JINSA
The Jewish Institute for National Security of America

The Typhoon Doctrine:
A New Strategy For Israel's Border Security

JINSA's Gemunder Center for Defense and Strategy | May 2025

Authors

IDF BG Yoram Knafo
Visiting Fellow; Former Chief of Staff, IDF Northern Command

Ari Cicurel
Associate Director of Foreign Policy

Yoni Tobin
Senior Policy Analyst

DISCLAIMER:

The findings and recommendations contained in this publication are solely those of the authors.

Table of Contents

I. Executive Summary

The October 7 attack and its aftermath revealed significant shortcomings in Israel's border security doctrine and its implementation. Israel's assumptions about the magnitude and nature of threats on its borders proved false, and, as a result, its operational concept and plans to protect against those threats failed. These struggles starkly underscore Israel's need for a new border defense doctrine to better detect and counter a wide range of threats to its homeland.

This paper, drawing on the co-author's extensive insights from his years serving as Chief of Staff of the IDF Northern Command, proposes a new doctrine—called the "Typhoon Doctrine"—to help Israel mobilize forces with the speed and precision required by today's complex security environment; more successfully integrate intelligence and advanced surveillance; enhance aerial and subterranean threat detection and interception; and better enable rapid force deployment. By adopting these recommendations, Israel can transition from a reactive border posture to a continuously adapting system calibrated for both anticipated and unanticipated threats along its borders.

Prior to the October 7 massacre, Israel's strategy rested on a three-pronged approach that can be described as "detect, delay, and reinforce." This approach was premised on the assumed threats Israel would face along its borders: namely that Israel's military superiority would deter large-scale incursions across its borders and, if necessary, quickly defeat an incursion—expected to be geographically constrained, ground-based, and occurring in a narrow timeframe—into Israeli territory. First, Israel anticipated its intelligence capabilities, particularly its first-class signals intelligence (SIGINT) collection, would detect preparations for an incursion, providing early warning alerts to Israel Defense Forces (IDF) commanders and, as necessary, civilian leaders. Second, this advance notice would allow local frontline IDF forces to mass along the threatened border areas and, together with Israel's high-tech solid border fortifications, delay the enemy's advance. Third, if terror operatives did successfully infiltrate into Israel, commanders would deploy additional IDF units to reinforce the area and mobilize the Israeli Air Force (IAF) as required and available, and civil defense forces would provide a last line of defense for border-adjacent population centers.

The events of October 7 and the days following revealed the shortcomings of this approach. Believing any infiltration from Gaza would be localized and narrow, Israel did not adequately collect intelligence on Hamas's plans and motives, nor did it properly disseminate what intelligence it did collect. Israel leaned heavily on SIGINT, rather than human intelligence (HUMINT), gathering on Hamas's operations. This limited its ability to understand Hamas's larger strategic aims and led it to misinterpret the key indicators it did collect on the group's planning and tactical preparations.

With its border security doctrine emphasizing a small holding force and having failed to grasp the imminence or full scope of the threat, the IDF had insufficient troops in the Gaza envelope on October 7 to respond to the Hamas attack. Israel's lack of appropriate early warning or adequate border forces then resulted in Hamas's massed multi-domain assault quickly overwhelming the high-tech cutting-edge border defenses and laying waste to civilian communities, many of them miles inside Israel, and their civil defense forces before Israel could muster an armed counterattack.

In light of these challenges, Israel should adopt a new "Typhoon Doctrine" for border security. Like its namesake, this much more dynamic and forceful approach would use more aggressive and integrated processes to surge forces quickly and flexibly, from all directions, to preempt and counter cross-border incursions of any size. Key elements of this new border security doctrine should include:

- Establishing a centralized intelligence fusion command center that collates SIGINT, HUMINT, geospatial intelligence (GEOINT), as well as other forms of information, to be continuously analyzed and readily accessed by all of Israel's military and intelligence entities;
- Making greater use of underground seismic sensors, soil-tracking methods, and other technologies to detect and map cross-border tunnel networks along Israel's borders and tunnels in enemy-held territory near Israel;
- Detailing a chain of command for commanding force deployment that includes multiple redundancies for decision-making in rapid, unclear, and complicated scenarios;
- Establishing traffic routes, assembly areas, and pre-designated staging areas that would allow faster movement of personnel, vehicles, and equipment in emergency situations;
- Prepositioning "ready-to-go" command-and-control (C2) nodes near Israel's borders that can be activated at a moment's notice to provide guidance to any unit;
- Developing cutting-edge counter-drone technologies, such as lasers and high-powered microwaves;
- Deploying more flexible firepower utilizing autonomous and unmanned border-based weapons stations;
- Using the greater synthesis of intelligence envisioned under the fusion command center concept to better equip soldiers before and during battle with critical information;
- Designing a modular force structure with rapid reaction units, supported by drones, infantry combat vehicles, and mobile artillery capable of responding to breached border sectors within minutes—not hours; and
- Improving the IDF's advanced communications and Blue Force tracking to better coordinate forces.

