ISRAEL'S COMPETITION WITH IRAN, 1991–2015
by Michael Matlaga

Context and Background

Iran and Israel, once partners with warm relations diplomatically and militarily, have never engaged in direct military confrontation. In the aftermath of the Iranian revolution in 1979, Iran and Israel severed official diplomatic ties, and relations between the two states quickly deteriorated into a decades-long gray zone competition, one that continues today. This case examines organizational and policy shifts made by Israel between the First Gulf War and the implementation of the 2015 national defense strategy, with particular emphasis on the 2006 Israel-Lebanon War.

The end of the First Gulf War defined what Israeli defense officials saw as a new security environment where state-based conflict was likely to be replaced by short, low-intensity conflict that involved the public on the home front more than ever before. The end of the war thus resulted in a period of organizational and procedural change, notably for the Israeli Defense Forces (IDF) with the creation of a new regional Home Front Command. It also prompted changes for the IDF’s intelligence arm, Aman, with the introduction of systemic analysis, which focuses on “systems” with cross-functional and multi-country portfolios rather than teams focused exclusively on specific countries or regions.

The 2015 IDF national defense strategy, prepared by IDF Chief of the General Staff Gadi Eisenkot, was Israel’s first public document of its kind and marked a turning point in how Israel views the threat from Iran and views strategy itself. The document reflects three key lessons for Israel from the preceding decades: (1) there is a need for a renewed focus on interagency integration in tackling gray zone competition, occurring during “campaigns between wars”; (2) Iran poses a strategic-level threat to Israel and thus merits a strategic response; (3) Israel’s mode of competing with Iran remains at the tactical and operational levels. The contradiction of some of the lessons from the defense strategy suggests that organizational forms can impose constraints on national purpose.

The relevant actors during these shifts have been the Prime Minister’s Office (PMO) and the relevant cyber domain oversight authorities, the Ministry of Strategic Affairs and Public Diplomacy (formerly Hasbara Ministry and Ministry of Public Diplomacy), the IDF and Aman (military intelligence), and Mossad (foreign intelligence). Of the gray zone activities identified in this study, the most prevalent in this case were Israeli efforts to counter Iranian proxies and state-backed forces, as well as information and cyber operations. The role of the political domain, especially with Israel expanding its diplomatic relationships with Sunni Arab states in the region, was largely muted but played an increasingly important role toward the end of the period.

Findings

The period examined in this case study is perhaps best defined by the culture of decentralized experimentation and widespread aversion to strategy and long-term planning throughout the various agencies within the Israeli defense and foreign policy establishments. Acting autonomously from each other with little central direction, each of Israel’s relevant agencies were and continue to be in a constant state of assessment of their performance, analyzing failures and looking for ways to better meet their priorities and compete with other agencies for influence despite clear divisions in areas of responsibility. Most changes occurred by adapting their individual approaches to the shifting security environments but also occasionally by making internal structural changes themselves. These organizational changes mostly involved expanding the number of internal structures or increasing funding for existing, lesser-funded units. A key commonality was a priority on the short term over the long term. While it is never explicitly stated as such by civilian officials or agency heads, this short-term tactical and operational focus is perhaps the driving force behind why, despite frequent self-assessments of agency organizational approaches and plans, meaningful organizational expansion or restructuring was infrequent. The creation of the Ministry of Public Diplomacy is one notable exception to this trend.

The PMO, relying heavily on public opinion to lend it political power over agencies, held more influence over other civilian bodies than the defense and intelligence communities and primarily sought to carve out control over emerging dimensions of gray zone policy, asserting control with reassignment and some active roles in the information space and oversight in the cyber domain. It also pushed for cooperation with traditionally hostile Arab neighbors in an effort to combat Iranian influence in the region.
Organizational changes to the defense and intelligence establishments were rarely prescribed or ordered by the PMO, the Knesset, or other civilian leaders. Rather, the PMO defined the roles of each of the agencies broadly (e.g., defense, foreign intelligence, information operations, and oversight) and occasionally articulated the need for new roles—as was necessary with the emergence of modern telecommunications technology and the cyber domain—but otherwise the PMO did not dictate organizational policies or activities. The relative independence of the agencies led to consistency in role assignments between them, as the civilian authorities generally lacked the political influence and, as it relates to the intelligence community, meaningful legal authority to force change or reassignment. The military and military intelligence concerned themselves with the real-time military demands of combatting Iran's proxies—Hezbollah and Hamas—albeit in multiple domains. Mossad was the dominant force in covert action and targeted assassinations and led in intelligence collection and offensive cyber operations against Iran. The PMO and the Ministry of Strategic Affairs and Public Diplomacy—formerly the Hasbara Ministry and Ministry of Public Diplomacy—took control of the information space (information and disinformation). Meanwhile the PMO seized the initiative in the regulation of the cyber domain and cyber defense through its subservient bureaucracies—in this case, offices like the National Cyber Bureau and eventually the National Cyber Security Authority.

