize its aerial superiority against

Col. Yuval Bazak, the former head of the combat doctrine division in the IDF General Staff, is the IDF military attaché in Poland.

Hizbollah's military deployment in Lebanon, Hizbollah launched its short range rockets out of civilian population centers towards the Israeli home front, with its strategic objectives being Israeli society on the one hand, and the international community on the other. Thus a situation is created in which both sides have in practice given up on destroying the other side's strategy, so that the war is conducted "like a football game between two teams playing against each other as if they were on separate playing fields, or like two ships passing each other in the night."<sup>1</sup>

One may draw a direct line from the Kafr Qana event during Operation Grapes of Wrath in 1996, to the allegations of a massacre in Jenin during Operation Defensive Shield (2002), the second Kafr Qana event during the Second Lebanon War in 2006, Operation Cast Lead in 2008-9 and the Goldstone Report issued thereafter, to the *Mavi Marmara* episode in 2010: all are the result of a new strategy devised by Israel's enemies born out of their understanding that it is impossible to successfully overcome Israel's military power directly and therefore it is necessary to limit Israel's capability to wield that power. This new strategy targets two primary arenas where public opinion can affect the IDF's freedom to operate: Israeli society, known to be sensitive to the loss of human life, and the international arena, deemed as highly sensitive to human rights and civilian casualties, especially vis-à-vis those who are perceived as the weaker side in the conflict. This phenomenon thrives on already fertile ground marked by the extensive and multi-dimensional trend to delegitimize Israel's existence.

On the eve of the 2010 Herzliya Conference, the Reut Institute published a comprehensive report entitled "Building a Political Firewall against Israel's Delegitimization." The report claims:

In the past few years, Israel has been subjected to increasingly harsh criticism around the world, resulting in an erosion of its international image, and exacting a tangible strategic price. The Israeli-Palestinian conflict serves as the "engine" driving this criticism, which peaked with and around the Goldstone report on Operation Cast Lead. In some places, criticism has stretched beyond legitimate discourse regarding Israeli policy to a fundamental challenge to the country's right to exist.

The report further claims that such phenomena are not chance events, rather the result of a "delegitimization network" that "tarnishes Israel's reputation, constrains its military capabilities, and advances the One-State

Solution," i.e., undermining the very legitimacy of the existence of the State of Israel as the Jewish state.<sup>2</sup>

During the early days of statehood, IDF thinking, organization, force buildup, and fundamental principles of force deployment were all designed to respond to wars of "no choice." Since the Yom Kippur War, however, the IDF has had to confront the challenge of internal legitimacy in order to gain the support of Israeli society. The initiated operations that became the central feature in the new confrontations demanded that the IDF find new solutions and modes of operation, particularly with regard to the need to reduce the number of casualties, considered one of the most influential factors in the support Israeli society shows for the army. In recent years another significant challenge has been added: international delegitimization, threatening to limit IDF freedom of action to operate force when undertaking its missions.

Indeed, with the rise of the delegitimization campaign, the question of the IDF's use of military force, which was never simple, has assumed extensive and essential ramifications. Therefore, and because the current security and political challenges facing Israel are some of the most complex and significant the state has ever known, it is important to consider how military force can be constructed, prepared, and deployed so that the army will fulfill the missions assigned by the political echelon to defend the State of Israel and its citizens, without furthering the delegitimization attempt and limiting the political echelon's freedom to act.

This essay analyzes the main changes that have occurred in the strategic arena, especially the rising influence of the delegitimization campaign on the deployment of military force. The essay claims that in light of these changes the IDF must formulate a comprehensive strategy to coordinate force buildup and force deployment, and thereby allow an effective confrontation with the complex challenges facing the nation.<sup>3</sup>

### **A World in Flux: Processes of Delegitimization**

Social phenomena, such as the devaluation of national idealism and its replacement by individualism, the loss of leadership authority (which makes it difficult for leaders to garner the consensus necessary for war), the anti-heroism of foreign policy that has become ingrained as the result of failures that have led to disappointments and skepticism regarding the capabilities of leaders to pave a path and lead, and the new media that brings war into people's living rooms and has changed the heroic image

of war in a fundamental way – all of these have constrained the necessary freedom of action for embarking on initiated wars that exact a fairly steep price tag,<sup>4</sup> thereby entrenching retention of the current world order as a value in international diplomacy.

These trends, which developed primarily in the second half of the twentieth century, were ripe once the Cold War ended. Indeed, the fall of the Berlin Wall and the dissolution of the USSR were the signal that brought these trends to the forefront of the stage of Western diplomacy. The “new world” that had suddenly come into being allowed the West, and Europe in particular, to amplify the trend of retreat that began at the end of World War II and increased after the withdrawal from the various colonialist adventures. The tortured European conscience led to revulsion from armed conflict and growing involvement in the defense of minority rights, alongside an increase in the sympathy for freedom fighters struggling for national liberation. Diplomacy has become almost the sole legitimate tool for resolving problems on the international stage, as defense budgets have been slashed, armed forces have shrunk, and the status of the military has been eroded as the result of delegitimization. The emphasis on individual rights in the West has turned public opinion and international law into significant parameters in nations’ abilities to express their military force. All these factors have been tremendously enhanced thanks to the development of the media, which has made it possible to transmit a huge amount of information in real time, greatly affecting the freedom of action of the other side (often in a manipulative manner).

### **The Name of the Game: International Legitimacy**

Legitimacy has always been an essential part of war. However, the conditions created in the West in the second half of the twentieth century, particularly since the fall of the Berlin Wall, have made it a strategic objective in and of itself. The understanding by Syria, Yasir Arafat, and Hassan Nasrallah (as well as other enemies of Israel) that they lack the ability to confront Israel’s military strength directly, together with their desire to maintain the struggle, led them to formulate a strategy that strives to limit Israel’s ability to bring that military strength to bear.

The Yom Kippur War was a turning point<sup>5</sup> that generated a change in the enemy’s strategy – from a direct approach, an attempt to bring about the physical destruction of the State of Israel by means of a military move



to conquer territory, to an indirect approach, by means of terrorist attacks against the civilian population, in an effort to undermine and break down Israeli society (seen as a central weak point), and to reduce Israel's freedom to apply force. Critical to this new enemy strategy were the absence of a political address and work from behind human shields. This approach was integrated into an extensive campaign aimed at undercutting Israel's image and the justness of its cause.

### **Adopting the Standoff Approach**

Time and again, Israel, continuing to rely on the justness of its wars to defend its citizens against terrorist organizations and guerrillas and retain domestic public support by reducing the number of military casualties, found itself in a seemingly impossible strategic trap – caught between its duty to defend its citizens and protect its critical interests and the way these mandates were viewed by ever expanding sectors of the Western world. Thus it happened that while Israel was increasing its physical relative advantage in the tactical and operative realms (particularly as a result of technological improvements), to the point at which it seemed unreasonable for enemies to provoke Israel, the other side changed the rules of the game, identifying the weaknesses and limitations at work on the intra-Israeli arena as well as the on international stage in order to reduce Israel's freedom of action and prevent the IDF from fully realizing its military potential. When Israel nonetheless acted, it paid a high price on the international arena, accelerating the process of delegitimization, strengthening Israel's image as an aggressive pariah state, and further reducing its potential scope of action in future military rounds.

Paradoxically, precisely the steps the IDF took to reduce the casualties among its soldiers by developing standoff fighting capabilities (which encouraged greater support among Israeli society for IDF freedom of action, especially since the IDF now initiated most of the operations), often led to a heavy cost in the legitimacy currency on the international arena. The new operations approach, founded on the rationale of disproportionate response (“the boss has gone wild”), was applied in Lebanon and the Gaza Strip out of the belief that Israel's withdrawal from those areas would earn it the legitimacy to operate there. While in a number of cases Israel did attain some positive results vis-à-vis leaders of terrorist organizations, thereby strengthening Israel's deterrence, this approach also led to steep

costs in terms of international legitimacy, capital whose reserves were dwindling from the state coffers.

In hindsight it seems that this approach, typified by IDF operations since the mid-1990s, played into the hands of Israel's enemies due to the extended length of the operations (while the Israeli civilian front was exposed to ongoing threats), the absence of a clear decision at the end of the fighting, the pictures of refugees from the war zones broadcast continually on TV screens, and operational errors (amplified by means of media manipulation). All of these created a sense in the world that the IDF was the bull wreaking havoc in the china shop without making any sort of real contribution to the nation's state of security.<sup>6</sup> Thus even Operation Cast Lead, viewed in Israel as successful in terms of its military operational achievements, became one of the major events that damaged Israel's international image in an essential way, undermined the nation's status, and imposed additional constraints on the Israeli government regarding future military operations and their goals.

### **The Need for a New Strategy**

Given the current reality, in which it seems that the ability to achieve significant gains on the battlefield drops while the cost on the international arena for every military operation spirals ever higher, how the IDF deploys force is becoming a key question for Israel's national security. Attendant to it are fundamental issues, such as victory and decision, ground maneuver versus standoff fire, duration of fighting and preferred end states, weapons and technology, the relationship between the army and Israeli society, the function of reserve duty, authority between the command structure and organizations and government, and so on. All of these are critical questions in a coherent approach to Israel's ability to concentrate the potential of its power base against the challenges faced by the nation.

Some would argue that the time for the use of military force has passed, that whoever uses it in the current reality is bound to be defeated, or at best, to attain a Pyrrhic victory. Statements such as "terrorism cannot be defeated by military means," or "the problem is social/economic/political/ideological and therefore cannot be resolved by force," have become commonplace in the public discourse of the Western world. A short study of Clausewitz demonstrates the difficulty of defining victory at the strategic level. Clausewitz claimed, "In strategy, there is no such thing as victory...

Strategic-political success can be discerned by means of measurements that lie outside the scope of the military, i.e., in political outcomes, by attaining an improved political position."<sup>7</sup> In other words, the function of military force is limited not to the attainment of a strategic victory, rather to creation of the conditions that allow political efforts to achieve political and security objectives. The relationship between military action and political action, never a simple one, becomes even more complex and significant in the current reality. This emphasizes the need for coordination between the two actions, together with sharp, effective management of the interfaces between them.

Creating a power base is perforce a necessary condition for confronting challenges, though in and of itself force is insufficient. Israel's national security doctrine includes a principle that describes comprehensive force as a product of force in practice and the freedom of action to operate it. In other words, investing in advanced capabilities and excellent manpower does not make an unequivocal contribution to security if the ability to use them is significantly limited by factors such as public opinion, leadership, or international legitimacy. Moreover, the military structure bears responsibility for the scope of action of the political echelon come the end of the fighting. That is, it is the military's obligation to ensure the attainment of the objectives of the war as its primary guideline, but at the very least it must ensure that the political echelon's freedom of action is not constrained once the fighting ends as the result of damage to the nation's international standing.<sup>8</sup> This freedom of action is required for the sake of future decisions to embark on a military operation; room for the political echelon to determine the objectives of the operations as it sees fit; the ability of the military echelon to pick the most appropriate *modus operandi* for the realization of these objectives; and the time frame and conditions necessary to complete the military move and attain the objectives. All are critical for ensuring the effective use of military force when it becomes necessary.

It seems that in light of existing and future threats to Israel, the discussion about the need to prepare for use of military force in different contours is superfluous, leaving behind one central question: what is the strategic approach Israel must adopt in order to be able to act effectively against any threat, attain the goals set by the political echelon, and do so without damaging the nation's legitimacy either at home or abroad?

Over the years, the IDF and the defense establishment have learned to adapt their capabilities to meet the challenges presented by the various arenas even in the thick of the fighting. In the period since the 1982 Lebanon War, and even more so since the outbreak of the second intifada, the defense establishment, standing shoulder to shoulder with the defense industry, has developed impressive capabilities for the operational echelons, in particular the tactical. These capabilities, when combined with vast operational experience and the ability to invent and improvise, have without a doubt bestowed on the IDF significant advantages. But this is no longer enough.

### **Improving the Strike Force and Ability to Operate: Strategy Guidelines**

The defensive plan must be directed not only at attaining victory against the enemy, but also at attaining a rapid victory with a minimum of losses to our side...Only by maximal improvement of the strike force and ability of each and every soldier and branch to operate can we achieve the double outcome required of us: to win in battle and minimize losses.<sup>9</sup>

Ben-Gurion's conclusions about the strategic approach required by the state's newly established army expressed in the clearest way possible the need to bridge the inherent tension between the need for a rapid victory and the need to keep losses to a minimum. He resolved this tension by coining the notion of quality – "improving the strike force and ability to operate" – that from then on became the backbone of Israeli military thinking. When the legitimacy factor is added to the principle of a rapid victory with a minimum of losses, three parameters are clearly required for any military operation:

- a. Almost complete certainty that the desired political goals will be attained
- b. Achievement of the objective at a bearable cost in terms of human casualties and property damage
- c. Protection of the political echelon's freedom of action once the military moves have ended.

The actual goals of military operations vacillate between the maximal, wresting a decision against the enemy, and the minimal, foiling the enemy's strategy. Many arguments have been sounded about the relevance of

decision to present-day confrontations. Clausewitz defined decision as the situation in which we “deny the enemy the ability to actually fight in practice, or in which we bring the enemy to a point at which such a denial is imminent.”<sup>10</sup> By contrast, foiling the enemy’s strategy and moves is designed – in the case of guerrilla warfare – to result in erosion and attrition of the enemy over time (in the examples of the Second Lebanon War and the confrontations in the Gaza Strip – the firing of surface-to-surface missiles to the point of a ceasefire) in order to reach a state of victory through not losing.

It seems that today all agree that no matter what the war’s goals, it is necessary to attain them rapidly. Therefore, today too, similar to Ben-Gurion’s initial directive, the IDF must strive to shorten the duration of the battle. Ben-Gurion assumed that the economic cost of mobilization and the window of opportunity granted to Israel by international factors required a short campaign.<sup>11</sup> This principle is even more urgent today when the civilian and military rears are exposed to rocket fire from the moment the campaign begins.

### **Back to the Maneuvering Approach**

Shortening the duration of the battle requires the IDF to return to the maneuvering approach, which was characteristic of the Israeli army in its early days. The maneuvering approach, unlike the ground maneuver, is an ingenious approach that manipulates the enemy by exploiting the enemy’s weaknesses and strives to demolish its will, thereby causing its complete collapse. As an operational approach, it contrasts with the attrition approach, whose purpose is the destruction of the enemy by exhausting it to the breaking point. The attrition approach is usually considered more conservative, secure, and wasteful in time and means, while the maneuvering approach is considered to be risky and operates quickly and steadily to attain a rapid victory. The famous modern example of an enemy defeated by means of attrition is the war in Kosovo in the 1990s. It was a unique and non-representative situation in which a coalition, unlimited by time, legitimacy, or munitions stockpiles, pressed the Yugoslav dictatorship for eighty days until the latter surrendered. Such circumstances will almost certainly not present themselves to the IDF and Israel in the foreseeable future.

In recent years, it has become commonplace to speak of the limitations on IDF forces as a consequence of the methods adopted by Israel's enemies on various fronts. However, herein also lie weaknesses for the enemy, which can be exploited in an effective military move. These weaknesses are linked to three fundamental disadvantages of any guerrilla deployment: the inability to build contiguous deployments in the depth of the operational space, which is located almost entirely within a civilian area (especially urban); limits on the ability to extend mutual assistance and maintain an offensive defense; and of course, the limited flexibility in altering deployment to respond to developments on the battlefield because of relative inferiority in mobility and command and control structure.

In face of these weak points, the IDF can and must realize its advantages in operational mobility in all dimensions, in deep precision fire supported by intelligence capabilities, and most of all, in command and control, in order to create parallel rapid pressure on all of the enemy's centers of gravity. At the same time, the IDF must improve its ability to defend the forces maneuvering on the front as well as the strategic assets and the civilians in the home front. One may see the Iron Dome and Trophy systems as examples of defensive systems critical to this approach, though not as systems on which the approach rests in its entirety.

The highest priority among all the entities against which the IDF may need to act is regime preservation. Therefore, it is necessary to direct all efforts at creating a real threat to the continued existence of that regime. Presenting the enemy's leadership with a tough dilemma – the continued loss of assets devoted to maintaining the regime versus accepting difficult conditions for ending the military move and entering negotiations – is inestimably preferable to an attempt to create pressure by means of destroying infrastructures or directly targeting the leaders, attempts that lay at the heart of the operational intelligence efforts in the most recent confrontations between Israel and its enemies.

The move proposed herein comes with other marked advantages that have the potential to affect the question of legitimacy: a maneuvering move will always sow less destruction resulting from firepower than that used in the attrition approach, thanks to the maneuvering force's better ability to distinguish civilians from combatants. Furthermore, the ability to supply targets as the result of friction created during a maneuvering move together with intelligence and precision fire capabilities operating in

restricted circles may well reduce collateral damage significantly and result in greater effectiveness of the force brought to bear against the enemy. There is no doubt that maneuvering moves deep in enemy territory pose a greater risk to one's forces. This issue must be addressed in the force buildup processes, both in terms of its technological aspects and in terms of training and preparation.

### **The Media Challenge and Humanitarian Missions**

The presence of forces deep in the heart of enemy territory would make it easier to practice media and humanitarian policies more effectively, two areas that seem to have become major weaknesses of the IDF and foundations of enemy strategy. The notion of bringing war to the urban sphere stemmed not only from the nature of the "popular resistance" as understood around the world, but also from a strategic choice based on the assumption that a military force operating in the civilian sphere would perforce cause damage to infrastructures and the civilian population that could easily be broadcast around the world in real time and stir up public opinion against the aggressor. The shelling of Kafr Qana, the death of the child Muhammad a-Dura in the second intifada, the operation in Jenin in 2002, the killing of the family of Dr. al-Ayash in Gaza during Operation Cast Lead, the *Mavi Marmara* affair, and the stories about the targeting of Sheikh Raed Salah – all located somewhere on the scale from operational error to media manipulation – had a strategic effect on operations as they unfolded. It appears that the combination of the basic camera, broadband access for transmitting information in real time together, and the standard positions of international public opinion creates essential risks in Israel's strategic environment that the state must confront.