While the onus is on Israel to update its border security doctrine to meet the threats posed by the Iran-backed terror armies that surround it, the United States can also play a helpful role. Most importantly, both countries should ensure that there is no daylight between their two governments. Public disagreements have needlessly and counterproductively emboldened mutual enemies.[1] The United States can also bolster Israel's border security by expediting the delivery of critical weapons; upgrading the U.S. prepositioned stockpile of weaponry — known as WRSA-I—in Israel; expanding joint research and development (R&D) to counter drones, tunnels, and other emerging threats; providing insights to help Israel develop intelligence fusion centers modeled after those used in the United States, including by liaising homeland security officials, intelligence analysts, and military flag officers, to share best practices with Israeli counterparts; and increasing the scale and frequency of bilateral exercises.

II. Israel's Pre-October 7 Border Defense Concept

Before October 7, 2023, Israel's official, codified border security doctrine—which applied to all its borders—relied on three pillars: advanced detection of cross-border attack plots; physical barriers and IDF soldiers stationed along the border to delay attackers; and the IDF's capacity to mobilize troop reinforcements and air force support, as needed, to neutralize border threats. The assumed threat scenario was one in which terrorist adversaries, deterred from planning and executing massive assaults by the prospect of overwhelming IDF response, would attempt at most a handful of geographically and size-limited ground-based border incursions. In the event—which Israeli planners largely discounted—that terrorists successfully crossed the border and entered Israeli villages, civil defense units in each village would hold off attackers until military reinforcements, including ground troops and air support, arrived.

A. Assumed Threat Scenario

Israel's pre-October 7 border security doctrine envisioned a specific threat scenario: limited aboveground or underground border infiltrations by individual terrorists or a handful of small terror cells. This doctrine assumed the prospect of massive, prohibitively costly Israeli retaliation would deter larger-scale attacks. As former National Security Advisor to the Prime Minister and JINSA distinguished fellow IDF MG (ret.) Yaakov Amidror said, the IDF "does not prepare itself for things it thinks are impossible."[2]

In Gaza, Israel assumed Hamas had adopted a political identity—to go along with its core function as a terrorist group—that valued improving Gaza's economy, thus ensuring it retained control of the territory, and was not interested in risking another war that could threaten its stronghold in Gaza. Based on the conception that Hamas's desire to retain control of Gaza would limit its willingness to escalate to a major war, Israel sought to improve economic conditions in Gaza, which included permitting Qatar to provide funds to Gaza and allowing thousands of Gazans to enter Israel for work.[3]

To inform its planning scenarios, Israel used Hamas's and Hezbollah's respective cross-border attacks in 2006, in which small terror cells kidnapped or killed Israeli soldiers and took with them living or deceased captives.[4] Israeli planners thus assumed any indicators to the contrary, such as Hamas plots for a wide-ranging invasion, were bluffs. Instead, they built their plans to protect against breaches that would be geographically limited, involving a few, slow-moving terrorists who could be neutralized quickly by local Israeli defense forces. Broadly speaking, the IDF did not expect a massive, simultaneous, multi-domain attack—involving ground, air, and sea components—and, therefore, did not structure or prepare its forces to defend against such a scenario. To the degree that aerial dangers were considered in its threat scenarios, Israel believed they would come in the form of short-range rockets and missiles which its highly capable Iron Dome system would intercept. If Israel's terror adversaries did attempt a multi-domain attack, Israel assumed it would detect and forestall such an operation well before it reached the operational stage.

B. Operational Concept

Israel's border security doctrine relied on a three-phased approach to address evolving border threats, with the assumption that earlier phases, if successful, would preclude the following ones. First, the doctrine anticipated that Israeli intelligence would, at minimum, detect preparations on the day of the attempted attack, generating early-warning notifications up the IDF's chains of command. IDF

commanders would then activate procedures, including increasing the number of border troops and weapons platforms on the border, to match the perceived threat. Second, if an attack was underway, Israeli frontline troops would detect assailants as they approached the border, quickly alert their superiors, and, in conjunction with Israel's extensive, high-tech physical border fortifications, neutralize or delay attackers until reinforcements arrived. Finally, if necessary, Israeli commanders would mobilize additional ground forces, and Israeli Air Force (IAF) support as needed, to prevent terrorists from penetrating into Israeli territory, with civil defense forces in border-adjacent villages serving as a last line of defense to complement IDF efforts.

i. Detect

Israel's military and intelligence services expected to detect cross-border attack preparations well before the threat materialized. Israel's doctrine presupposed that, even were a cross-border attack to begin, the array of radars, cameras, and sensors embedded along Israel's borders would alert troops of an impending attack and enable them to relay this information up the IDF's chain of command. Doing so would enable relevant commanding officers to issue clear directives and send reinforcements, including additional battalions and air support.

a. Advanced Collection on Adversary Plans

Israel's standard operating procedure prior to October 7, 2023, for collecting and analyzing intelligence on unfolding enemy plots was heavily segmented across its military and security apparatus and relied largely on cyber intelligence and signals intelligence (SIGINT) collection. Relevant intelligence-gathering entities included the IDF's regional command and divisional levels; the standalone Military Intelligence (AMAN) entity; and the civilian Israel Security Agency (Shin Bet).