This decentralized, delegated form of control led the individual agencies to take responsibility for and to institute their own organizational changes at all levels, as well as to take cues for the need for change from different stimuli. Change in the IDF depended on the public perception, both of the IDF itself and of the competence of civilian leadership. Aman, relatively insulated within the IDF, adapted based on its own perceptions of the changing security environment. Mossad's direction was mostly defined by the agency leadership but was occasionally forced to contend with bad publicity. Yet, the agencies generally decided that long-term strategic plans were not well-suited to the current security environment, choosing instead to focus on the operational and tactical levels. While civilian authorities generally did not force change on the agencies, they were each subject to the public opinion of a well-informed and involved civilian population and sometimes implemented changes when faced with intense scrutiny and failure.

After the 2006 war with Lebanon, the defense establishment contended with intense public scrutiny over its performance—leading to a number of important personnel changes like the IDF chief of staff and the minister of defense. While overall funding continued to decline, damage to the civilian sector spurred a renewed interest in the need for a robust Home Front Command. These constraints and the public failures during the campaign also led the IDF and Aman to shift focus from special operations and airpower to fighting “hybrid” enemies like Hezbollah that, in their assessment, fell between low-intensity and high-intensity conflict. This chiefly involved the re-expansion of IDF ground forces with a renewed focus on maneuverability. The acknowledged strategic threat from Iran served mostly as an overture for the more real-time threats Israel faced through Iran’s proxies.

Mossad largely operated with a level of secrecy beyond that of any comparable Western intelligence agency. Behind this veil of secrecy, Mossad enjoyed near limitless autonomy. However, highly public cases like the assassination of Hamas leader Mahmoud al-Mabhouh, the suicide of Mossad agent Ben Zygier, the exposure of Mossad agents using British and New Zealand passports, and a report by the state comptroller exposing abuses did cause promises of internal reorganization, adaptation, and personnel changes to appease calls for greater oversight of the spy agency.

One significant organizational change, however, occurred due to internal pressure on then-Mossad chief Meir Dagan to increase cooperation with foreign intelligence agencies. In response, he transformed and expanded the traditionally decrepit Tevel foreign liaison unit to meet these demands. Oversight by the PMO or any other arm of the government was essentially non-existent, allowing the agency to pursue its goals relatively free of constraints. Mossad consistently recognized Iran as the greatest source of concern for both their counterterrorism and counterproliferation priorities, but its fixation on the operational and tactical levels prioritized weakening Iran’s influence over Hezbollah, Hamas, and the proxies themselves.

The decentralized command structure, the diminished importance of civilian leadership over the agencies, and the clear lines between responsibility for the various aspects of modern gray zone competitions not only meant that the agencies were largely responsible for instituting their own changes but also resulted in a general lack
of coordination across them and, in fact, competition between them. The IDF, which had its own intelligence service in Aman that aligned with the needs of the military, did not frequently need to enlist the assistance of the PMO or Mossad in executing its mission. In fact, the involvement of the civilian leadership in military decisions fluctuated with public opinion about foreign policy. After the 2006 war, civilians largely blamed the political leadership for its lack of military expertise despite numerous internal reports about IDF failures. Mossad’s unparalleled secrecy and independence in choosing its own missions meant that it rarely conducted operations that required cooperation with the military or the PMO.

These characteristics all meant that strategy was not defined in a centralized process by the country’s leadership but at best evolved out of an accretion of independent activities directed by autonomous agencies. However, the end results were less than the sum of their parts, not strategies so much as a series of specialized operational plans. Even the 2015 national defense strategy largely focuses on the interim operational national defense concerns. This aversion to long-term planning and focus on the short term produced relatively static organizational structures with highly malleable organizational plans and internal roles.