One operating assumption vis-à-vis this question must be that a political system cannot effectively confront information and disinformation disseminated at an ever-increasing pace by the enemy or its proxies. The IDF spokesperson's bureau cannot put out a trustworthy announcement that will refute falsified statements distributed by the other side, because there is a clear asymmetry between a state entity and organizations lacking an address. A second operating assumption touches on how the term "proportionality" is understood by world public opinion. Here too, photographs of a destroyed home and an old woman picking through the ruins or of a child next to a tank or an F-16 fighter jet bombing homes in



retaliation for a Qassam rocket attack make it difficult for Israel to transmit the message about the justness of its cause to international public opinion.

What can be done? The IDF must combine offensive elements (positive media) with defensive ones (barring media from the fighting zone). It cannot bar the media for long, but it can and must do so for the relatively short period of time during which it conducts the major operations. As far as time permits, the IDF must strive for media control in the given arena of operations, both by means of physical control that would prevent the uncontrolled entry of journalists and by means of developed capabilities for cybernetic control in the arena of operations that would allow monitoring, filtering, and delay of communications coming out of the arena by means of the various media. Once the force has gained control of the arena, the operations would have a lower communications signature, after which a controlled media policy would be required to deepen the gain over time. Without a doubt, this requires a response in the form of a force that has the necessary technological capabilities, but no less so in the creation of the organizational structures and the training of manpower of a scope and quality required to confront the potential threat inherent in this field.

Regarding the humanitarian realm, the approach must be to turn the weakness into an advantage, both because Israel is not interested in harming civilians and the principle of distinguishing civilians from combatants is a fundamental principle in IDF use of force, and because Israel can leverage the humanitarian question to its own advantage. To do so, the IDF must avoid damaging critical civilian infrastructures that have no direct link to the enemy's ability to fight. The attempt to pressure civilians to exert pressure on their governments so that they will in turn put pressure on the terrorist organizations not only fails to promote the objectives of the war, but also creates an excuse to accuse Israel of causing a humanitarian crisis. Moreover, the IDF must stabilize the civilian system as quickly as possible and work in full cooperation with the local humanitarian organizations. Establishing field hospitals near civilian population centers (or encouraging foreign organizations to do so) and ensuring the supply of humanitarian goods and enforcing proper distribution are critical to the differentiation of civilians from combatants, but to no less a degree to effective (even manipulative) use of the media in order to increase freedom of action in the operational arena.



## Conclusion

David Ben-Gurion once stated:

We possess moral advantages that have a decisive military value: the moral and intellectual superiority of the human element of our people, the recognition of the world of the justness of our undertaking and our ambition. With these two we can withstand any enemy if we prepare properly and equip the population...However, our matter will not be decided by force alone...Without force we are liable to be destroyed. But with force alone we will not implement the vision of redemption, nor will we establish a state.<sup>12</sup>

Since the rise of modern political Zionism, the justness of Israel's cause has been a cornerstone of the goals set by the leadership of the state-in-the-making and later, by the leaders of the State of Israel. It would seem that this element is currently put to a serious test, as Israel scores higher than only Iran, Pakistan, and North Korea on the popularity scale published by the BBC.

One may describe the system delegitimizing Israel as comprising two parallel and mutually fostering circles: one circle of delegitimization operates directly to undermine the legitimacy of Israel's existence as a Jewish state, while the second operates to expand the physical threats to Israel and reduce its freedom of action to operate its military force as a response to these threats. The strategic objective of both circles is identical – to eliminate the existence of the State of Israel as a Jewish state in the region and thereby “correct” the “historical error” generated by the Zionist movement starting in the late nineteenth century.

The challenge now faced by the State of Israel – perhaps the most severe challenge since the War of Independence – requires action in two synchronized circles, both against the multi-dimensional threat to the state's legitimate right to exist (countered through what is erroneously called “public diplomacy”) and against the circle of physical threats, based on the defense establishment's maintained ability to operate effectively. The difficulty the defense establishment must confront stems not only from the need to neutralize these threats, but also from the need to do so without feeding the first circle (as was the case with the Goldstone Report or the events of the *Mavi Marmara*).

More than ever, this challenge, along with the other security challenges faced by the State of Israel, requires the combination of matter and spirit demanded by Ben-Gurion. The changes that have taken place in recent years in the international arena, both in the way in which Israel's enemies act and in terms of the free world's negative attitude to the use of military force to solve conflicts in general, have created a reality thick with tension between Israel's need to defend its population and the international price it must pay to fulfill that task. This issue, amplified by trends of both change and normalization in Israeli society (instead of Israeli society being constantly battle-ready), without a doubt requires a Ben-Gurion-like act to extricate the nation from the tensions and traps ranging from the Winograd Commission Report about the Second Lebanon War to the Goldstone Report about Operation Cast Lead.

Israel must pursue a sphere where it can achieve the results expected by Israeli society and the international community, at a tolerable cost to Israeli society that is also one that Western society and moderate Arab states can live with. Obviously this requires much more than the simple use of force; military force alone cannot resolve the challenges Israel faces. Moreover, every time it is possible to promote Israel's strategic security goals without the obvious use of force (concealed operations, information warfare of various types, and so on) or even without the use of any force whatsoever (through diplomacy, etc.) it is right and proper to do so. However, when Israel is required to use its military force, it would be wise to be prepared to do so in a way that will promote its vital security interests, including those connected to its international standing. Such an achievement by the IDF will generate not only an improvement in the nation's security situation, but will also generate understanding by the other side that the path it has chosen is hopeless. The other side will then again be forced to choose between accepting the existence of the State of Israel in the region and finding a new strategy to destroy it.

## Notes

- 1 Giora Romm, "A Test of Rival Strategies: Two Ships Passing in the Night," in Shlomo Brom and Meir Elran, eds., *The Second Lebanon War: Strategic Perspectives* (Tel Aviv: Institute for National Security Studies, 2007), p. 59.
- 2 Reut Institute, "Building a Political Firewall against Israel's Delegitimization," pp. 13-14, at <http://reut-institute.org/data/uploads/PDFVer/20100310%20Delegitimacy%20Eng.pdf>.

- 3 Military strategy combines the idea of the use of force against future threats with the construction of major capabilities.
- 4 Vietnam for the US and Afghanistan for the USSR were formative events that expressed the paradox of the rise of the power of the superpowers versus their inability to impose their authority on mid-sized and small nations by means of their power. The sense of a useless cost of war caused hesitation and even avoidance in the use of military means.
- 5 In this context, see *Military and Strategic Affairs* 2, no. 1 (2010), specifically, see Gadi Eisenkot, "A Changed Threat? The Response on the Northern Arena," pp. 29-40, at [http://www.inss.org.il/upload/\(FILE\)1289912280.pdf](http://www.inss.org.il/upload/(FILE)1289912280.pdf), and Gabi Siboni, "The Changing Threat," pp. 3-7, at [http://www.inss.org.il/upload/\(FILE\)1289912214.pdf](http://www.inss.org.il/upload/(FILE)1289912214.pdf).
- 6 Francisco Suárez and Francisco de Vitoria, sixteenth century jurists who dealt with the legitimacy of war, determined successful outcomes as one of the significant parameters for examining the justification of a military move. They claimed that "Even a reasonable chance that a war may have a successful outcome is necessary; without it, the benefits of the war will be canceled out by its cost, and the war, despite its justified grounds and good intentions, will only increase suffering." See Yehoshafat Harkabi, *War and Strategy* (IDF-Maarachot Press, Ministry of Defense Publications, 1990), p. 70.
- 7 *Ibid.*, p. 593.
- 8 In a proposal for the document entitled "The Purpose of the IDF" by the Doctrine Department in the Doctrine and Training Brigade, the following was written about the army's functions: "Fulfilling all required actions in a war when it breaks out and attaining the required goals to a sufficient degree without losing territory and without incurring unbearable losses in terms of casualties, destruction, and other damage, as well as our standing on the international arena, especially with relation to our allies."
- 9 David Ben-Gurion, *Road to the State: From the Archives March-November 1947* (Tel Aviv: Am Oved, The Society for the Dissemination of the Thought of David Ben-Gurion, 1994), p. 304.
- 10 Roger Ashley Leonard, ed., *A Short Guide to Clausewitz on War* (Ministry of Defense Publishers, 1977), p. 62.
- 11 In a war against guerrilla forces there is primarily a "major operation," i.e., a maneuver whose purpose is to attain the minimal goal of foiling the enemy's intentions. One may well imagine a situation in which this operation entails successive operations to attain damage to the enemy's capabilities in accordance with the goals to be set by the political echelon.
- 12 Ben-Gurion, *Road to the State*, pp. 494-95.



# Force Deployment Planning in the IDF General Staff

Gabi Siboni

## Introduction

IDF General Staff planning processes relate to two primary areas: force buildup and force deployment. The fundamentals of military doctrine of any army, and particularly the IDF, necessitate full synchronization between the two, and the element that underlies all planning processes is what is needed for force deployment. Upon the establishment of the IDF, these processes were assigned to a single framework: the General Staff Branch.<sup>1</sup> However, more than sixty years later, planning in the General Staff today has been decentralized among various bodies in a way that complicates effective processes.

Of the significant difficulties posed by this situation, three should be singled out. The first is the weakness of planning for force deployment, which ostensibly is the responsibility of the IDF Operations Branch.<sup>2</sup> However, such planning concerns itself with operational aspects of operations planning. The strategic component of planning, on the other hand, is under the authority of the Planning Branch. This situation occasionally results in the lack of a common language as well as built-in difficulties and friction in preliminary planning processes for operational plans, both in times of routine and in real time war situations.

The second difficulty concerns weak planning for force buildup, which must be based on force deployment needs. In practice, the body responsible for force buildup planning in the IDF is the Planning Branch; the Operations Branch has less influence on the process. This separation

---

Dr. Col. (ret.) Gabi Siboni is head of the Military and Strategic Affairs Program at INSS and head of the Neubauer Cyber Warfare Program at INSS.

between the branch in charge of force deployment and the branch in charge of force buildup causes inherent friction and difficulties in the process.

The third difficulty is the absence of synchronization in the planning processes. There is no officer in the General Staff aside from the chief of staff who has authority over the overall operational process. Given the attention demanded of him in his daily affairs, the chief of staff is hard pressed to synchronize force buildup and force deployment processes. This difficulty positions the deputy chief of staff as the natural candidate for synchronizing between the Planning Branch and the Operations Branch. However his work as coordinator and synchronizer is not efficient, due to the fact that he operates through the heads of two branches who, as far as they are concerned, deal with multiple areas rather than the operations process alone. This results in a situation where the operations process is prone to receive inferior and insufficient attention.

The State Comptroller's 2001 Report 52A, which dedicates a sizable section to the Planning Branch at the General Staff, remains valid to this day. In the report, the State Comptroller details an array of failures stemming from the decentralization of the operations planning process and its division between the Operations and Planning Branches. According to the report, the Planning Branch's strategic division, the body meant to supply the strategic operational framework for force deployment planning, has deepened its activity in the strategic-political area rather than focusing on the strategic-operational process. The report states: "The State Comptroller's Office observes that as long as there is no integrative state planning body that bears full responsibility for political-strategic planning or serves as the primary source for this purpose and instead the IDF is charged with this task, the IDF must make certain that the correct balance between investing in what must be done regarding military planning and the requisite contribution in the area of political planning is not violated."<sup>3</sup> The anomaly in IDF operations planning has not changed since, charted in the extensive analysis of these processes in an article in *Maarachot* by Nurit Gal.<sup>4</sup>

This article seeks to examine operational planning within the IDF command in three ways. The first avenue of approach describes the evolution of operational planning and its implementation in the IDF over the years; the second analyzes the principles of operational planning and the limitations of the current situation in the IDF; and the third presents a

possible model that could obviate some of the anomalies that exist today in the IDF. The scope of this article dictates a focus on the General Staff's operational planning for force deployment. The limitations involved in planning processes related to force buildup should be discussed in a separate framework.

### **How the General Staff Acted until Now**

The establishment of the IDF General Staff began in mid-1947 prior to the expected war with Arab countries and continued during the War of Independence. Ben-Gurion's concept of civil-military relations generated a unique command structure: the chief of staff was supreme commander of IDF forces and at the same time subordinate to the authority of the government. The government cannot directly activate military forces but must do so through the chief of staff as military commander. During the War of Independence, several branches of the General Staff were formed to work alongside the chief of staff. The central branch, which oversaw operational activity, was the Operations Branch, which included departments for planning, intelligence, support, engineering, and communications. Furthermore, as specified in the General Staff establishment order of 1948,<sup>5</sup> it had command over the front headquarters as well as those of force deployment bodies such as the air force, artillery corps, and navy. In practice, the Operations Branch under the leadership of Yigael Yadin guided the General Staff in a broad variety of matters, while PM and Defense Minister Ben-Gurion was in direct contact with the heads of the General Staff Branches. This state of affairs continued until the appointment of Mordechai Maklef as Deputy Chief of Staff in October 1949 and his appointment by Yigael Yadin one month later to head the General Staff Branch.<sup>6</sup> This appointment entrenched – for decades – the role of deputy chief of staff as bearing the duties (in addition to his other duties) of head of the IDF General Staff Branch.

In practice, throughout the years the deputy chief of staff has worn two hats. The first was that of deputy, acting as second in command of the military and stand-in for the chief of staff when the latter was absent or unable to function. But in the IDF system of functions and daily performance, the role of deputy chief of staff is of limited significance, because the only and supreme authority as far as the IDF is concerned is

the chief of staff. Accordingly, the role of deputy chief of staff is to maintain his ability to assume the authorities of chief of staff if necessary.

The second hat worn by the deputy chief of staff was head of the IDF General Staff Branch. An order by the supreme command defined the duties of the deputy chief of staff as head of the General Staff Branch and determined that his main duties would include:

- a. Directing and coordinating the General Staff branches and the officers of the professional staff in the General Staff; the air force HQ; the navy HQ; and the other bodies subordinate to the chief of staff.
- b. Shaping the security doctrine of the IDF in accordance with government national security policy.
- c. Preserving war-readiness, including the drafting of operational contingency plans and preparing the IDF HQ post for action.
- d. Exercising responsibility for building, equipping, and ensuring the fitness of the IDF; ensuring IDF preparedness; and exercising responsibility for its doctrine and for its safety.

This state of affairs existed in the IDF for years, where the deputy chief of staff is assisted by an aide holding the rank of major general in order to fulfill his authority as head of the General Staff Branch. Naturally, the fact that the deputy chief of staff was the senior general of the General Staff usually helped him wield the authority needed to coordinate the other branches as per the activity of the General Staff Branch. This authority is reflected mainly in his ability to conduct formal operational discussions with elements in the General Staff, including the IDF Intelligence Branch, the Planning Branch, and others. In effect, the deputy chief of staff served as a link in the IDF's line of command, while engaging in coordination of operational activities, in parallel to his involvement in the process of force buildup.

This situation created a command anomaly. In all IDF headquarters, up to the level of the regional commands, an orderly command structure was maintained, including, in most cases, an operations staff to be coordinated by the General Staff officer (see for example the structure of the IDF regional command HQ or an IDF division HQ). The deputy commander (or the chief of the staff in the case of a regional command headquarters) was not part of the operational track but rather performed force buildup duties or his duties as deputy. However, the lines within the General Staff are tangled, as the deputy chief of staff took it upon himself



to be chief of the General Staff Branch, coordinating the operational track. This anomaly produced an odd command structure in which the chief of staff acts operationally through his deputy, while at the same time directs other staff branches directly.

The establishment of the Operations Branch in late 1999 plus its assumption of a portion of the General Staff Branch's roles (duplicating the job of deputy chief of staff, who continued as the head of the General Staff Branch) made it difficult for the General Staff Branch to fulfill its responsibilities. It wasn't clear who was the IDF General Branch officer; in fact, the General Staff acted without any party that assumed overall authority for matters included within the duties of the head of the General Staff. This situation worsened due to the insufficient authority of the head of the Operations Branch as compared with the other General Staff Branches, in part because Operations was the newest branch and hadn't yet positioned itself fully within the overall General Staff apparatus.

This phenomenon generated significant difficulty for the IDF operations processes. In 2005, recognition of these limitations led then-Chief of Staff Lt. Gen. Dan Halutz to establish two fundamental principles of command. The first concerns the IDF's organizational and command concept. The chief of staff stipulated that the IDF would operate through two tracks: the force buildup track, under the deputy chief of staff, and the force deployment track, under the head of the Operations Branch. The second principle concerns the concept of the General Staff as the operational headquarters of the IDF. The chief of staff stipulated that the General Staff is not an executing body, rather an IDF headquarters body involved in resources allocation and review and coordination of force buildup and force deployment processes by executing bodies.

Chief of Staff Halutz further stipulated that the deputy chief of staff would be charged with three roles: deputy commander of the IDF – as second to the commander of the IDF and his stand-in when he is absent or prevented from functioning; head of staff of IDF headquarters – coordinating the work of the General Staff; and the coordinating authority in the IDF force buildup track. The head of the Operations Branch, directly subordinate to the chief of staff, received overall authority to coordinate IDF force deployment.

The Second Lebanon War interrupted the attempt to implement these changes, and when Gabi Ashkenazi assumed the position of chief of

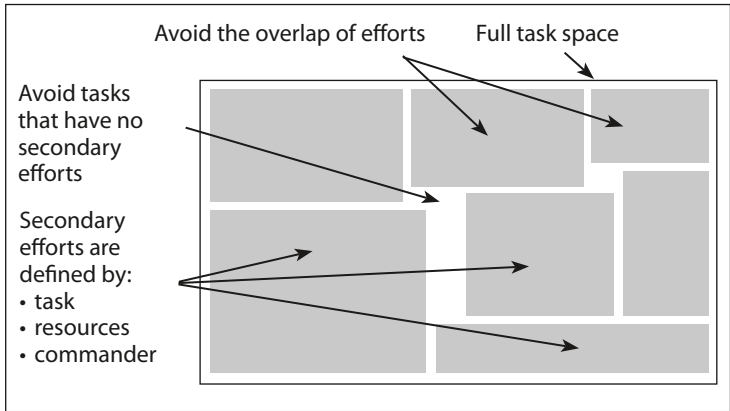
staff in early 2007, the wheel was turned backwards. At the same time a process was launched to formulate an order of the supreme command that would seek to regulate the work of the General Staff and the various IDF headquarters.<sup>7</sup> One component of the process concerned the definition of the IDF general headquarters, and of the deputy chief of staff as chief of the IDF headquarters entrusted with coordinating and directing authorities for force deployment and buildup. Although the supreme command order improved the prior situation, it did not change the authorities of the various branches. Consequently, it did not actually remove the central anomaly of decentralized IDF planning processes between the Operations and Planning Branches.

### Planning Force Deployment

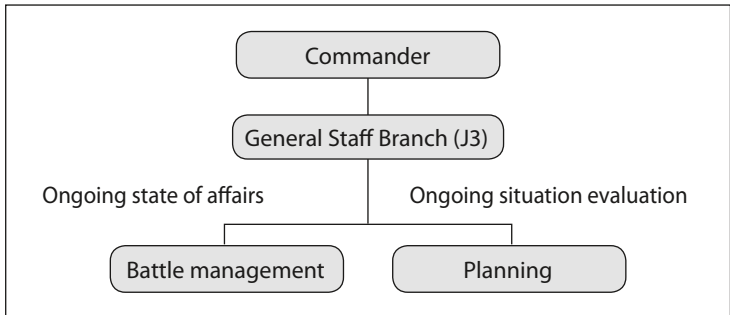
The principles of military planning for IDF force deployment necessitate the existence of a methodical and well-ordered situation evaluation process, which allows the development of an operational plan. Operational contingency plans may be developed beforehand for various scenarios and formulated as operative orders, or alternatively, formulated as an operation order demanding actual execution. The command and control concept of any military organization, in this case the IDF, obliges the methodical arrangement of tasks separated into secondary tasks (some regular and some variable). In this way all objectives and tasks the IDF needs to achieve are fulfilled by the various headquarters and secondary bodies. These fundamentals coalesce in the IDF's principal operational headquarters, e.g., the regional commands.<sup>8</sup>

Figure 1 depicts the art of military planning for force deployment. The figure's outer frame plots the space of the task and the overall objectives to be attained. Dividing the space into secondary tasks makes possible a situation in which the entire task space is covered by the secondary efforts.<sup>9</sup> The art of military planning and command obliges avoiding a situation in which a task space is left without representation by any authority or responsibility.

The process of planning for force deployment is meant to serve one goal: force application when there is an actual call to arms. Therefore one must examine the full circle of command and control, which includes components of planning (battle procedure) and components of actual execution (battle management). These must be coordinated and



**Figure 1: The Art of Military Planning for Force Deployment**

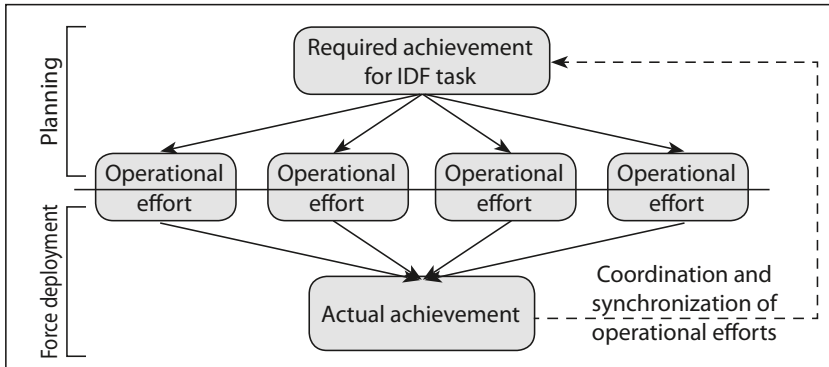


**Figure 2: General Model for Planning and Battle Management**

synchronized in an optimal manner and by a single body (the General Staff Branch), as shown in figure 2.

The art of military command compels the regular review of planned vs. actual performance in order to verify that performance achieves the defined objectives. Figure 3 depicts the full process that comprises both the planning (upper section) and performance (lower section) components. A gap (motley reduction) will always exist between planned and actual performance; therefore it is vital to close the circle and make adjustments following actual situation changes.

As a rule, at key operational headquarters, the officer responsible for coordinating and synchronizing the entire process is the General Staff officer. However, the General Staff Branch was abolished within IDF general headquarters, and its portion of the planning process is performed



**Figure 3: Planned and Actual Performance**

outside of the Operations Branch. The State Comptroller's 2001 Report states: "Since the strategic planning division focused more and more on political-security facets at the expense of military strategy, it was also perceived by the IDF bodies that deal with military strategy (Operations Branch, and territorial arms and branches) as not being a partner in the process of developing operational military knowledge on those levels."<sup>10</sup>

The situation has not changed over the years. Nurit Gal, who served in the Planning Branch, writes:<sup>11</sup>

During the Second Lebanon War, and today as well, the strategic-operational planning process is divided among three separate branches in the General Staff: intelligence evaluation is performed by the Intelligence Branch; strategic planning is done by the Planning Branch; and operational planning is performed by the Operations Branch. In order to produce integrated products, those three branches must cooperate. At times, cooperation is too limited; consequently vital intelligence and relevant strategic insights will not necessarily be expressed in operational plans and orders. On the other hand, operational limitations will not necessarily be expressed when defining strategic purpose. Thus this process exists in a form that is neither complete nor effective.

Such a state of affairs necessitates change. The following guidelines address the requisite change.

## Action Proposals

The IDF approach to command and control supplies a whole response to the needs of force deployment. This exists in a reasonable form at the various main headquarters, but a serious disruption has occurred at IDF headquarters. Seemingly, the desired alternative is the “zero” alternative: bringing the system back to the starting point, i.e., reestablishing the IDF General Staff Branch while unifying the relevant branches (Intelligence, Operations Branch, Planning Branch) under one roof.<sup>12</sup> Or, alternatively, parts of the Operations Branch and Planning Branch could be united while adopting the existing model in the IDF through to the level of territorial command. Indeed, there is no doubt this alternative could supply a framework for developing and regulating a complete response for planning processes for both deploying and building force. However, we can assume there would be great difficulty in implementing this framework amid the existing state of affairs in the IDF.

One can also propose another alternative based on the principle of uniting all authorities for planning force deployment within the framework of the Operations Branch and adapting it to the new situation, with a clear division of its duties (synchronized by the head of the Operations Branch) between two working frameworks: the Planning Division and the Operations Division.

The Planning Division could supply a complete, overall response for force deployment planning in the General Staff, from the strategic level to the operational level and culminating in formulating and actually producing operation orders. The importance of creating a planning totality within one framework – starting from developing strategic ideas through to actual formulation of operation orders – is a cornerstone of IDF principles of command and control that exist at all levels, down to the level of territorial command. Command and control principles necessitate the existence of ongoing and permanent processes of situational awareness. Consequently, the proposed Planning Division would be required to carry out regular planning processes in which different alternatives would be drafted and proposed to the chief of staff. When the chief of staff chooses an alternative or decides on a different option, his instructions would be relayed to the Planning Division. Subsequently, the Planning Division would need to formulate them as an operation order to be carried out by key headquarters. The Operations Division would focus on control, synchronization, and

the management of actual operations, verifying that the operations of key headquarters are managed in view of plans and actual orders together with strategic goals that have been set.

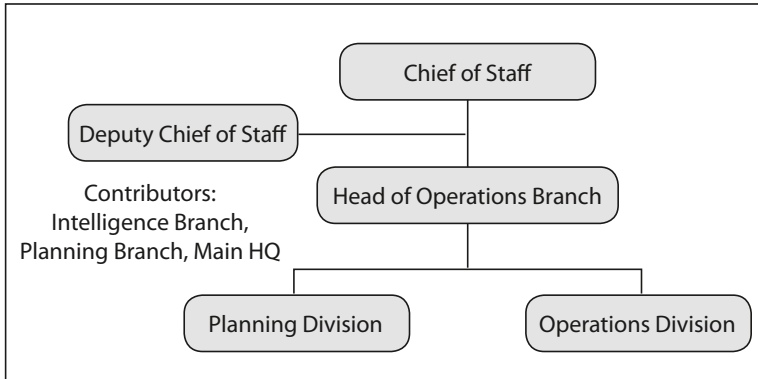
Tables 1 and 2 chart the advantages and disadvantages of the two possible alternatives via two main indicators: the quality of the response to the presented problem, and the ability to be implemented under the current IDF situation.

**Table 1. Unification of Branches – Establishment of the General Staff Branch**

	Advantages	Disadvantages
<b>Quality of the response</b>	<ul style="list-style-type: none"> <li>• The response matches the needs of the IDF from the aspects of planning for force buildup and force deployment.</li> <li>• Unifying the branches under one commander could produce significant synergy by reducing resources and making the planning process more efficient and focused.</li> </ul>	<ul style="list-style-type: none"> <li>• Over the years, the strategic force in the Planning Branch evolved to become also a staff arm of the political echelon as needed.<sup>13</sup> Establishing the General Staff Branch might dilute this capability, leaving the political echelon without capabilities for strategic-military analysis.</li> </ul>
<b>Ability to be organizationally implemented</b>		<ul style="list-style-type: none"> <li>• Difficulty in implementing the change due to decades-long organizational history.</li> <li>• Difficult to administer a change of this scale in tandem with the need to maintain military readiness and fitness in the face of threats.</li> </ul>

**Table 2. Unification of the Planning Authorities in the Operations Branch**

	<b>Advantages</b>	<b>Disadvantages</b>
<b>Quality of the response</b>	<ul style="list-style-type: none"> <li>• The response partially matches IDF needs from aspects of planning for force buildup as well as force deployment; however it supplies a significantly better response than exists in the current situation.</li> <li>• Separating the duties for the operational process in the Operations Branch into two frameworks, planning and operations, would enable the management, coordination, and synchronization of the entire operational process within one command framework.</li> </ul>	<ul style="list-style-type: none"> <li>• Supplies a response to force deployment needs but does not supply a full response to force buildup needs.</li> </ul>
<b>Ability to be organizationally implemented</b>	<ul style="list-style-type: none"> <li>• Implementation is relatively easy, transferring authorities of strategic-operative planning from the Planning Branch to the Operations Branch (in practice: defining the strategic purpose).</li> <li>• The Planning Branch would supply strategic insights to the operational body.</li> </ul>	<ul style="list-style-type: none"> <li>• No significant disadvantages.</li> </ul>



**Figure 4: Planning in the Operations Branch**

Clearly the preferred and more readily implemented alternative places all planning authorities in the Operations Branch, as depicted in figure 4.

Accordingly, the head of the Operations Branch can manage the entire operational process, from strategic planning to operational planning, formulating the command order and culminating in managing the operations of key operations HQ. Similar to the Intelligence Branch, which supplies intelligence for the purpose of portraying and evaluating the present situation, the Planning Branch would supply the Operations Branch with strategic insights formed within the Planning Branch.

This recommendation sits well with the recommendation of the State Comptroller in his 2001 Report.

Seeing as the Operations Branch, which possesses operational knowledge within the General Staff Branch, has been defined in a directive of the Supreme Command as being responsible for developing the force deployment approach... and since, in the opinion of the Office of the State Comptroller, it is fitting to declare a single staff entity in the General Staff Branch as responsible for overseeing, synchronizing, and channeling the process for the development of strategic-military knowledge...it is fitting for the Operations Branch, which oversees the operations division, to be imposed with overall responsibility for this.<sup>14</sup>



## Conclusion

Regulating a division of authority between the Operations Branch and the Planning Branch, in tandem with creating a planning framework in the Operations Branch and clearly dividing its duties with those of operations, could produce a new situation. It would enable a single, coordinating entity in the General Staff to focus on force deployment processes while afforded with a view of the entire operational picture. Such an arrangement would also assist in developing and coordinating a full and comprehensive military situation evaluation. This kind of situation evaluation obliges reliance on two informational components: intelligence information that includes a relevant intelligence picture, alongside information concerning fitness of IDF forces, quantitative evaluation of IDF resources and their quality, operational deployment, and limitations vis-à-vis force deployment. Only a reliance on these two informational components can make possible a complete military situation evaluation. Upon the regulation of the authority of the Operations Branch in relation to exercise of force, it will be possible to realize a full and ongoing IDF military situation evaluation.

The real test of this concept will be in its practical implementation. The command concept is a core component in the optimal functioning of a hierarchal body such as the IDF as well as in warfare success against the gamut of operational challenges. The IDF must make sure that the command concept of the coming years is based on its own command and control doctrine. At the same time it must understand that the realization of this concept constitutes a vastly greater challenge due to the persistent and continuing threat to its basic principles of command and control. Examples of this threat's materialization are woven into the operational history of the IDF, including in the Second Lebanon War. Suffice it to recall the war's operational burdens, which almost led to a paralysis and degeneration of IDF operational capability.

IDF commanders must remember that the goal of all command and control processes is to produce a maximal operational flow: in other words the ability to fulfill as many tasks as possible with a high quality response and within the shortest time possible. All bodies in the General Staff must internalize the fact that their supreme role is to enable the key operational headquarters to act at the highest possible level of effectiveness and efficiency.

## Notes

- 1 This was the situation only from 1949 to 1953.
- 2 The Operations Branch of the IDF is similar in function to the J3 Branch of the US Army.
- 3 State Comptroller's Report 52A, 2001, p. 77.
- 4 Nurit Gal, "Where Have All the Senior Command and General Staff Branch Gone?" *Maarachot* 431, June 2010.
- 5 Brief, AGA / 0, MATKAL / AGA, guidance, June 27, 1948, IDF archives.
- 6 The General Staff Branch (AGAM) was appointed as the branch to coordinate all actions of the General Staff. In practice, no new branch was established; instead this was a formalized definition of the authorities and roles of the Deputy Chief of Staff.
- 7 Shir Cohen, "Thus the IDF Sees Itself," August. 4, 2008, <http://www.shavuz.co.il/magazine/article.asp?artid=3067&secid=2026>.
- 8 Despite this fundamental principle, in the past it was possible to note cases in which tasks were left directly for the General Staff, as directly responsible for activating operational forces. One must bear in mind that the General Staff is not a command agency but a headquarters agency. The sole command element in the General Staff is the chief of staff. Thus in many instances, the chief of staff found himself as direct commander of operational forces, simultaneous with the principal headquarters. Each command body in the military hierarchy is invariably given the authority to command through to the lowest rank; however, the actual fulfillment of this authority must be in extreme and extraordinary cases.
- 9 One must always make certain that there is no overlap of tasks among the efforts, because otherwise there would be tasks with more than one body that is authorized to perform them.
- 10 State Comptroller's Report, 52A, p. 88.
- 11 Gal, "Where Have All the Senior Command and General Staff Branch Gone?" p. 14.
- 12 Within the context of the discussion in principle, it can be said that occasionally one can obtain cooperation and synchronization, even between separate branches. Subordinating different bodies within one organizational framework must be done while examining the relative advantages and conflicts of interest in the shared work across the full extent of the work and tasks of the bodies. In this way one can identify the optimal organizational equilibrium point.
- 13 In this context, see the State Comptroller's Report 52A, section 4: "Realization of the roles of the Strategic Planning Division in matters of military strategy."
- 14 State Comptroller's Report 52A, p. 89.

# A Troubled Geostrategic Marriage: US-Pakistan Relations

Dan Barak, Einav Yogev, and Yoram Schweitzer

## Introduction

The targeted killing of Osama Bin Laden by the United States in early May 2011 and the complex sequence of related events, including the terrorist attack by the Pakistan-based Haqqani network<sup>1</sup> on the American Embassy in Kabul in early September, have thrown the complicated relationship between the US and Pakistan into the spotlight. The two nations are deeply divided with regard to the war on terrorism, reflected in recent months by increasingly loud calls by members of Congress to end military and economic aid to Pakistan in light of suspicions and accusations by senior army officers, chief among them then-outgoing Chairman of the Joint Chiefs of Staff Admiral Mike Mullen, that the Pakistani intelligence services have helped Haqqani's network and have not taken a firm enough stand against terrorist organizations located within the state's borders. During a surprise visit to Kabul in late October, Secretary of State Hillary Clinton even declared that Pakistan must be part of the solution to the Afghanistan issue and take a more aggressive stance at home in the war on terrorism.<sup>2</sup> For its part, the Pakistani parliament has threatened sanctions and demanded the end of American drone attacks in Pakistani territory.<sup>3</sup> Likewise, following the White House's rebuff of Admiral Mullen's comments,<sup>4</sup> Pakistani Prime Minister Raza Gillani claimed that the Pakistani nation had scored a victory against the Americans, as the unification of the political parties caused the US to signal that it needed Pakistan and could not win the war on terrorism without Pakistan.<sup>5</sup>

Dan Barak is an intern at the Institute for National Security Studies. Einav Yogev is a research assistant at the Institute for National Security Studies. Yoram Schweitzer is head of the Program on Terrorism and Low Intensity Conflict at INSS.

Nonetheless, in the midst of this sparring, the two nations, partners in the war on radical Islamic terrorism, are trying to maintain a correct relationship. Prime Minister Gillani repeatedly stressed that although US-Pakistan relations have fluctuated, they are starting to return to the proper course, with a shared drive to continue to work together towards peace in the region and advance issues besides the war on terrorism.<sup>6</sup> President Obama too tried to temper the atmosphere: in a speech in early October he stated that while the US would not feel comfortable with its strategic links with Pakistan should Islamabad fail to consider American interests, at this point the US would continue its assistance despite the concern about connections between the Islamabad intelligence community and radical Islamic elements in Afghanistan.<sup>7</sup>

This essay surveys Pakistan's national interests and the rationale underlying its posture vis-à-vis the United States, especially regarding cooperation in the war on terrorism. It also examines the regional struggles in which Pakistan is involved, specifically, its bitter conflict with India and its relations with China. Despite the recent US criticism of Pakistani conduct and deteriorating bilateral relations, a comprehensive examination of the geostrategic regional situation and the interests of both the United States and Pakistan reveals the sensitive complexity of the arena in which Pakistan operates and the fact that American involvement is indeed bearing fruit and contributing to regional stability.