Lessons Learned

Israel’s organizational approaches to gray zone-like competition with Iran between the end of the First Gulf War and the implementation of the first official, public national defense strategy in 2015 provided several lessons that could be useful for application in the United States. Overall, six major lessons emerged:

- **Since organization was decentralized, and strategy not defined, each agency’s priorities and adaptations were shaped by factors specific to the nature of the organization rather than the gray zone threat itself.** Agencies prone to secrecy like Mossad react strongly to high-profile failures that bring media attention and threats of additional oversight. IDF and other military decisions, while also often effected by high-profile failures, are chiefly constrained by historically risk- and cost-averse organizational cultures. It also leads organizations to focus on what is in front of them—operations and tactics—like preparing for protracted conflict with Hezbollah or carrying out covert operations against non-strategic enemies. This reactive approach successfully mitigates known threats but is vulnerable to adversary adaptation at the strategic level.

- **Nevertheless, organizational autonomy leads to extremely effective tactical and operational responses to gray zone threats. Weak interagency coordination still held the line against adversary (Iranian) activities without strategically reducing them.** With the agencies sticking to their specialized expertise and lines of effort, specific tasks can be closely monitored and feedback loops tight. Even without highly coordinated interagency efforts, the IDF can conduct responsive operations, the PMO can generate relatively positive messaging about Israeli foreign policy aims and goals in the region, and Mossad can chip away at Hezbollah, Hamas, and Iranian command structures through covert operations. This will produce effective results in the short term but likely will not shift the overall advantage to Israel or allow it to compel a change in Iranian behavior. The United States might be able to learn from the tactical and operational successes of Israeli agencies while applying its own principles about the interagency process in an attempt to produce results at the strategic level.

- **Limited institutional constraints encouraged experimentation, self-regulation, and cultural consistency but also resulted in a lack of coordination and strategic direction.** Without meaningful civilian oversight, primarily from the PMO, the agencies were generally left to pursue their engrained mission sets under their own direction and implement changes largely as they saw fit, undergoing internal cultural change only when driven by internal factors. This led to strong internal organizational cultures and a willingness to make changes on their own, something that is not necessarily characteristic of U.S. bureaucracies. However, without overarching direction from civilian leadership, these agencies often worked in silos and pursued their lines of effort without meaningful cooperation across agencies. Without institutionalized interagency cooperation or mission reassignment from civilian leadership, agencies had very little incentive to work across offices beyond an ad hoc basis.

- **Excessive agency autonomy increased the power of outside pressure.** Even with decentralized control, other factors can constrain organizational decisions, reducing government control over agencies further. Despite the PMO’s lack of meaningful influence
over the organizational decisions of gray zone-related agencies, the IDF, Mossad, and others were not completely immune to outside pressures. For the IDF, public opinion determined the degree of autonomy they had for decisionmaking as well as the degree of blame they received for blunders. This was particularly evident after the 2006 war, when public opinion surrounding the relatively unsuccessful operations called for military adaptation but laid blame on the civilian leadership for its lack of expertise and encouraged the military to be largely responsible for its own adjustments. Mossad has enjoyed unparalleled secrecy within the government and in the public eye, but high-profile failures or abuses—like the death of Ben Zygier, the highly publicized Dubai operation to assassinate Hamas leader Mahmoud al-Mabhouh, which was caught on video, or the abuses exposed by the comptroller’s office—force the organization to react in ways that the public or other parts of the government would otherwise not be able to force.

- **Even with strong institutional reforms and structures, individuals and their backgrounds dictated organizational direction, public discourse, and the viability of oversight.** Oversight by civilian authorities of foreign policy and national security agencies—which in the case of Israel was mostly political and not institutional in nature—can be weakened by a perceived lack of expertise of the civilian leadership. This can also be further derailed by the political behavior of agency officials, both current and former, whose expertise often carries more weight in public discourse. The 2015 defense strategy, in addition to its productive calls for better interagency cooperation and recognition of gray zone challenges, also seemed to serve a political role of shifting potential future responsibility and blame to civilian leadership, a common theme after the 2006 war and the wars with Gaza that followed. These dynamics can be further amplified by the presence of officials with such expertise in politics, as is overwhelming the case in Israel. Party leaders, Knesset members, and ministers with career agency and military experience can bring their institutional biases to civilian positions and complicate political discourse and oversight.