### **The Pakistani Paradox**

Pakistan was established as a secular state after it was apportioned territory from India in order to realize the autonomous ambitions of India's Muslim minority. In practice, religion has always served politicians and the military, especially during the rule of General Muhammad Zia-ul-Haq, when the function of the military was defined as defending not just the state and the people but also Islam itself. Yet despite the centrality of Islam in Pakistan, the country produced a Western-oriented secular elite, a product of the era of British control. Many members of this elite were educated in the West and adopted a liberal democratic outlook. However, the regional instability of central Asia in the last decade and the lack of internal peace in Pakistan have challenged the development of a democratic society with an efficient public sector and proper educational and employment infrastructures: a difficult economic situation, high unemployment, the

lack of human capital, and natural disasters together with a low rate of tax collection, which quickly depletes government coffers and makes it hard to implement the structural reforms required to stimulate economic growth, have all led to growing alienation between the Western secular elite and the tradition-minded majority that has experienced counter processes of religious radicalization, and to an undermining of political stability and functional political administration in Pakistan.<sup>8</sup>

The religious radicalization of the Muslim population and the tension with the secular elite became highly apparent with the violent ouster of national leaders from the secular liberal elites, namely Zulfikar Ali Bhutto, who established the Pakistan Peoples Party, and his daughter, Benazir: Zulfikar was found guilty in a controversial trial and hanged in 1979,<sup>9</sup> while Benazir Bhutto was assassinated by radical Islamic elements in 2007 during her term as prime minister.<sup>10</sup> In addition, inspired by clerics of the Red Mosque in Islamabad and led by Baitullah Mehsoud,<sup>11</sup> 2007 also saw the establishment of the organization known as the Pakistani Taliban, a union of a number of Islamic militias. The organization's goal is to topple the secular regime and end the support to the US in the war on terrorism. To date, it has carried out many acts of terrorism in Pakistan, exacting hundreds of civilian and security service lives.<sup>12</sup> 2010, for example, was notable for particularly "quality" attacks, with a growing number of explosions taking place in major cities (unlike previous years when attacks were generally carried out in outlying areas), where the average number of injured and dead per attack also rose. In addition, the assassinations of liberal political figures continued; in 2011, Salman Taseer, the governor of the province of Punjab and a leader of the resistance to religious radicalization and the imposition of infidel laws, and Shahbaz Bhatti, the Roman Catholic Federal Minister for Minorities, were murdered, the former by his own bodyguard and the latter ambushed by the Pakistani Taliban.<sup>13</sup> Nonetheless, the concerted efforts of the Pakistani and American security services led to a drop in the number of attacks in 2010 compared to the previous year.

Over the years, religious tensions, problems of governance, and the shaky democratic infrastructures in Pakistan have created a political culture that positioned the military as the strongest force in the country. Consequently, throughout its existence Pakistan has alternated between military and civilian rule. The undermining of internal stability during civilian regimes triggers military intervention and control; the renewed

imposition of military order generates public disgust with the military regime and the return to civilian rule, and thus the cycle begins anew. Still, the extensive power and freedom of action enjoyed by Pakistan's military and its Inter-Services Intelligence (ISI) have made it difficult for the government to channel the nation's resources towards the promotion of national interests. This has dramatized the leadership crisis in the country, manifested by the election of President Asif Ali Zardari by virtue of his status as the widower of Benazir Bhutto rather than on his own record, and challenged American efforts to advance democracy in Pakistan.

This dynamic is also a result of the ongoing conflict between Pakistan and India, its neighbor to the east, regarding the region of Kashmir. Two-thirds of the region was given to India during the division between the two countries in 1947, despite the region's Muslim majority. The national ethos of the struggle with India has contributed much to securing the undisputed status of the military establishment in Pakistan.<sup>14</sup> In addition, India's extraordinary development in recent decades has determined its military superiority over Pakistan, which has since then worked tirelessly to acquire military aid from its major allies, the US and China, which increases Pakistan's dependence on them and limits its political scope for maneuver.<sup>15</sup> Today the balance of military power against India rests on Pakistan's nuclear program, which includes 80-100 nuclear warheads and impressive missile capabilities. However, this effort comes at an enormous monetary cost: fully one-quarter of the national budget is earmarked for security.<sup>16</sup> In tandem with the balance of nuclear terror between the two countries, Pakistan supports terrorist organizations active against Indian targets in Kashmir. These organizations carry out joint activities and share a similar ideology with al-Qaeda, the Haqqani network, and the Afghani Taliban, all operating against Pakistan's major ally, the United States. Some see this as one of the most compelling reasons for Pakistan's refusal to respond to the American request to undertake a broad offensive operation in the Federally Administered Tribal Areas (FATA), the mountainous buffer zone between Pakistan and Afghanistan and host to many terrorists.<sup>17</sup>

The Pakistani regime is thus caught between the need to maintain an internal support base among the Pakistani public, which is experiencing a process of religious radicalization that leads to identification with terrorist organizations and repugnance towards the Western presence in the region (a sentiment that has of late trickled down to some senior security officers),

and the desire to retain American support, which is imperative given India's growing economic and military power and given the risk to the viability of Pakistan's state institutions.

### Relations with the US

US-Pakistan relations date back to the establishment of Pakistan and have known ups and downs. The first significant bond between the two nations was in the context of the 1955 Baghdad Pact, which allied the Muslim nations bordering the USSR and was supposed to serve as a buffer against Soviet expansion into Asia. During the India-Pakistan War of 1965, America's refusal to send weapons to Pakistan led to a sense of betrayal and distrust on the part of many Pakistanis towards the US. This sentiment grew stronger when the US cut military aid in 1979 after the Pakistani nuclear program came to light. Relations improved later that year when the USSR invaded Afghanistan and the US Congress authorized the resumption of security assistance, despite Pakistan's nuclear program. The nuclear test Pakistan conducted in 1998, in response to a nuclear test by India, again derailed relations with Washington. The 9/11 attacks against the US in 2001 served as a catalyst for a renewed closeness of relations, largely due to the understanding by General Musharraf, who headed Pakistan at the time, that Pakistan had better join the angry United States after the attacks rather than be identified as an opponent and risk a direct confrontation, as was the case with Iraq and Afghanistan. For the US, helping Pakistan become a more stable and democratic nation fighting radical Islamic terror elements became a central goal in the post-9/11 era.

Once US-led NATO forces took control of Afghanistan, the al-Qaeda and Afghani Taliban leaders fled to the tribal region inside Pakistan. Since then the area has become a veritable terrorism paradise for a number of reasons: relative independence and only partial subordination to the central government, closeness to the Afghani border, and in particular, relative protection against the Americans. The freedom of action enjoyed by terrorists in FATA also extends outside of Pakistan, especially in the major battleground in the area, Afghanistan. Indeed, 2010 was the deadliest year for NATO forces in Afghanistan as a result of the movement of terrorists across the mountainous Af-Pak border. Therefore, when the US understood that Afghanistan's "terrorism central" had moved into Pakistan – a sovereign nation that offered a very limited scope of action



compared to Afghanistan – it adopted the new method of attack, namely drones. This method earned silent approval from the Pakistani government and has had some successes, most recently the killing of Ilyas Kashmiri, a senior al-Qaeda operative, in early June 2011.<sup>18</sup> The scope of these attacks has significantly increased since they began, from about 35 in 2008, to 53 in 2009, to 117 in 2010, primarily against Taliban and Haqqani network operatives.

At the same time, the increase in the number of aerial attacks by the US has caused a higher number of Pakistani civilian deaths and added to the frustration of the Pakistani public, which views these attacks as an American infringement of Pakistani sovereignty. Moreover, the need for precise intelligence to assist American drone attacks has translated into more CIA personnel on the ground and, consequently, friction with the locals: in January 2011, a CIA contractor named Raymond Davis shot two Pakistani intelligence personnel to death in Lahore, suspecting they were about to rob him. Davis was arrested immediately after the incident, despite his diplomatic immunity, and many Pakistanis demanded that he be tried for first degree murder, a capital offense. After a month of discussions, Davis was smuggled out of Pakistan following a compromise that involved the US paying blood money to the families of the dead men. The Davis incident generated a public debate about the scope of clandestine activity by American intelligence personnel in Pakistan and became a cause célèbre for local politicians opposed to American activity in the country. The negative feelings in the Pakistani street, as expressed in this public debate, range from fear of an American takeover and confiscation of the nuclear installations – a source of Pakistani national pride – to an extreme scenario in which the US topples the government and conquers Pakistan, similar to events in Iraq and Afghanistan.<sup>19</sup>

Another source of friction between the US and Pakistan is the Pakistani interest in Afghanistan. The Pakistani regime supported the Afghani Taliban upon its inception, assisted the military coup that brought it to power in 1995, and was one of only three nations (along with Saudi Arabia and the UAE) that recognized its rule. Even today, with Pakistan defined as a major non-NATO ally, a status that brings it extensive military and economic assistance from the US, there are contacts between its intelligence services and the Afghani Taliban, which are obviously contrary to American interests.



Hostile Pakistani public opinion and concerns about Pakistan playing both sides have damaged the willingness of several US lawmakers to continue to budget either civilian or military aid to Pakistan. Rep. Steve Chabot (R-OH) conveyed this sentiment when he remarked, "We spent all this money and they still hate us."<sup>20</sup> Moreover, the identification of Osama Bin Laden's complex in the city of Abbottabad near the capital of Islamabad and the presence of other al-Qaeda leaders in Pakistan (such as the Quetta Shura, including the Afghani Taliban's senior leadership headed by Mullah Muhammed Omar, who fled Afghanistan when the Americans invaded) strengthen the claim that terrorist leaders are in fact assisted by Pakistan's security services. In addition, Pakistan has time and again failed to maintain its military achievements in the war on terrorism or translate them into successes in the civilian realm; areas that were cleared of terrorists are reclaimed by terrorists in the absence of a stable local government (in some areas, the military has engaged in a third round of cleansing in the last two years). Therefore, it is not inconceivable that the next stage in the war on terrorism in Pakistan may go beyond the FATA borders and entail expanding American drone attacks into the Balochistan region.

And so, while the tension between the US and Pakistan continues to grow because of hostile public opinion; a terrorist attack on the embassy in Kabul – which according to Admiral Mullen took place with the full foreknowledge of Pakistan's intelligence community; and the extensive presence of terrorist operatives in FATA, the Americans continue to try to enlist the support of the government in Islamabad for the decisive battle against the terrorist organizations by means of a joint attack by both countries. However, this desire conflicts with an obvious interest of Pakistan, which is trying to maintain good relations with elements that support groups active against India in Kashmir.

Still, despite the angry reverberations from declarations by senior American government and military personnel, a closer examination of Pakistan's war on terrorism demonstrates that America's copious criticism is both overstated and imprecise in several ways. First, of all the nations fighting terrorism, including the United States, Pakistani security forces have suffered the greatest number of casualties, with close to 4,000 dead. Second, Pakistani security forces have succeeded in catching senior al-Qaeda and Taliban leaders, such as Khaled Sheikh Muhammad, the brains

behind 9/11. Third, the Pakistani army and border patrol have long been fighting the terrorist organizations in FATA, and have paid for this with serious retaliations on the internal arena following the establishment of the Pakistani Taliban, which carries out many attacks targeting both urban centers and the security services. Fourth, the fact that Pakistan permitted the stationing of CIA agents on its soil and agreed to American drone attacks was another important contribution to the war on terrorism, coming at the cost of damaging the legitimacy of the regime in large segments of the Pakistani population and arousing a great deal of opposition.

Therefore, some of the criticism should be addressed to the US, given that the vast majority of the economic aid it awards Pakistan goes towards military ends rather than to strengthening its democratic nature by means of reforms or investments in civilian infrastructures. The Kerry-Lugar-Berman 2009 Enhanced Partnership with Pakistan Act was an attempt to deal with this problem. It made clear that security assistance to Pakistan was conditional on State Department authorization that Pakistan was not a state sponsoring terrorism (especially the Taliban and the Haqqani network) and is working to root it out.<sup>21</sup> Other conditions for military aid were: gaining access to Pakistan's nuclear installations and nuclear knowledge distribution network; confronting Pakistan legislatively over money laundering; and receiving a commitment that the Pakistani military is not undermining the political echelon and that its power is limited. In response to these requirements, Secretary of State Clinton submitted an affidavit in this spirit in mid-March 2011, when the preparations for killing Osama Bin Laden were in high gear. Even then there were Congressmen who called for a reexamination of US-Pakistan relations and a freeze on economic assistance until receiving clarifications from the Pakistani government about its commitment to the war on terrorism. In response, Kerry and Lugar published statements about the need to continue to support Pakistan in order to allow control of nuclear proliferation and pursue the war on terrorism.<sup>22</sup>

Past events have shown that the US can greatly influence Pakistan: when then-President Musharraf dismissed the president of Pakistan's Supreme Court, suspended the constitution, and instituted emergency rule, he was forced by then-Secretary of State Condoleezza Rice to give up one of the functions he was fulfilling – president and commander of the army. In a different instance, in 2010, when floods brought Pakistan

to the verge of collapse and there was a real concern that the army would try to wrest control of the country, it was again the US that intervened and ensured the survival of civilian rule. It appears that the current crisis in US-Pakistan relations indicates a greater Pakistani willingness to push the envelope, reflected, for example, in statements by Prime Minister Gillani and threats made in the Pakistani parliament to attack American supply convoys to Afghanistan traveling through Pakistan unless the drone attacks are suspended and the American military presence is curtailed. For its part, the US policy combines high level diplomacy and economic assistance, plus encouragement of the Pakistani army to act against terrorism networks, together with the attempt to limit the political influence of the security forces.

Some of the current tensions between the US and Pakistan may be attributed to the sudden death of America's special envoy to the region, Richard Holbrooke, who enjoyed a special status there, was an expert in all regional matters, and was a proponent of a policy that placed greater emphasis on the civilian aspect than on the military,<sup>23</sup> and to the fact that he was replaced by American security personnel. The latter tend to lend greater significance to military parameters in every examination of Pakistan's efforts in the war on terrorism, thereby strengthening claims by Pakistani regime officials that the US is fairly indifferent to Pakistan's own national security needs in the region and is conducting itself arrogantly in its repeated infringements of Pakistani sovereignty.

### **China as an Alternative to the US**

Pakistan's second significant ally after the US is China, which shares a border with northern Pakistan and in the context of a longstanding alliance – strengthened after the 1962 Sino-Indian War when Pakistan was viewed as a balance to India – provides Pakistan with extensive economic and military aid. Chinese assistance includes various components in the Pakistani nuclear program, key platforms such as fighter jets, and even a 2001 initiative for a joint Sino-Pakistani project for planning and manufacturing a battle tank called the MBT 2000. In exchange Pakistan has shared technological intelligence about American weapons with China, including selling China one unexploded Tomahawk cruise missile from the 1998 failed attempt to kill Bin Laden when President Clinton was still in office and sharing F-16 fighter technology on the basis of the plane's

service in the Pakistani air force. Recently the Chinese asked Pakistan for the fragments of an American helicopter that was grounded and then bombed during the raid in Abbottabad during Operation Geronimo to kill Bin Laden and which may have been equipped with advanced stealth technology.

However an examination of past confrontations between Pakistan and India (1947, 1965, 1971, and 1999) shows that China did not help Pakistan in any significant way in any of them, and even sided openly with India in 1999 in the Kargil conflict. Moreover, as a member of the UN Security Council, China has voted for defining the Jamaat-ud-Dawa as a terrorist organization, in clear contrast to the Pakistani position. An examination of Chinese aid to Pakistan shows that the major portion is military, with only a small allotment to civilian needs. For example, after the destructive floods in 2010, China offered Pakistan the relatively modest sum of only \$100 million, as opposed to the \$500 million given by the US.

China's clear interest lies in maintaining the tension between India and Pakistan in order to impede India's growth and keep it from vying with China for regional hegemony. Therefore China might be expected to continue providing Pakistan with military aid, thereby preventing a disruption of the balance of power favoring India and an armed conflict between India and Pakistan. By contrast, leaders of the Pakistani regime are using the strategic alliance with China as a tool in negotiations with the US. About a week after the successful attack on Bin Laden, Prime Minister Gillani left for a visit to China and even declared in Pakistan's parliament that China is "an all-weather partner" – a dig clearly directly at Washington.<sup>24</sup>

## Conclusion

The alliance between the US and Pakistan, despite its complexity and vagaries, is quite firm and founded on mutual interests. The sense among Pakistan's political leaders is that the US abandoned Pakistan when the Soviet occupation of Afghanistan came to its end in the late 1980s, and has since then preferred India, and that it was only the events of September 2001 that led to a renewal of close relations. Not only do the Pakistanis enjoy economic and military assistance, but the close relations that the US has with India are used by Pakistan as leverage, and Pakistan has rejected American requests to embark on an offensive in FATA on the spurious

claim that most of Pakistan's ORBAT is needed for routine security on the Indian border. The Pakistanis are thereby trying to make the US persuade India to reduce its military presence on its western border.

For their part, the Americans see Pakistan as a critical partner in stabilizing Afghanistan and an important element in the war on terrorism inside Pakistan. The geostrategic considerations of the US, which views Pakistan as a nuclear state with a key role in maintaining regional stability, together with Pakistani signals about its intentions to forge closer relations with China as a possible alternative to its current pro-Western orientation, are encouraging the American administration to avoid taking extreme steps against Islamabad.

In recent months both the US and Pakistan have expressed their displeasure with one another and taken actual steps to convey this displeasure, and so, in addition to the declarations by Obama and Clinton, American security officials have openly begun to criticize Pakistani conduct. CIA Deputy Director Michael Morell went furthest: in a closed conversation he gave a low grade to Pakistan's security services. The US has also taken a relatively extreme measure by freezing \$800 million in military aid, out of the \$2.7 billion package planned for 2011. For their part, twice in the last six months the Pakistanis revealed the names of two CIA station chiefs in Islamabad (thereby forcing their replacement) and arrested locals who helped the CIA target Bin Laden, as part of a propaganda campaign aimed at highlighting America's infringement of Pakistan's sovereignty. In addition, Pakistan has severely cut back its joint routine security activity with the US, and has made it increasingly difficult for American military and CIA personnel to obtain entrance visas.

Nevertheless, the two countries have avoided crossing the line and causing irreversible damage to relations. Both nations have a vested interest in maintaining correct relations: thanks to its pro-Western stance, Pakistan, with its difficult economic situation, has enjoyed generous American aid, both economic and security-military, for a total of \$20 billion since 2002. The end or reduction of this assistance could have severe ramifications for the local economy, paralyze state institutions, and worst of all, push Pakistan into China's waiting arms. Pakistan is also confronting a complex internal security challenge and finds itself in an ongoing conflict with India, which it sees as a constant threat. Pakistanis are well aware of the cost of a potential rift in relations with the US, which could play into India's hands,

and this serves to spur Pakistan into maintaining its special relations with the US and accepting the US presence as a balancing element in the region. In addition, despite the negative aspects in Pakistani policy and popular hatred of the US, Pakistan is seen as holding the leading cards in the war on terrorism, earned through extensive military action that cost many Pakistani lives, military and civilian alike. Pakistan is a problematic ally but it cannot be presented as an entity that collaborates with the enemies of the West and tricks the US solely out of pecuniary motives, as it is sometimes described by Western analysts. Its achievements are particularly striking in light of the nation's internal instability, the struggle between secular, liberal trends and Islamic religious radicalization, and the unresolved conflict with India, which translates into a primal fear and a celebration of the military.

In light of Pakistan's centrality in the war on terrorism, the US drive to stabilize Afghanistan, and the host of thorns in US-Pakistan relations, the American administration is now facing two major alternatives. One alternative is to cut off aid to Pakistan and abandon it and its democratic regime, which in practice would allow radical Islamic elements to take control of the nation and further destabilize the situation on the Indian and Afghani borders. The second alternative is to take advantage of the crisis to strengthen relations by nurturing Pakistan's security services, improving its commitment to the war on terrorism, and strengthening the nation's democratic political institutions, while understanding that from time to time Pakistan will continue to play both sides. The latter alternative would allow the US to maintain a critical hold in this key region of central Asia, which has become a locus of activity against radical Islamic terrorism challenging the Western way of life.

Despite conflicts of interest in certain realms, one may expect that America's ambitions in the region will encourage the US to opt for the second alternative. It is almost certain that contradictory statements, secret military cooperation, and much mutual and open criticism will continue to characterize the conduct of both nations. However, despite the many ups and downs in the complex US-Pakistan relations, it seems that the nations' profound shared interests and the desire of both to survive serve the two nations more deeply and extensively than would a dismantling of the alliance between them.

## Notes

- 1 The Haqqani network was part of the mujahideen who fought the Soviet occupation in the 1980s. The founder of the network was Jajaluddin Haqqani who served as a minister in the Taliban government. Today the network is considered the most dangerous armed element facing Western forces in eastern Afghanistan. In addition to its terrorist activities against Western forces, including NATO and US forces, the network has extensive links with armed militias such as al-Qaeda and the Taliban, and it provides those organizations with safe haven. Jason Ukman, "The Haqqani Network: Al-Qaeda's Dangerous Patron," *Washington Post*, July 7, 2011, [http://www.washingtonpost.com/blogs/checkpoint-washington/post/al-qaedas-dangerous-haqqani-patron-in-pakistan/2011/07/18/gIQAAtWmcLI\\_blog.html](http://www.washingtonpost.com/blogs/checkpoint-washington/post/al-qaedas-dangerous-haqqani-patron-in-pakistan/2011/07/18/gIQAAtWmcLI_blog.html).
- 2 "Clinton Presses Pakistan to Broker Talks with Afghan Insurgents," *Los Angeles Times*, October 21, 2011, [http://latimesblogs.latimes.com/world\\_now/2011/10/us-pakistan-afghanistan-haqqani-militants.html](http://latimesblogs.latimes.com/world_now/2011/10/us-pakistan-afghanistan-haqqani-militants.html).
- 3 David E. Sanger and Eric Schmitt, "As Rift Deepens, Kerry Has a Warning for Pakistan," *New York Times*, May 14, 2011, [http://www.nytimes.com/2011/05/15/us/politics/15diplo.html?\\_r=2](http://www.nytimes.com/2011/05/15/us/politics/15diplo.html?_r=2).
- 4 Thomas Joscelyn, "Admiral Mullen: Pakistani ISI Sponsoring Haqqani Attacks," *The Long War Journal*, September 22, 2011, [http://www.longwarjournal.org/archives/2011/09/admiral\\_mullen\\_pakis.php](http://www.longwarjournal.org/archives/2011/09/admiral_mullen_pakis.php); Reuters, "Pakistan Warns U.S.: 'You Will Lose an Ally,'" *New York Times*, September 23, 2011, <http://www.nytimes.com/reuters/2011/09/22/world/asia/news-us-pakistan-usa.html>; Anwar Iqbal, "White House Refuses to Endorse Mullen's Claims," *DAWN.com*, September 29, 2011, <http://www.dawn.com/2011/09/29/white-house-refuses-to-endorse-mullens-claims.html>.
- 5 Rob Crilly, "Pakistan Claims Victory over US Haqqani Spat," *The Telegraph*, October 3, 2011, <http://www.telegraph.co.uk/news/worldnews/asia/pakistan/8804227/Pakistan-claims-victory-over-US-Haqqani-spat.html>.
- 6 AFP, "Pak-US Ties Thawing: Gilani," *Tribune*, October 5, 2011, <http://tribune.com.pk/story/267693/pak-us-ties-thawing-gilani/-APP>; "Pak-US Relations should Go beyond Counter-terrorism: PM," *DAWN.com*, October 13, 2011, <http://www.dawn.com/2011/10/13/pak-us-relations-should-go-beyond-counter-terrorism-pm.html>.
- 7 Rick Gladstone, "Obama Warns Pakistanis on Militants," *New York Times*, October 6, 2011, <http://www.nytimes.com/2011/10/07/world/asia/obama-obliquely-warns-pakistan-about-long-term-relations.html>.
- 8 Omar Waraich, "Taseer Murder Reveals Depth of Pakistan's Extremist Drift," *Time*, January 10, 2011, <http://www.time.com/time/world/article/0,8599,2041558,00.html>; Raja Menon, "Pakistan Futures," Atlantic Council, January 11, 2011, [http://www.acus.org/new\\_atlanticist/pakistan-](http://www.acus.org/new_atlanticist/pakistan-)



- futures; International Institute for Strategic Studies, "South Asia still Beset by Violent Extremism," <http://www.iiss.org/publications/strategic-comments/past-issues/volume-17-2011/january/south-asia-still-beset-by-violent-extremism/>.
- 9 "1979: Deposed Pakistani PM is Executed," *BBC*, [http://news.bbc.co.uk/onthisday/hi/dates/stories/april/4/newsid\\_2459000/2459507.stm](http://news.bbc.co.uk/onthisday/hi/dates/stories/april/4/newsid_2459000/2459507.stm).
  - 10 "Pakistan: Benazir Bhutto Murdered in a Suicide Attack," *Ynet*, December 27, 2007, <http://www.ynet.co.il/articles/0,7340,L-3487400,00.html>.
  - 11 Killed in an American drone attack in 2009; "Taliban Film Shows Leader is Dead," *BBC*, September 30, 2009, [http://news.bbc.co.uk/2/hi/south\\_asia/8282174.stm](http://news.bbc.co.uk/2/hi/south_asia/8282174.stm).
  - 12 Jayshree Bajoria, "Pakistan's New Generation of Terrorists," Council on Foreign Relations, May 13, 2011, [http://www.cfr.org/pakistan/pakistans-new-generation-terrorists/p15422?breadcrumb=%2Fbios%2F13611%2Fjays\\_hree\\_bajoria%3Fgroupby%3D1%26hide%3D1%26id%3D13611%26filter%3D456](http://www.cfr.org/pakistan/pakistans-new-generation-terrorists/p15422?breadcrumb=%2Fbios%2F13611%2Fjays_hree_bajoria%3Fgroupby%3D1%26hide%3D1%26id%3D13611%26filter%3D456).
  - 13 Ed Husain, "Explaining the Salman Taseer Murder," Council on Foreign Relations, January 7, 2011, [http://www.cfr.org/publication/23755/explaining\\_the\\_salman\\_taseer\\_murder.html?cid=rss-fullfeed-explaining\\_the\\_salman\\_taseer\\_m-010711&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+cfr\\_main+%28CFR.org+-Main+Site+Feed%29](http://www.cfr.org/publication/23755/explaining_the_salman_taseer_murder.html?cid=rss-fullfeed-explaining_the_salman_taseer_m-010711&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+cfr_main+%28CFR.org+-Main+Site+Feed%29).
  - 14 Menon, "Pakistan Futures."
  - 15 "India-Pakistan Troubled Relations – Timeline," *BBC*, [http://news.bbc.co.uk/hi/english/static/in\\_depth/south\\_asia/2002/india\\_pakistan/timeline/1998.stm](http://news.bbc.co.uk/hi/english/static/in_depth/south_asia/2002/india_pakistan/timeline/1998.stm).
  - 16 For the sake of comparison, India's military budget is equal to Pakistan's entire national budget. Menon, "Pakistan Futures."
  - 17 Jayshree Bajoria and Eben Kaplan, "The ISI and Terrorism: Behind the Accusations," May 4, 2011, Council on Foreign Relations, <http://www.cfr.org/pakistan/isi-terrorism-behind-accusations/p11644>.
  - 18 In late July 2011, *Asia Times* speculated that Kashmiri faked his own death in order to make it easier for himself to avoid American intelligence. Amir Mir, "Kashmiri's Great Escape (Reprise)," *Asia Times*, July 22, 2011, [http://www.atimes.com/atimes/South\\_Asia/MG22Df04.html](http://www.atimes.com/atimes/South_Asia/MG22Df04.html).
  - 19 Jane Perlez "Mystery over Detained American Angers Pakistan," *New York Times*, February 8, 2011, <http://www.nytimes.com/2011/02/09/world/asia/09pakistan.html>; "Pakistan's Intelligence Ready to Split with CIA," *China Daily*, February 24, 2011, <http://www.webcitation.org/5xtOcem4M>.
  - 20 "U.S.: Pakistan Making Little Progress on Insurgents," *Fox News*, April 6, 2011, <http://www.foxnews.com/politics/2011/04/06/pakistan-making-little-progress-insurgents/>.
  - 21 Howard L. Berman and John F. Kerry, "Joint Explanatory Statement, Enhanced Partnership with Pakistan Act of 2009," October 14, 2009, <http://>



- [www.cfr.org/pakistan/joint-explanatory-statement-enhanced-partnership-pakistan-act-2009/p20422](http://www.cfr.org/pakistan/joint-explanatory-statement-enhanced-partnership-pakistan-act-2009/p20422).
- 22 Laurie Ure, "Kerry, Lugar Defend Pakistan Aid," *CNN*, May 5, 2011, [http://articles.cnn.com/2011-05-05/politics/kerry.lugar.pakistan\\_1\\_pakistan-aid-india-and-pakistan-samina-ahmed?\\_s=PM:POLITICS](http://articles.cnn.com/2011-05-05/politics/kerry.lugar.pakistan_1_pakistan-aid-india-and-pakistan-samina-ahmed?_s=PM:POLITICS).
- 23 Robert D. McFadden, "Strong American Voice in Diplomacy and Crisis," December 13, 2010, <http://www.nytimes.com/2010/12/14/world/14holbrooke.html?ref=world&pagewanted=all>.
- 24 Karen de Young, "New Estimates Put Pakistan's Nuclear Arsenal at More than 100"; see <http://www.washingtonpost.com/wp-dyn/content/article/2011/01/30/AR2011013004136.html?hpid=topnews>.



# Fighting against Irregular Forces: Afghanistan as a Test Case

Tal Tovy

America's involvement in Afghanistan since late 2001 (Operation Enduring Freedom) is an excellent example of the highly problematic nature of fighting against irregular forces in a state with a long history of instability.<sup>1</sup> From Afghanistan's perspective, the American involvement represents yet another stage in the country's lack of stability, ongoing since the late 1970s.<sup>2</sup> In this sense, the fall of the Taliban regime, rather than a watershed, was another link in Afghanistan's checkered history.

This essay analyzes the factors behind Afghanistan's instability and argues that understanding them can explain the political and military difficulty in destroying irregular forces that share a strong ideology and operate in a given geographical arena. This essay does not purport to offer solutions or recommendations for action; rather, it claims that the primary and most basic action a state must undertake when embarking on a confrontation with irregular forces in a given geographical setting is to understand the history of the region. Such an understanding will allow it to assess how local history has created a political, social, and economic system that is a convenient base for a guerrilla activity grounded in a firm ideological base. The essay claims that understanding the area politically, socially, and demographically allows for the formulation of a strategy and varied *modi operandi* for defeating the guerrilla forces.<sup>3</sup>

The essay concentrates on the period between 1978 and 2010. During this time, Afghanistan's instability grew from an internal phenomenon, or at most a limited regional issue, to an international one that entailed the involvement of various powers that offered assistance to the warring sides.

Dr. Tal Tovy is a lecturer in military history in the History Department at Bar-Ilan University.

During these years, guerrilla forces enjoyed external support and fought against regular forces; their overall objective was toppling the existing regime and replacing it with one that would be based on the guerrillas' own political framework. For example, in the early stages of Operation Enduring Freedom, responsibility for most of the fighting was in the hands of the militias that comprised the Northern Alliance, backed by massive aerial assistance and tight cooperation with small US special forces and CIA teams.

The scope of this essay does not allow an in-depth examination of the history of Afghanistan and the factors behind the country's instability. Clearly, however, modern Afghani history is marked by stubborn resistance to both foreign occupation and a central government. Furthermore, the common denominator of all struggles in Afghanistan since 1979 is that while regular armies have succeeded to one degree or another in wresting control of central traffic arteries, control of the rural areas has remained entirely in the hands of armed guerrilla groups and militias that have over the entire period received assistance from a third party power. In other words, in the last 30 years, no central government in Afghanistan has ever managed to establish its authority over the whole country.<sup>4</sup>

### **Puncturing the Guerilla Forces' Supportive Environment**

A study of campaigns waged against irregular forces points to five fundamental elements intrinsic to a guerrilla movement's success. Accordingly, the absence of some of these elements may spell failure for the movement. The five elements are: (a) a weak central government; (b) ineffective security forces; (c) external assistance; (d) safe havens for guerrillas; and (e) support of the civilian populace. These elements derive from each other, operate in tandem at different levels of intensity, and affect and in turn are affected by one another.

How are these elements manifested in Afghanistan?

At no time have the rulers of modern Afghanistan managed to establish total control over the mosaic of ethnic minorities, especially the Pashtun tribes, which represent one of the major loci of resistance to any central government in the country.<sup>5</sup> Although throughout most of Afghanistan's history the country was controlled by foreign powers, the actual power always lay with the tribal leaderships, and the state never came under full colonial rule.<sup>6</sup> Accordingly, the basic loyalty of Afghans is to their

tribe of origin and their tribal familial and blood relations; in this they are no different from other tribal village societies in the Third World. These societies, including in Afghanistan, never experienced the development of a solid Western-style defined nationalism, and with it absolute loyalty to a central government.

Since no central Afghani government has ever managed to win the loyalty of all ranks of Afghani society and earn comprehensive legitimacy, no government has been able to gain a monopoly on the use of force or on law and order enforcement at the national level. The political instability and lack of governmental confidence have strengthened the tribal militias, which have seen to the security of their peoples; this in turn has further damaged the legitimacy of the central government.<sup>7</sup>

Any desire to reach a political solution in Afghanistan must understand the tribal and political structure of Afghani society, because no settlement is possible without the tribal groups as partners. The major problem for the USSR in Afghanistan in the 1980s was the attempt to impose Communist rule without understanding the complexity of Afghani society and the particular political tendencies of the different ethnic groups in the country.<sup>8</sup> Understanding the tribal structure and the political tendencies of each ethnic/tribal group is the key to attaining political stability in Afghanistan. The recognition that Afghani society is not homogeneous and that each group has its own particular socioeconomic and political features enables the creation of a plan of action relevant for each group.<sup>9</sup> For example, it may be that with regard to the Pashtuns, it is necessary to implement more civilian programs, whereas for the foreign fighting groups that are not part of the country's basic society it is necessary to stress the military dimension.<sup>10</sup>

The elements of internal instability in Afghanistan are compounded by another highly influential factor: external assistance and involvement by foreign powers. External intervention is first and foremost a function of Afghanistan's geostrategic location in Central Asia<sup>11</sup> and the massive foreign aid that has been channeled there over the last 30 years, allowing the various guerrilla groups to operate. So, for example, US aid to the mujahideen during the war against the Soviet Union, estimated at \$5 billion, enabled the guerrillas to continue fighting much longer and was one of the causes of Afghanistan's ongoing instability.<sup>12</sup> After the withdrawal of the USSR and the renewal of the civil war in Afghanistan, the Taliban

received economic and military assistance from Pakistan and Islamic movements all over the world,<sup>13</sup> while Shiite tribes in western Afghanistan, which fought the Sunni Taliban regime in the second half of the 1990s, were assisted by Iran.

The foreign aid that was funneled into Afghanistan was meant to weaken the government and prompt the creation of a new government aligned with the interests of the intervening parties. The pattern was as follows: when the Kabul government would fall, a new government that did not enjoy national support and consensus would be created. It would usually operate against the interests of some foreign power or another, which would then start assisting irregular forces opposed to that central government. So, for example, the US funded the mujahideen, a composite of tribal Islamic militias without a uniform political or military system. This group spawned the Taliban, which adopted a policy opposed to American interests. As a result, the US began funding a group of a different tribal-ethnic composition – the Northern Alliance.