- **Unique expertise protected organizational autonomy.** One of the primary factors that undermined civilian control over the national security departments and agencies responsible for conducting and defending against gray zone activities was public perceptions about expertise. That is, the public generally perceived civilian leadership as lacking sufficient expertise to exercise oversight or drive change within the agencies, and even often placed blame on civilian leadership for agency failures. The general population and each of the agencies largely considered the expertise of Mossad and the IDF/Aman to be specific to the organization and unique to those who serve over the long term. This resulted in broad organizational autonomy across several lines of effort, including proxy conflict and relations, offensive information operations, covert operations, and countering some types of disinformation. The most notable gray zone tool that could be replicated or distributed throughout the different agencies and sectors, cyber security, was not claimed by or isolated to a single agency. Additionally, the expertise of the Ministry of Foreign Affairs in *hasbara* and public diplomacy was not considered unique, and the PMO was able to stand up a new agency dedicated to the information domain. This has drastically weakened the role of the MFA overall.

### Best Practices
- **Strategic gray zone competition takes a coalition:** As illustrated in the Cold War case study in this report, gray zone competition cannot be conducted without allies and partners with influence over the variety of domains and locations where such competition takes place. This case study further builds out this point from difficult lessons that Israel learned not only about working with international partners, particularly international intelligence partners, but also across government agencies. Without a coherent, widely accepted strategy, Israeli agencies pursued tactical-level objectives with the utility of success not extending beyond the tactical or operational level. Israel was moderately successful at beating back Iranian gray zone activity at the tactical level—fighting Iranian proxies, justifying Israeli foreign policy positions with information campaigns, and countering disinformation from Iranian proxies. It was not, however, able to roll back Iranian influence or broader foreign policy goals that it sought to achieve through the gray zone in ways that serve larger Israeli security interests in the region. While Israel has not suffered any mean-
ingful military losses to Iran in Gaza or Lebanon, local populations in the Palestinian territories and Lebanon deeply distrust Israeli intentions following these interventions. In combination with local governance failures and other factors, this creates favorable conditions for Iranian-backed proxies, investments, and influence to persist. In fact, Iran’s broader regional footprint has only grown. So just as gray zone competition takes a coalition of allies and partners, strategic-level success in the gray zone also takes a well-integrated interagency effort.

- **Build in flexibility for initiative without losing organizational and strategic principles:** Israel’s organizational approach and the autonomy of the agencies encouraged internal-, operational-, and tactical-level experimentation. This type of initiative would likely be more difficult in a more cumbersome, bureaucratic entity like the USG, but there are ways the USG could look to replicate some of the flexibility afforded to agencies in Israel without changing the organizational and strategic principles of U.S. foreign and defense policy. Chiefly, civilian and political oversight of the national security apparatus is not mutually exclusive with looking for ways for agencies to experiment at the tactical and operational levels. This could encourage the type of experimentation that, in Israel, led to the establishment of a new regional command, the decisions within Mossad to work more closely with international intelligence partners, and the IDF ultimately adjusting its forces to deal with more hybrid enemies like Hezbollah. In the U.S. system, this type of freedom would still see civilian political leadership exercising control and setting the strategic direction of U.S. gray zone activities while allowing for agencies with unique expertise to adjust operational and tactical approaches that might allow the United States to more effectively pursue its desired outcomes in the gray zone.
Endnotes


5 Belfer Center for Science and International Affairs, <i>Deterring Terror: How Israel Confronts the Next Generation of Threats</i>.

6 In February 2019, the Committee on the Formulation of National Security Doctrine (Meridor Committee) released a report originating in the aftermath of the 2006 war that recommends the Israeli government formulate a longer-term, integrated strategic doctrine to meet the security priorities for today’s security environment. While this itself is not a new national security doctrine, it is worth noting that the national security community in Israel is beginning to look at long-term implications and priorities.

7 It is worth noting that the prime minister of Israel has often also acted as defense minister, as empty government positions are legally filled by the prime minister. The first such case was David Ben Gurion.

8 The PMO has launched programs to recruit and pay university students to defend Israeli policy decisions and reputation and engage in other online and social media information battles.


11 Belfer Center, <i>Deterring Terror</i>.


14 Chachko, “Cyber Reform in Israel at an Impasse.”


16 Kuperwasser, <i>Lessons from Israel’s Intelligence Reforms</i>.

17 Libel, “Looking for Meaning.”


20 Johnson, “Military Capabilities for Hybrid War.”

21 Ibid.


24 Libel, “Looking for Meaning.”

25 Ibid.

© 2019 by the Center for Strategic and International Studies. All rights reserved.
26 Farquhar, *Back to Basics.*
27 Belfer Center, *Deterring Terror.*