Safe havens for guerrillas and the support of the local populace are two conditions necessary for further erosion of the central government and damage to its ability to impose its authority. Throughout history these conditions have constituted the foundation for the successful operation of any irregular force. Military theoreticians such as Carl von Clausewitz and Thomas Edward Lawrence long ago pointed out the advantages of using irregular forces and stressed that these forces need to operate within a sympathetic civilian environment. Their writings emerged from a military reality in which decisions were achieved by regular armies.<sup>14</sup>

It was Mao Zedong who elevated guerrilla fighting to the strategic and political levels and whose writings set forth the process necessary for converting guerrillas from an irregular force to a political system with a regular army. In his book *On Guerrilla Warfare* (1937), he contends that it is necessary to wrest control of a certain area (base of operations) and convince the local population to support the goals of the political movement. The movement gradually expands its areas of control and influence while widening its popular base. In Mao's thinking, the safe haven and the base are the same geographical region; China's vast size allows a political movement to find a hideout far from the reach of the government and its military (its safe haven).<sup>15</sup>

Practitioners of Mao's philosophy who operated in smaller geographical regions than Mao himself, such as Vo Nguyen Giap, adapted Mao's teachings to their smaller expanses and separated their bases from their safe havens. "Bases" remained the areas in which it was necessary to gain the support of the local population and convince it of the revolutionary ideology in question on the way to taking control of the country.<sup>16</sup> "Safe havens" were regions with a geographical character that were hard for the central government to access and attack the guerrillas there. In the safe haven guerrillas can find shelter and train, regroup, and plan their next steps. The difficulties may stem from harsh topographical conditions, such as the Hindu Kush mountain range in northeast Afghanistan, but usually the safe haven is a country near the base area where those fighting the guerrilla forces cannot operate freely or at all. Thus the Vietcong found safe haven in Laos and Cambodia, and the FLN guerrillas found safe haven in Tunisia. The Taliban uses Pakistan as its safe haven and even gets help from elements within the Pakistani government as well as assistance from the local population of Afghani refugees.<sup>17</sup> The Pakistani regions adjacent to the Afghani border also serve as a base of sorts because there are many Afghani refugees who could join in the military efforts; similarly, the regions are home to Pashtuns who do not recognize the international border and have blood and familial ties to the Taliban fighters.

## The Historical and Theoretical Record

What, then, are the ways to confront the complex reality facing the United States and its allies in Afghanistan, and facing any nation or regular army – including Israel – trying to fight irregular forces?

One of the most interesting aspects of the American confrontation with the Afghani challenge is the return to the study of theories written in the 1950s and 1960s about methods of operation against guerrillas, or counterinsurgency (COIN), as well as a relearning of the lessons from the wars fought by France (in Indochina and Algeria), Great Britain (in Malaya and Kenya), and the United States (in the Philippines and Vietnam). The American field guide dealing with counterinsurgency declares that only a learning organization can be effective with regard to COIN, and that one of the ways of developing such knowledge is studying the wars of the past.<sup>18</sup>

This approach is not unusual for the US Army. As early as the Vietnam War, it commissioned a number of studies dealing with the British

experience in Malaya, which it viewed as a successful attempt to suppress the Communist revolution there.<sup>19</sup> The most telling evidence of the fact that the Americans sought to learn from the British experience was the stationing of Sir Robert Thompson as a senior advisor to the US Army in Vietnam (1961-65) in order to implement the pacification programs that had proven their efficacy in Malaya.<sup>20</sup> The United States also studied the French failures in Vietnam and Algeria, in order to understand the errors of the French and avoid repeating them.<sup>21</sup> At the same time, French literature dealing with the lessons learned from the confrontations in Vietnam and Algeria, such as the book by Roger Trinquier, an experienced French officer who had served in Indochina and Algeria, was translated into English.<sup>22</sup> Trinquier's book is still considered one of the most important theoretical works in the field of COIN.

In the United States, alongside writing about COIN theory and practice, much research was published on the phenomenon of insurgency itself, with an emphasis on Mao Zedong's military philosophy and analysis of guerrilla warfare in Southeast Asia. Likewise, many essays discussing the topic were published in American army periodicals.<sup>23</sup> David Galula's book, published in 1964, represented one of the first systematic discussions of the ways to defeat guerrilla.<sup>24</sup> Analyzing a number of test cases and relying on personal experience as an advisor in China and an officer in Algeria, Galula lays out the strategy and tactics for successful COIN management. His key points are the need for total destruction of the revolutionary organization's political force and the need to gain the support of the civilian population, or at least deny it to the guerrillas or rebels.<sup>25</sup> Another important book on the topic is by Robert Thompson, who summarizes his experience in Malaya and Vietnam while noting the differences between the two confrontations. Thompson also deals with the political action the government must take in order to eliminate the revolutionary guerrilla.<sup>26</sup>

Galula's and Thompson's books may be classified as military philosophy based on operational experience. These books join the ranks of studies dealing with the phenomenon of guerrilla and the ways to fight it.<sup>27</sup> The American field guide on counterinsurgency, quoting Galula and Thompson, is evidence of the importance and relevance of the theories formulated in the 1960s and strengthens the thesis of this essay that it is possible to extract lessons for contemporary confrontations by means of historical analyses.<sup>28</sup>



After the Vietnam War, the US Army focused on reconstructing its force with a view to a future war with Warsaw Pact forces in central Europe and abandoned the preoccupation with COIN theory. A significant change in this trend occurred only after the end of the conventional stages of America's war in Afghanistan and Iraq during 2003. Since then there has been a revival of writing about COIN in military periodicals as well as in military doctrine. For example, *Military Review* published two special editions (in 2006 and 2008) devoted to both historical and contemporary essays published since 2004 on the topic of COIN.<sup>29</sup> Another important publication, by the History Department of the US Army, is a study dealing with America's experience with COIN in its broader definition from late World War II until the end of the Vietnam War.<sup>30</sup> This is further evidence of the American precept that studying the past is critical for understanding the present and creating *modi operandi* to deal with it. The latter source joins a series of theoretical and historical works prepared by the RAND Corporation for the US Department of Defense, all dealing with different aspects of COIN and the lessons that may be learned from various COIN campaigns, including Vietnam, and adapting them to contemporary reality.<sup>31</sup>

The United States Army currently operates in Afghanistan according to procedures derived from COIN theories, especially with regard to strengthening government forces and gaining the support of the civilian population. These activities are carried out on two parallel levels: the first is an attempt to bring about both social and economic improvements in the population's standard of living, by rebuilding medical and health systems, investing in infrastructures, and providing assistance in agriculture; the second is constructing and strengthening the security forces (including their intelligence capabilities) to allow for confrontations with the guerrilla forces without external aid. Until these two processes are complete, the American army will continue with its routine military activities against Taliban and al-Qaeda forces, with occasional forays by coalition forces on large operations in the areas considered the Taliban's strongholds.

## Conclusion

The history of Afghanistan since the 1980s demonstrates that the five elements listed above have helped – and continue to help – guerrilla groups operate effectively and damage the central government's ability to impose

its authority and attain political legitimacy in the country. The Taliban government (1995-2001) did not manage to control all of Afghanistan, the United States used the Northern Alliance as the opposition to topple the regime, and the new Afghani government has not yet established its rule over the whole country, especially in light of the renewed guerrilla efforts of the Taliban, which still enjoys the support of some of the local population as well as the safe haven located in Pakistan. As long as American forces operate in Afghanistan, the Taliban is clearly incapable of regaining its control of the government. However, should the United States leave Afghanistan before the country is politically and economically stable, the country will likely be drawn into a civil war once again, as was the case after the USSR withdrawal.

These five elements are relevant to the attempt to examine contemporary instances of a regular army confronting a guerrilla force. They represent a nexus that makes it very difficult to battle irregular forces united by a solid, clear ideology. Since the five derive from one another, eliminating one will perforce bring about the collapse, albeit not immediate, of the entire system that allows guerrillas to operate in a given arena.

An historical debate, relevant to this day, exists between two schools of thought about the ways to defeat guerrillas that are descended from or influenced by the political-military thought of Mao Zedong. One school of thought emphasizes the application of military force, whereas the other school of thought focuses on operating civilian programs, i.e., programs that will improve the socioeconomic situation of the population in the fields of education, healthcare, employment, agriculture, and so on, while improvements in security will be effected by continuing the fight against the guerrillas' military and political power. This debate was conducted in the United States before and during the war in Vietnam. Simplistically, one could say that the most effective way to fight a guerrilla movement with a firm ideological base is with a formula that stresses the civilian operations alongside the continuation of military operations.

The reasons for the instability in Afghanistan demand that most of the attention be focused on attaining legitimacy for the central government. This may be done by improving the internal security system and the socioeconomic situation of the various tribespeople in the country. Such improvements, which would be based on understanding the local centers of power and traditions, would generate the central government's gradual

acquisition of legitimacy. Such a mode of operation was undertaken in Malaya, Kenya, and the Philippines, where the gradual strengthening of the central government and consolidating popular legitimacy finally defeated the guerrilla. While it is impossible to project exactly this or any other historical example onto a contemporary reality, it is important to study the principles and examine which of them remain relevant, which methods need adjustment, and which operations are completely irrelevant.

The study of Afghanistan as a test case for regular forces waging warfare against guerrillas can be instructive in a number of ways, some of which are relevant also for Israel, especially in Judea and Samaria.<sup>32</sup> First, it is necessary to understand the history and culture of the specific region. Such understanding will facilitate the creation of relevant *modi operandi* for a given society, while giving attention to the special problems of that society. Second, it is necessary to identify the center of gravity of the enemy and operate against it. Although anti-guerrilla warfare entails fighting irregular forces, it is important to remember that such forces also have their strategic weaknesses. From an analysis of Mao's writings and a study of Afghanistan's history it is possible to identify two points representing the guerrilla's/terrorists' center of gravity: the civilian population and the bases or safe havens. Therefore, it is necessary to concentrate a significant portion of the effort on severing the link between the civilian population and the guerrillas.

Indeed, it would be a mistake to focus on the military aspect alone. Fundamentalist Islam, similar to Communist guerrillas, stems from an ideology with political, social, and economic potency. Such ideologies have always succeeded in attracting thousands of active supporters – the fighters; but they have also mobilized millions of passive supporters – the civilian population. It is impossible to eliminate the thousands of fighters, because new fighters are recruited all the time from the ranks of the millions. Therefore, it is necessary to damage the bridge that links the two groups: military operations, both defensive and offensive, must not be abandoned, but most of the effort must be centered on the civilian and political front. Severing the population from the guerrillas is possible by presenting political alternatives that will generate direct improvement to that society's socioeconomic reality. This is not an easy task, but the various examples from history demonstrate that it is possible.

## Notes

- 1 For a discussion of the historical components that shaped modern day Afghanistan, see Larry P. Goodson, *Afghanistan's Endless War: State Failure, Regional Politics, and the Rise of the Taliban* (Seattle: University of Washington Press, 2001), pp. 23-53.
- 2 C. Christine Fair, "Insurgency, Instability and the Security of Afghanistan," in Sumit Ganguly, Andrew Scobell, and Joseph Liow, eds., *Handbook of Asian Security Studies* (London: Routledge, 2010), p. 186.
- 3 As was the case in Malaya, Kenya and the Philippines in the 1950s. See Tal Tovy, *Like Eating Soup with a Knife* (Tel Aviv, 2006), pp. 54-65; and Tal Tovy, *Guerrilla and the War Against It* (Jerusalem, 2010), pp. 130-54.
- 4 For a discussion of the reasons for the weakness of the Afghani regime, see Antonio Giustozzi, *Koran, Kalashnikov and Laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007* (New York: Columbia University Press, 2008), pp. 15-20.
- 5 For a survey of the ethnic fabric of Afghanistan, see Ralph H. Magnus and Eden Naby, *Afghanistan: Mullah, Marx and Mujahid* (Oxford: Westview, 2002), pp. 11-15; Martin Ewans, *Conflict in Afghanistan: Studies in Asymmetric Warfare* (London: Routledge), 2005, pp. 11-14; Deepali Gaur Singh, *Afghanistan: Challenges and Opportunities*, vol. 3 (New Delhi: Pentagon Press, 2007), pp. 34-40. For ethnic diversity as a destabilizing factor in Afghanistan, see Amalendu Misra, *Afghanistan: The Labyrinth of Violence* (Cambridge: Polity Press, 2004), pp. 41-60; Burchard Brentjes and Helga Brentjes, *Taliban: A Shadow over Afghanistan* (Varanasi, India: Rishi Publications, 2000), pp. 40-48.
- 6 Ewans, *Conflict in Afghanistan*, p. 173.
- 7 Antonio Giustozzi, *War, Politics and Society in Afghanistan* (London: C. Hurst & Co., 2000), pp. 207-12. For more on the armed militias operating in Afghanistan, see Seth G. Jones, *Counterinsurgency in Afghanistan* (Santa Monica: RAND, 2008), pp. 37-48.
- 8 Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2004), pp. 155-69.
- 9 For the political trends derived from the changing economic conditions, see Manmath N. Singh, "Ethnicity and Politics in Afghanistan," in K. Warikoo, ed., *Afghanistan: Challenges and Opportunities*, vol. 1 (New Delhi: Pentagon Press, 2007), pp. 33-42. In this context and as part of the discussion of the study of history for the sake of understanding reality, see also the 1927 anthropological study by Sirdar Ikbali Shah, a British diplomat of Indian ancestry, which describes the political problems of the British in Afghanistan that stem, inter alia, from the complexity and great heterogeneity of Afghani society. See Sirdar Ikbali Shah, *Afghanistan of the Afghans* (New Delhi: Bhvana Books, 2000), pp. 9-18.

- 10 The political reality in Iraq should also be analyzed on the basis of this model: the ethnic composition, although less complex than that of Afghanistan, and the armed militias there preclude political and social stability. See Bruce R. Pirnie and Edward O'Connell, *Counterinsurgency in Iraq 2003-2006* (Santa Monica: RAND, 2008), pp. 22-32.
- 11 Brentjes and Brentjes, *Taliban*, pp. 49-67; Goodson, *Afghanistan's Endless War*, pp. 133-66; Misra, *Afghanistan*, pp. 13-20.
- 12 Thomas Powers, *Intelligence Wars: American Secret History from Hitler to al-Qaeda* (New York: New York Review of Books, 2002), pp. 285-88.
- 13 Pakistan's involvement was – and continues to be – the result of its refusal to recognize Afghanistan as a sovereign state within the borders determined by the British in the late nineteenth century. Likewise, Pakistan has ambitions of becoming a major political factor in Central Asia. For more on this, see Amin Saikal, *Modern Afghanistan: A History of Struggle and Survival* (London: I. B. Tauris, 2004), pp. 219-25; Angelo Rasanayagan, *Afghanistan: A Modern History* (London: I. B. Tauris, 2005), pp. 177-90.
- 14 Clausewitz deals with the guerrilla phenomenon in Book 6 (“Defense”), chapter 26. See also Werner Hahlweg, “Clausewitz and Guerrilla Warfare,” in Michael I. Handel, ed., *Clausewitz and Modern Strategy* (London: Frank Cass, 1986), pp. 130-32.
- 15 For a discussion of Mao's revolutionary guerrilla philosophy, see Tovy, *Guerrilla and the War against It*, pp. 42-57. For Mao's influence on the mujahideen, see Barnett R. Rubin, *The Fragmentation of Afghanistan* (New Haven: Yale University Press, 2002), pp. 78-79.
- 16 For the meaning of the concept “safe haven” in the Afghani context, see Abdulkader H. Simmo, *Organization at War in Afghanistan and Beyond* (Ithaca: Cornell University Press, 2008), pp. 13-16.
- 17 Giustozzi, *Koran, Kalashnikov and Laptop*, pp. 99-102.
- 18 Department of the Army, FM 3-24: *Counterinsurgency*, 2006, pp. 1-26. See also the theoretical overview in John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: University of Chicago Press, 2002), pp. 3-11.
- 19 Riley Sunderland, *Antiguerrilla Intelligence in Malaya, 1948-1960* (Santa Monica: RAND, 1964); Riley Sunderland, *Winning the Hearts and Minds of the People: Malaya, 1948-1960* (Santa Monica: RAND, 1964); P. B. G. Waller, *The Evolution of Successful Counterinsurgency Operations in Malaya* (Menlo Park, CA: RAND, 1968).
- 20 Spencer C. Tucker, *Vietnam* (Lexington: University Press of Kentucky, 1999), p. 96; Douglas S. Blaufarb, *The Counterinsurgency Era: U.S. Doctrine and Performance* (New York: Free Press, 1977), pp. 47- 51; Rowland S. N. Mans, “Victory in Malaya,” in: T. N. Greene, ed., *The Guerrilla and How to Fight Him* (New York: Praeger, 1962), pp. 115-43.
- 21 See Paul A. Jureidini, *Case Studies in Insurgency and Revolutionary Warfare: Algeria 1954-1962* (Washington, D.C.: American University, 1963);

- Constantin Melnik, *The French Campaign against the FLN* (Santa Monica: RAND, 1967).
- 22 See. J. Croizat, *A Translation from the French: Lessons of the War in Indochina* (Santa Monica: RAND, 1967); Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (New York: Praeger Security International, 1964; the book was published in France in 1961).
  - 23 During the 1960s a selection of Communist literature presenting Mao's revolutionary strategy and its impact, especially on the confrontation in Vietnam, was translated into English. For example, in 1968 an anthology was put together that compiled a range of Communist writings about revolutionary guerrilla wars. See William J. Pomeroy, ed., *Guerrilla Warfare and Marxism* (New York: International Publishers, 1968). The military writings of Communist thinkers were required reading for US Military Academy cadets. See Andrew J. Birtle, *U.S. Army Counterinsurgency and Contingency Operations Doctrine 1942-1976* (Washington, D.C.: Defense Dept., Army, Center of Military History 2006), p. 261.
  - 24 David Galula, *Counter-Insurgency: Theory and Practice* (New York: Praeger Security International, 1964).
  - 25 *Ibid.*, pp. 107-35.
  - 26 Robert Thompson, *Defeating Communist Insurgency: Experiences from Malaya and Vietnam* (London: Palgrave Macmillan, 1966), pp. 51-58.
  - 27 See., e.g., Peter Paret and John Shy, *Guerrillas in the 1960s* (New York: Praeger, 1965); John S. Pustay, *Counterinsurgency Warfare* (London: Free Press, 1965); Abdul Haris Nasution, *Fundamentals of Guerrilla Warfare* (London: Pall Mall Press, 1965); John J. McCuen, *The Art of Counter-Revolutionary War: The Strategy of Counter-Insurgency* (London: Stackpole Books, 1966).
  - 28 Robert R. Tomes, "Relearning Counterinsurgency Warfare," *Parameters* 34, no. 1 (2004): 26.
  - 29 Of the dozens of essays published since 2004, one essay in particular stands out as demonstrating the importance of the theories developed in the 1960s for the military reality in Afghanistan: Dale Kuehl, "Testing Galula in Ameriyah: The People are the Key," *Military Review* 99, no. 2 (2009): 72-80.
  - 30 Birtle, *U.S. Army Counterinsurgency and Contingency Operations Doctrine*.
  - 31 Angel Rabasa et al, *Money in the Bank: Lessons Learned from Past Counterinsurgency (COIN) Operations* (Santa Monica: RAND, 2007); Daniel Byman, *Understanding Proto-Insurgencies* (Santa Monica: RAND, 2007); Austin Long, *Doctrine of Eternal Recurrence: The U.S. Military and Counterinsurgency Doctrine, 1960-1970 and 2003-2006* (Santa Monica: RAND), 2008. These studies are part of the RAND Counterinsurgency Study series.
  - 32 This model is irrelevant with regard to Hizbollah in Lebanon and Hamas in the Gaza Strip, as Israel has no permanent military presence in those areas.

# Critical Infrastructure Protection against Cyber Threats

Lior Tabansky

## Introduction

A functioning modern society depends on a complex tapestry of infrastructures: energy, communications, transportation, food, and many others. This article discusses the developing cyber threat to critical infrastructure while focusing on several dimensions: aspects to the threat that require an interdisciplinary approach; defense against the threat; the existing Israeli response; and the developing challenges. An informed public debate is likely to lead to improved protection of national infrastructures in the civilian and public sectors.<sup>1</sup>

The article begins by defining the subject of critical infrastructures, and discusses the origins, uniqueness, and innovativeness of the threat to them. It then discusses levels of coping with the threat, using conceptual parallels to the world of military content. The existing Israeli response will be reviewed briefly, with an emphasis on the central challenges the cyber threat poses to public policy. Finally, directions for future research and action will be presented.

## What are Critical Information Infrastructures

An infrastructure is a system that combines various facilities and enables certain activities, for example, a pipeline that conducts water from wells to homes and fields, paved roads, bridges and intersections that allow movement of people and goods, flight, communications, fuel, and health services. One of the properties of an infrastructure is the dependence of

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



various spheres of activity on it. In the past, the dependence stemmed from physical or geographical relationships only. With the development of cyberspace, which includes data communication systems and computerized methods of automatic command and control, there are additional relationships, which in turn create further vulnerability. These are computerized relationships (for example, command and control by remote electronic means) and logical relationships (such as the international financial market as a factor influencing inputs and outputs of critical infrastructures), which are innovations that would not exist without information technologies. It is therefore worth distinguishing between infrastructures in the traditional sense and the modern use of this concept, which includes a cyber dimension.

In the information age, traditional infrastructures become information infrastructures because they incorporate computers. In addition, new critical infrastructures have been created that are purely information infrastructures: computerized databases that contain important data, such as records of capital in the banking system, scientific and technical intellectual property, and the programmed logic that manages production processes and various business processes. In the information age, the concept of “infrastructure” also includes computerized components, and thus “infrastructure” today necessarily refers to an information infrastructure.

Infrastructure is defined as critical when it is believed that disrupting its function would lead to a significant socio-economic crisis with the potential to undermine the stability of a society and thereby cause political, strategic, and security consequences. Different countries have offered a variety of definitions of critical infrastructures.<sup>2</sup> What all have in common is the existence of a computerized element upon which other physical systems are dependent and which, if harmed, would likely cause widespread damage in physical terms.<sup>3</sup>

Three factors can define a critical infrastructure. The first is the symbolic importance of the infrastructure. Thus, several democratic countries include heritage sites, museums, archives, and monuments among critical infrastructures that should be protected from cyber threats.<sup>4</sup> Another source of symbolic power is the perceived control of a government. For example, a hostile disruption of traditional media used by the state for communicating with its citizens will immediately harm the government’s



ability to function. Moreover, in the longer term, such disruption may diminish the citizens' confidence in the existing government, or even the general form of government or regime.

The second factor is the immediate dependence on infrastructure, such as the electricity grid or telecommunications network, which is obvious for most processes in society. The emergence and prevalence of cyberspace created a situation in which computerized networks constitute an infrastructure in and of themselves. Cyberspace is a representative example of an infrastructure that has become critical because of the interface of most of society's activity with computerized communications networks.

The third factor involves complex dependencies. The accelerated trend toward adding connectivity capabilities enables unanticipated effects beyond the local level (the "butterfly effect").<sup>5</sup> The relationships among various infrastructures are presumably not fully known, and the failure of one component is liable to cause a wide range of results and damage. The types of failure fall into three classes:

- a. *Common cause failure.* For example, various facilities (fuel storage, airports, and power stations) that are located in geographic proximity are likely to be harmed from a single incident of flooding. It is hard to imagine a cyber attack that would directly cause a failure of this type.
- b. *Cascading failure.* Disruption of a control system in one infrastructure (for example, water) leads to disruption of a second infrastructure (for example, in transportation, the flooding of a railway line), and then a third (for example, food supply chain) and so on, even if it is not directly dependent on it. A cyber attack could directly cause such a failure.
- c. *Escalating failure.* Disruption of one infrastructure (for example, a communications network) harms the effort to fix other infrastructures that have been damaged by another entity (emergency services, commerce).<sup>6</sup> A cyber attack could directly cause this type of failure.

The commercial aviation sector, which has attracted the attention of enemies of the developed states and prompted noticeable acts of hostility – hijacking of commercial planes, the September 11 attacks, and other terrorist attacks using civilian airplanes – can illustrate the importance of critical infrastructures and the significance of an attack on them. Civil aviation is a basic infrastructure for developed societies: in 2009, commercial air transport carried more than 2 billion passengers on 28

million flights on 27,000 airplanes operating from 3,670 commercial airports around the world.<sup>7</sup> In addition to commercial flights, military aircraft (some unmanned) also populate the skies. Intra-state laws, regulations, and procedures, along with international cooperation, regulate the administrative aspect of the airline industry. Airports are connected to each other through scheduled air traffic, and the air traffic control system in each given location is part of the international aviation infrastructure. Air traffic control is based on computerized systems: methods of detection, monitoring, surveillance, automation, communications, command and control, and so on. Disrupting the proper functioning of air traffic control systems would harm all air traffic.

### **The Novelty of the Threat**

Recent years have brought increased concern over the potential vulnerability of the infrastructures that are the basis of developed modern societies,<sup>8</sup> yet the fact that this discussion is taking place now is surprising. Critical infrastructures have always been critical and their importance is obvious. International and internal conflicts are not new to the world, and in war it is reasonable to anticipate attempts to harm the adversary's critical infrastructures with the goal of weakening and defeating it. In 1917, during the Bolshevik Revolution, Lenin and Trotsky ordered their activists to take over the post office, telegraph systems, bridges, and train stations. In prolonged wars, such as the Second World War, attempts have been made to harm critical infrastructures in order to interfere with the enemy's fighting ability and spirit.<sup>9</sup> A country's critical infrastructures, whatever they are, are elemental targets during a conflict, and therefore organizations and states have labored throughout history over defense systems for their infrastructures: camouflage, guarding, fortification, defensive forces, deterrence, and so on. Why, then, is there a growing fear of damage to critical infrastructures, particularly in the strongest countries?<sup>10</sup>

A critical infrastructure is a tempting target for an enemy, be it a terrorist organization or a hostile state. However, the developed countries currently enjoy total military superiority over their respective enemies. The US and Europe have not experienced wars on their territories in recent decades. Israel is the only developed country that is under ongoing military threat that is manifested in a variety of ways (missile attacks in 1991, rockets in the north and south of the country,<sup>11</sup> and suicide bombers in 2000-

2005). Several developed countries have been harmed by hostile acts that directly attack the civilian population by circumventing the military that was supposed to protect it. The terrorist attacks could not threaten the countries attacked, but they did succeed in causing a change in their policy in one way or another.

In all forms of traditional warfare, the identity of the enemy is disclosed following the attack because in order for the attack to be carried out, the weapons must physically reach the target. In the event of a missile launch as well, there is no doubt as to the location of the launch site. The hijacking of commercial aircraft in the 1970s, the suicide bombings in Israeli population centers, the attacks in the United States in September 2001, and the attacks in Madrid in 2004 and London in 2005 all required the attackers to be physically present at of the attacks.

Identifying the enemy is critical for response and deterrence. Thus what prevented harm to critical infrastructures in the past was the defensive force placed in the path of the enemy, and even more so, the deterrence that promised to exact a heavy price. This familiar state of affairs came to an end with the development of cyberspace. For the first time in history, it is possible to attack strategic targets (such as critical infrastructures) without physically being in the place where they are located, without confronting defensive forces, and without exposure. In today's reality, the existing computerized infrastructure can be exploited through penetration of communications networks or the software or hardware of the command and control computers in order to disrupt, paralyze, or even physically destroy a critical system.<sup>12</sup> The threat stems from the vulnerability inherent in the properties of cyberspace,<sup>13</sup> and because of these special characteristics, the cyber threat challenge differs fundamentally from the challenges of traditional threats.

### **Levels in Confronting the Threat**

This article focuses on the cyber threat to the computerized part of the infrastructures, based on the realization that such a threat has become possible, available, significant, and is liable to disrupt the functioning of developed society.

Confronting the threat to critical information infrastructures includes prevention, deterrence, identification and discovery of the attack, response, crisis management, damage control, and a return to full function. When

examining ways to confront threats to national security, the accepted practice is to divide the discussion into the tactical, operational, and strategic levels. Proposed here is a division of methods for confronting the threat to critical communications infrastructures into a number of levels: technological, technical-tactical, operational, and national-strategic.

The technical level focuses on an organization's computerized system, which is the most common activity in this realm. Given the large volume of activity, the technical aspect of "information security" is often emphasized, though it is actually a concept that deals with both defense of critical infrastructures and cyber security in general. In addition, activity that examines the issue from a comprehensive national perspective, referred to below as the national level of cyber security, is underway.

All the levels are required to confront the threat, but given the different focus, it is worthwhile distinguishing between these levels of protection. The proposed division will help identify the essence of the challenges of protecting critical infrastructures particular to cyber security.

### *The Technical Levels: Tactical and Operational Levels*

Since the threat is derived from the properties of computer technologies, the response to the threat is generally sought among computer experts. As expected, the proposed solutions are also based on computer technologies. The problem is perceived as a technical problem, and therefore, the proposed solution is an engineering solution. The technical and operational levels for confronting the cyber threat, which come from engineering, mathematics, and computers, focus on identifying vulnerabilities in an organization's computerized systems and seek an engineering solution that reduces this vulnerability.

Table 1 displays common issues confronted by the technical levels of protection.<sup>14</sup>

The primary means of attempting to build resilience<sup>15</sup> is to invest in backup, redundancy, air gap, and the like. Accordingly, important computer systems are built twice, in separate locations, in order to enable continued function in the event of physical damage to the system.

Today, most solutions to the engineering problems identified are implemented through the private market. Information security is a wide ranging field, and describing it is beyond the scope of this article. In the division proposed here, information security lies in the technical-

**Table 1. Types of Vulnerability and Responses**

Vulnerability	Response
Access passwords for devices and systems are not changed from the default.	Password management
Passwords are saved and sent without encryption.	
Access passwords are not changed periodically.	
Physical security is lacking.	Physical access security
People who do not deal with critical equipment have access to it.	
Faulty management of user permissions gives a low level employee access to a critical process.	Computer access security
A firewall configured improperly allows unnecessary types of communication.	
The process network is not separated from the office network.	
The possibility of remote access to the computer system has been left open.	
The computer system can be accessed from a wireless network.	
The remote access process uses an open protocol and weak passwords.	
The manufacturer of the system supplied security updates but they were not installed in the system.	Configuration management
Administrator rights were given to regular users.	
Access to critical system components was not monitored; no log information was collected.	
Information log is not checked on an ongoing basis.	

operational levels. Information security is a developing discipline that brings together many resources for research and development, consulting services and outsourcing, a security product industry, and the like. The worldwide information security market is expected to grow, and some market analysts claim (perhaps with some exaggeration) it will reach \$125 billion in 2015. Most of these revenues will go to US and European

companies that offer combined solutions of technical goods and services, together with technological-business consulting.<sup>16</sup>

The issue of cyber security, and especially of critical infrastructure protection, came about as a result of technological change. At first, it was expected that the solution to a problem of technical origin would be technical. However, there is a growing understanding that this problem cannot be dealt with on a technical-operational level only, since a precise engineering formula for dealing with the cyber threat is not possible: society's structure, values, and institutions are integral parts of the environment.

### *The Top Level: The National Strategic Level*

The national strategic level examines the threat to critical infrastructures in the framework of national security, with a national focus that goes beyond the boundaries of an organization or a business process. This approach sees the protection of critical information infrastructures as part of the protection of society as a whole. Protection of information infrastructures actually becomes protection of an information-based society.<sup>17</sup> Information security, which is at the center of the technical level, is a necessary but by itself insufficient part of the strategic vision. The highest national level is based on technical and operational foundations, but in a broader approach it is not sufficient to fix local problems of organizational systems. As in the military, the strategic level needs an appropriate operational level, but this is not sufficient to achieve the strategic goal.

In a wider national perspective, a comprehensive national policy on protecting critical infrastructures is needed, which in addition to the engineering foundations will take into account the complex social, political, economic, and organizational aspects. An organizational entity capable of taking into account the complex of relationships between critical infrastructures and a functional society and the state is also required. The national level of protection requires cross-organizational activities, backed by effective authority. Without a doubt, this is a complex challenge for public policy, considering the structural limitations of public service on the one hand and a required level of strategic focus of those in the private sector, on the other. Just as the state defends its entire physical space, it also sees an increasing need to protect cyberspace fully, in spite of its special characteristics, which make the task more difficult.

## Issues for Policymakers

The information revolution continues to change the strategic environment, and it affects a range of social, cultural, and economic issues in complex ways. Cyber security, and in particular, protection of critical infrastructures, is already on the agenda. The development of cyber threats to a national security issue makes governments into the main customers of protection services. Even limited experience shows that there are differences in the framework of the discussion and the types of solutions proposed in different countries, in spite of the great similarity in the source of the threat. Since the threat is similar, the explanation for the differences must be the role social institutions play in the discussion and in determining the response. What follows are the main issues concerning cyber threats that call for a public debate.

*Which infrastructure is critical?*<sup>18</sup> Any discussion on protection and defense measures must begin with prioritization. Assessing and measuring the level of the threat to components, computers, and systems is a necessary precondition for effectively confronting the threat. The exact sciences and engineering have mathematical methods for measuring the relationships and the dependence between components and the system. These tools are also used in the technical levels of protection of critical infrastructures. Nevertheless, more comprehensive methods are needed for assessing risks that stem from the intricate relationships among complex technological systems that critical infrastructures contain.

An assessment of how critical an infrastructure is on a national level must address the full matrix of social values, goals, and interests. Therefore, the relative importance of infrastructure and the amount of public investment needed to protect it are not derived from an engineering formula, and require a wide ranging and informed public discussion. Representative political institutions are the place for such a discussion in a democratic society. Given the constraints of the political system, such a discussion will presumably be lengthy and at times frustrating. Nevertheless, only through a joint political process will it be possible to design an optimal response to the threat for the long term.

*Cyber vulnerability: technical issue, economic risk, or security threat?* What is the potential significance of the growth of cyberspace in general, and the harm to critical cyber infrastructures in particular? The topic clearly goes beyond the scope of computers, engineering, and information

security to the question of the role of the state in cyber protection of critical infrastructures. Is this task military, partially civilian, “homeland defense,” or civilian-commercial? The answer directly affects the solution proposed, and it has wide political, budgetary, and organizational consequences. Until recently, the common assumption was that this is mainly a technical issue, and the response therefore was placed in the hands of computer experts. Commercial companies provided technical solutions for the military, commercial, and civilian sector, and governments did not play a significant role. Today it is clear that the optimal answer can be found only in a joint discussion between various sectors in society because it is derived from the values of the society, its political and social structure, and its national security concept.

*A political process for finding the balance between the values of freedom, market ideology, and security requirements:* Critical infrastructures and the information necessary for their proper functioning affect all areas of a citizen’s life. They raise many issues that affect civil rights, such as privacy, confidentiality, and due process; the relative strength of the state, citizens, and corporations; and allocation of public funds. Therefore, the central challenge in designing a policy to protect critical infrastructures from cyber threats is not technical or operational, rather a challenge of a comprehensive national-strategic vision. Critical infrastructure protection is not the exclusive preserve of systems engineers and computer experts. The optimal response to the cyber threat in general and the threat to critical infrastructures in particular will be created only through a broad public discussion in the framework of a democratic political system.

*The private market and cyber security:* The cyber threat is affected by the decentralized nature of economic activity in an era of rapid technological change, globalization, and privatization. The global market economy has created the situation in which large parts of the critical infrastructures are privately owned.<sup>19</sup> The unprecedented mutual dependence in international trade is one of the prominent expressions of globalization and privatization. The industrialized nations import most of the raw food that their citizens consume and export finished products and services. Food retailers do not keep inventory beyond several days’ worth of typical consumption, and they depend on the continued undisturbed function of the extensive logistical supply chain to satisfy demand within a short time.<sup>20</sup> Given that disruptions in food supply would be a grave problem of wide social



implications, this supply chain could be perceived as a “critical information infrastructure” and become an urgent policy issue.

Open societies<sup>21</sup> with free economies shy away from state intervention in business processes. In the world of free markets, any attempt at government intervention in market processes is viewed with suspicion. Thus, for example, the arguments against government regulation of the internet originate with the ideology that goes along with a free market. The solution adopted thus far was focused on regulation: in the United States, since the mid-1990s detailed standards have been developed and adopted for securing information in various sectors and industries,<sup>22</sup> and organizations for supervision and control have been established. However, the world financial crisis of 2008 illustrated the dangers of private ownership of critical infrastructures, even if subject to regulation.

In the past year, the critical infrastructures protection policy in the United States has shifted from an emphasis on market mechanisms and voluntary “private-public cooperation” to a model that gives the government broad powers to guide business institutions and supervise implementation.<sup>23</sup> Israel too has regulation of critical infrastructures, and there was a proposal to expand it to small businesses.<sup>24</sup>

*The computer products market and cyber security:* The state of the market in this area is not encouraging. Security is secondary, as opposed to quick time to market. Furthermore, it is much more difficult to make the effort necessary for resilience and reliability testing in a private commercial environment, because achievements are measured by the length of time it takes to receive a return on the initial investment and the reduction of expenditures not connected to the core activity, and there is protection of limited liability only. Today, manufacturers of computer systems have no incentive to invest in increased reliability and protection. Security is seen as an external function, an addition to the core system, sometimes from another manufacturer that does not receive the cooperation of the original manufacturer.

The level of reliability and information security in most software, hardware, and computer system communication is thus lacking today, and this broad vulnerability has undoubtedly contributed to the rise of the cyber threat. Security systems must be easy for any user to operate, require minimal computer resources, and not harm the functionality of the core system or the user experience. Given the legal, economic, and competitive

circumstances, it is difficult to expect productive voluntary cooperation between private companies in these fields. However, nationalization is not the answer, nor should it be expected as a condition for increasing cyber security. In light of the cyber threats, what is needed is developing government policies to direct the market towards a greater level of security overall.

### The Israeli Response

Securing sensitive information and protecting computer infrastructures are not new issues for the State of Israel, and there are Cabinet decisions dating back to 1996 on defense against cyber threats.<sup>25</sup> The format for protecting computer infrastructures was laid out in decision B/84 of the Ministerial Committee on National Security, "Responsibility for protecting computerized systems in the State of Israel" on December 11, 2002. To this day, this decision serves as the basis of the Israeli response to the cyber threat to critical information infrastructures. The response mandated by the decision includes establishment of a steering committee which, from time to time, examines the identity of the institutions that it is critical to protect, and the establishment of a government unit to protect civilian computerized infrastructure, the Information Security Authority<sup>26</sup> (RE'EM). RE'EM was established within the Israel Security Agency (Shabak) in order to comply with legal restraints on government intervention in business, since by law only civilian authorities, such as the police or the GSS, can intervene in private businesses. RE'EM oversees IT security in institutions that have been defined as critical: provides guidance, oversees implementation, and is authorized to institute sanctions against those that violate its directives. The institutions bear the costs of the protection required. Other important institutions that are under the responsibility of a government ministry operate according to RE'EM professional guidelines but are not legally overseen by it. The IDF and intelligence community protect their specific infrastructures independently, with RE'EM formal guidance

In comparison with the situation abroad, it appears that at the time this decision was made and implemented, Israel was relatively advanced in designing and implementing protection of critical infrastructures on a national level. However, cyberspace has continued to develop rapidly since then, and new systems and relationships have developed that cannot necessarily be defined as critical national infrastructures. One

example is small and mid-sized businesses dependency on commercial communications providers and open internet. The bloom of commercial and consumer “cloud computing” applications raises new issues and indicates yet again the increasing importance of cyberspace in all realms of life.

The Israeli policy for critical infrastructure protection was set up nearly a decade ago and served it well. Nowadays it may lack a comprehensive view of the interconnectivity developing in cyberspace that serves all civilian commercial activity. It is therefore worth reexamining the existing and anticipated challenges and the desired response. Last year, the government launched a National Cyber Initiative to advise the government on cyber security issues.<sup>27</sup> The National Cybernetic Task Force, an expert committee of academics and practitioners working under the auspices of the National Council for Research and Development in the Ministry of Science and Technology, formulated recommendations.<sup>28</sup> On August 7, 2011 the government of Israel decided:

To work to promote the national capability in cyberspace and to better confront the current and future challenges in cyberspace: to improve protection of national infrastructures that are critical for normal life in the State of Israel and to protect them, to the extent possible, from cyber attack, while promoting Israel’s status as a center for developing information technologies, encouraging cooperation between academia, industry, and the private sector, government ministries, and special institutions...Accordingly, pursuant to decision number B/84 of the Ministerial Committee on National Security, dated December 11, 2002, and without prejudice to the authority given to any other party under any other law or Cabinet decision [it is decided]:

1. To establish a national cyber headquarters in the Prime Minister’s Office.
2. To arrange responsibility for handling the cyber field.
3. To promote the ability to protect cyberspace in Israel and to promote research and development in the cyber field and in supercomputing.<sup>29</sup>

The Cabinet decision is likely to lead to improved regulation for an Israeli response to the cyber threat in general, and the threat to critical infrastructures in particular.

## Conclusion

The renewed discussion on critical national infrastructure protection focuses on the cyber dimension. Since all infrastructures have been affected by the information revolution and all now include computerized components that are mainly for command and control, this rapid technological change has created a new, additional security threat. The nature of cyberspace allows an attacker to disrupt the functioning of critical infrastructures without being physically near the target and without risking unequivocal discovery by the party attacked.

Although at first glance it appears that the subject of protecting critical information infrastructures belongs in the realm of computer engineering, upon further examination it becomes clear that it should be expanded beyond the technical aspect. Indeed, the major challenge in protecting critical infrastructures from cyber threats is not technical, but strategic and political. Today most states have legal and technical regulation for selected sectors. Since 2002, through the oversight and guidance of a particular organization, the State of Israel has been protecting infrastructures it deems critical. However, the development of cyberspace has left its civilian and non-critical sectors unprotected, and at the same time, raised both the level of vulnerability and the potential severity of effects. The recommendations of the new National Cyber Initiative are expected to set a policy process in motion.

The cyber threat to critical infrastructure is perhaps the most significant issue in the realm of cyber security. Only a thoughtful, informed process can design a policy of effective critical infrastructure protection from cyber threats and thus reduce the risk confronting the State of Israel and other developed countries from cyberspace. The major recommendation, therefore, is to broaden the public discussion of cyber security to include social and cultural aspects, which will make it possible to cope with the threat optimally on a national-strategic level with a comprehensive national perspective.

## Notes

- 1 This article was written before the launch of the National Cyber Initiative, which also dealt at length with the topic discussed here. However, the recommendations of the National Cyber Initiative have not yet been released publicly.

- 2 Critical information infrastructures are systems and facilities whose destruction or interference (by means of computers) would: “a. cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction; b. impair Federal departments and agencies’ abilities to perform essential missions, or to ensure the public’s health and safety; c. undermine State and local government capacities to maintain order and to deliver minimum essential public services; d. damage the private sector’s capability to ensure the orderly functioning of the economy and delivery of essential services; e. have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or f. undermine the public’s morale and confidence in our national economic and political institutions.” See U.S. Government, White House, Homeland Security, Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, [http://www.dhs.gov/xabout/laws/gc\\_1214597989952.shtm#content](http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#content).
- 3 Elgin Brunner and Manuel Suter, *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies* (Zurich: Center for Security Studies, ETH Zürich [Swiss Federal Institute of Technology], 2008); John Moteff, Claudia Copeland, and John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?* (Washington, D.C.: Congressional Research Service, Library of Congress, 2002); Myriam Dunn, “The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP),” *International Journal of Critical Infrastructures* 1, no. 2-3 (2005); U.S. Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2009*, [http://www.dhs.gov/xprevprot/programs/editorial\\_0827.shtm](http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm); Tyson Macaulay, *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies* (Boca Raton, FL: CRC Press, 2009); Robert Radvanovsky, *Critical Infrastructure: Homeland Security and Emergency Preparedness* (Boca Raton, FL: CRC/Taylor & Francis, 2006).
- 4 For example, Australia and the United States, which are countries that clearly attribute great importance to their political history as a central element in their collective national identity and social and political strength. *International CIIP Handbook 2008/2009*, Table 1; U.S. Department of Homeland Security, U.S. Department of the Interior: *National Monuments & Icons: Critical Infrastructure and Key Resources, Sector-Specific Plan*, 2010, <http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf>.
- 5 This refers to a tenet of chaos theory describing how tiny variations affect complex systems. The chaos theory attempts to describe the phenomena through mathematical methods.
- 6 Harm to the government’s level of functioning, which harms services to citizens, creates escalation: public confidence in the government drops, and this is liable to be expressed in political change (a change of government in a representative regime) or even regime change (a revolt against an

- authoritarian regime or a change in the structure of the regime in a democracy).
- 7 IATA (International Air Transport Association), *Air Transport Facts (2009)*, [http://www.iata.org/pressroom/facts\\_figures/fact\\_sheets/Pages/economic-social-benefits.aspx](http://www.iata.org/pressroom/facts_figures/fact_sheets/Pages/economic-social-benefits.aspx). The IATA represents 93 percent of scheduled air traffic in the world.
  - 8 The United States was a pioneer in this field, initiating a discussion on the presidential level in 1996: United States, President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection* (Washington, D.C.: U.S. G.P.O., 1997).
  - 9 In the "strategic bombing campaign" in World War II, the allies concentrated their aerial effort on attacking German factories producing ball bearings and lubricating oils, refining facilities, and railroad junctions. The operation was intended to harm the critical infrastructure for weapons manufacturing.
  - 10 The United States has led the response to cyber vulnerability since the mid-1990s, having enormous technological and military strength and being the only superpower.
  - 11 Since 2001, terrorist organizations have launched rockets and mortars from the Gaza Strip at towns in the Negev. The rockets have thus far caused nineteen deaths, and the mortars ten, and they have seriously disrupted life in the region. Following an escalation, Israel launched Operation Cast Lead in December 2008, which ended with a military victory. High trajectory fire from the Gaza Strip continues to this day, although there is less than before the operation.
  - 12 The feasibility of using cyber means to cause physical damage has been shown in experiments. A CNN broadcast that discussed the Aurora experiment, ordered by the US Department of Homeland Security and conducted at Idaho National Labs, noted that broadcasting instructions to the command and control system of the electricity generating system caused a generator to stop working and then to explode.
  - 13 Following is a summary of the challenges stemming from the characteristics of cyberspace as it exists today: the major vulnerability of computerized systems; the difficulty in distinguishing between a glitch and an attack, making the connection between an event and the result, tracing the source of the damage, and identifying the attacker, even if the source of the damage is known; and the widespread use of off-the-shelf commercial technologies. For a discussion of cyberspace in the context of national security, see Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75-92.
  - 14 Jason Stamp et al., *Common Vulnerabilities in Critical Infrastructure Control Systems* (Albuquerque, NM: Sandia National Laboratories, 2003), <http://energy.sandia.gov/wp/wp-content/gallery/uploads/031172C.pdf>.

- 15 Resilience is the system's ability to absorb an attack and return to proper function quickly. In computerized systems, the result is achieved by restoring the original situation (going back in time) or by quickly adjusting to new constraints (adaptation).
- 16 See [http://www.strategyr.com/Information\\_Security\\_Products\\_and\\_Services\\_Market\\_Report.asp](http://www.strategyr.com/Information_Security_Products_and_Services_Market_Report.asp).
- 17 James Der Derian and Jesse Finkelstein, "Critical Infrastructures and Network Pathologies: The Semiotics and Biopolitics of Heteropolarity," in Myriam Dunn Cavelty and Kristian Soby Kristensen, eds., *Securing "The Homeland": Critical Infrastructure, Risk and (In)Security* (London and New York: Routledge, 2008).
- 18 There is a great difference between the definition of critical infrastructure and the means taken to protect it in the various countries. See Brunner and Suter, *International CIIP Handbook 2008/2009*. The civilian aspect of protection of critical infrastructures in Israel is grounded in the Laws to Regulate Security in Public Places, 1998. The law authorizes the General Security Services to instruct various public institutions in physical security, information security, and essential computer system security, according to details appearing in annexes to the law. This law set punishments for failure to follow its instructions, including a civil fine and incarceration. In 2003, the government Information Security Authority was established, which is "charged with professional guidance of the institutions under its responsibility in the area of protecting critical computer infrastructures from the threats of terrorism and sabotage, in the area of classified information security, and in threats of espionage and exposure." See <http://www.shabak.gov.il/about/units/reem/pages/default.aspx>.
- 19 Most public transportation in the United States and more than 85 percent of the country's energy sector are controlled by private commercial companies. Some 85 percent of the communications of the US Defense Department uses commercial networks. See <http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/energy1.htm>.
- 20 The State of Israel, by virtue of its geopolitical situation, keeps an inventory of food and equipment in order to assure the needs of the economy in an emergency. The Supreme Emergency Economy Authority – Food and General Economy, which is part of the Ministry of Industry and Trade, is the body responsible for this issue today.
- 21 This concept comes from philosopher of science Karl Popper. See Karl Popper, *The Open Society and its Enemies* (Routledge: 2011).
- 22 See, for example, the publications of the US National Institute of Standards and Technology, <http://csrc.nist.gov/publications/PubsFL.html>, as well as the electrical standards of the North American Electric Reliability Corporation (NERC), CIP-002-3 through CIP-009-3, [http://www.nerc.com/fileUploads/File/Standards/Revised\\_CIP-002-1\\_FAQs\\_20090217](http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217).



- pdf and [http://www.nerc.com/fileUploads/File/Standards/Revised\\_Implementation\\_Plan\\_CIP-002-009.pdf](http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf).
- 23 CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, 2011).
  - 24 Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks," *Military and Strategic Affairs* 3, no. 1 (2011): 93-101.
  - 25 See, for example, Cabinet decision 1886 BK/9 from March 20, 1997: Establishment of a steering committee on computerization in every government ministry; Cabinet decision 3582 BK/77 from March 16, 1998: Responsibility for the subject of information security in government ministries; Cabinet decision 4956 BK/179 from March 23, 1999: Establishment of a council to secure sensitive information in the Prime Minister's Office; Cabinet decision TM/80 from November 26, 2000, on responsibility for computer information security in the IDF and cooperation with civilian authorities; Cabinet decision TM/14 from July 18, 2001: A secure internal network for government ministries.
  - 26 <http://www.shabak.gov.il/about/units/reem/Pages/default.aspx>.
  - 27 The National Cyber Initiative deals in part with the subject of protecting civilian cyberspace.
  - 28 The committee recommended establishing a national cyber headquarters to report directly to the Prime Minister, with a budget of NIS 100 million; establishing an office to deal with the country's infrastructure and the civil sector; policy and regulatory change to encourage the cyber industry; encouraging cyber R&D; developing centers of excellence and encouraging academic and industrial research. Shmulik Shelah, "Israel Vulnerable to Cyber Attack on Civilian Targets," *Globes* July 5, 2011, <http://www.globes.co.il/serveen/globes/docview.asp?did=1000660740>.
  - 29 Cabinet secretary announcement at the end of the Cabinet meeting of August 7, 2011, paragraph 4: Promoting national capability in cyberspace, <http://www.pmo.gov.il/PMO/Secretarial/Govmes/2011/08/govmes070811.htm>. At the time of writing the organization is not yet functioning.



## INSS Memoranda 2007 – Present

---

- No. 111, December 2011, Benedetta Berti, *The Ongoing Battle for Beirut: Old Dynamics and New Trends*.
- No. 110, November 2011, Meir Elran, Owen Alterman, and Johannah Cornblatt, eds. *The Making of National Security Policy: Security Challenges of the 21<sup>st</sup> Century – Conference Proceedings*.
- No. 109, June 2011, Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts, Trends, and Implications for Israel* [Hebrew].
- No. 108, May 2011, Emily B. Landau and Tamar Malz-Ginzburg, eds., *The Obama Vision and Nuclear Disarmament* [Hebrew].
- No. 107, March 2011, Emily B. Landau and Tamar Malz-Ginzburg, eds., *The Obama Vision and Nuclear Disarmament*.
- No. 106, November 2010, Yehuda Ben Meir and Olena Bagno-Moldavsky, *Vox Populi: Trends in Israeli Public Opinion on National Security 2004-2009*.
- No. 105, August 2010, Meir Elran and Yoel Guzansky, eds. *Vision and Reality in the Middle East: Security Challenges of the 21<sup>st</sup> Century – Conference Proceedings*.
- No. 104, June 2010, Gallia Lindenstrauss, *Mediation and Engagement: A New Paradigm for Turkish Foreign Policy and its Implications for Israel* [Hebrew].
- No. 103, May 2010, Tamar Malz-Ginzburg and Moty Cristal, eds., *A Nuclear Iran: Confronting the Challenge on the International Arena* [Hebrew].
- No. 102, December 2009, Michael Milstein, *Muqawama: The Challenge of Resistance to Israel's National Security Concept* [Hebrew].
- No. 101, November 2009, Meir Elran and Judith Rosen, eds. *The US and Israel under Changing Political Circumstances: Challenges of the 21<sup>st</sup> Century – Conference Proceedings*.
- No. 100, September 2009, Aron Shai, *Sino-Israeli Relations: Current Reality and Future Prospects*.

- No. 99, June 2009, Meir Elran, ed., *The Civil Front* [Hebrew].
- No. 98, April 2009, Anat N. Kurz, *The Palestinian Uprisings: War with Israel, War at Home*.
- No. 97, March 2009, Shmuel Even and Amos Granit, *The Israeli Intelligence Community: Where To?* [Hebrew].
- No. 96, September 2008, Ron Tira, *The Struggle over the Nature of War* [Hebrew].
- No. 95, August 2008, Anat N. Kurz, *The Palestinian Uprisings: Struggle on Two Fronts* [Hebrew].
- No. 94, July 2008, Ephraim Kam, ed., *A Nuclear Iran: Implications for Arms Control, Deterrence, and Defense*.
- No. 93, April 2008, Shmuel Even and Zvia Gross, *Proposed Legislation on the IDF: Regulating Civil-Military Relations in the Wake of the Second Lebanon War* [Hebrew].
- No. 92, December 2007, Dani Berkovich, *Can the Hydra be Beheaded? The Campaign to Weaken Hizbollah* [Hebrew].
- No. 91, July 2007, Benny Landa and Shmuel Even, *The Israeli Economy in the Age of Globalization: Strategic Implications* [Hebrew].
- No. 90, May 2007, Yehuda Ben Meir and Dafna Shaked, *The People Speak: Israeli Public Opinion on National Security 2005-2007*.
- No. 89, March 2007, Ron Tira, *The Limitations of Standoff Firepower-Based Operations: On Standoff Warfare, Maneuver, and Decision* [English and Hebrew].
- No. 88, February 2007, Ephraim Kam, *A Nuclear Iran: What Does it Mean, and What Can be Done*.
- No. 87, January 2007, Ephraim Kam, *A Nuclear Iran: Analysis and Implications* [Hebrew].