Israel's different intelligence-gathering entities worked in parallel to collect intelligence on Hamas, with each collection effort highly compartmentalized within Israel's military and security apparatus. Prior to the October 7 attack, Israel tasked the Gaza Division with amassing intelligence on Hamas anti-tank and special forces units; the Southern Command with gathering data on Hamas rocket systems, tunnels, command structure, and senior military leadership; AMAN with surveilling Hamas's force buildup and political leadership; and the Shin Bet with gathering information across all these domains.[5] Furthermore, the IDF's Southern Command and subordinate divisional levels divided responsibility between themselves for collecting and collating intelligence, on the one hand, and identifying anomalies in threat patterns, on the other.[6] Though military officers and intelligence officials periodically circulated intelligence believed to have significant implications to other entities, Israel lacked a permanent cross-channel fusion center to continually pool and analyze intelligence data across this large military and security apparatus.[7]

While advanced intelligence collection methods varied by theater, Israel's intelligence collection in Gaza largely hinged on SIGINT and cyber intelligence. AMAN's Unit 8200, in particular, provided the bulk of information on developing plots, and the Southern Command's intelligence center primarily relied on intelligence from AMAN and the Shin Bet. Unit 8200 reportedly accounted for the most reports on Gaza threats to the Southern Command intelligence center in the years before October 7.[8]

b. Day-Of Tactical Early Threat Detection

Israeli officials believed that, even if they failed to detect an adversary plot in advance and attackers began approaching or amassing on Israel's borders, Israel's suite of advanced cameras, radars and sensors would send clear signals of an impending attack up the chain of command. Israel's particularly fortified Gaza border barrier included advanced infiltration-detection technology, including hundreds of

cameras, radars, and sensors.[9] In addition to its ground-based detection, the IDF flew surveillance balloons on the Gaza periphery carrying a long-range, 360-degree rotating camera.[10]

Under Israel's doctrine before October 7, 2023, intelligence entities would relay significant indicators of a cross-border attack to the divisional commander, who could, at his or her discretion, place subordinate forces on high alert.[11] In the event of an unfolding attack falling under their responsibility, the divisional commander would notify the regional commander and the IDF General Staff, as well as alert the IAF and other relevant units to mobilize troops to boost the existing border force posture.[12]

However, Israel's intelligence apparatus did not actively pool information collected from border cameras, radars, and sensors so that commands could have awareness of intelligence in other domains or nearby locations. The IDF's divisional commands primarily monitored intelligence collection, but the IDF lacked systems to perpetually aggregate data about border threats across commands and domains and send them to other divisional commands, regional commands, or other nodes of the IDF and the Israeli intelligence apparatus.[13] To the extent such systems existed, they did not permit simultaneous access by entities across Israel's intelligence and security apparatus, and were not always fed into automated models to analyze pattern discrepancies in the collected data.[14]

ii. Delay

Anticipating that enemy forces would restrict their attack to a limited ground incursion or cross-border tunneling, Israel predicated its pre-October 7 doctrine on the notion that a combination of above- and below-ground barriers and Israeli border troops would hinder the attack until additional units could deploy to neutralize the threat.

a. Physical Barriers

Israeli strategic planners expected physical fortifications to dramatically delay, if not thwart, infiltration attempts. In keeping with this core doctrinal tenet, Israel spent roughly $1 billion on a 20-foot-high, above- and below-ground barrier spanning its 40-mile border with Gaza, completed in December 2021.[15] Unlike the barriers on its other borders, Israel equipped the above-ground wall with autonomous weaponry, including remotely-fired machine guns, and a below-ground component, colloquially called the "Steel Dome," saturated with underground sensors and other technology to detect tunnel digging and thwart any underground infiltration attempts.[16]

b. Border Posture

Absent indications of an immediate border threat, the IDF deployed a predetermined number of battalions to its borders to prevent breaches. In addition to being charged with monitoring advanced surveillance equipment and early alert systems, and relaying intelligence about imminent threats to their superiors, these soldiers were tasked with firing upon and neutralizing terrorists attempting to breach the Israeli border until troop reinforcements arrived.

c. Air Defenses

In its planning assumptions, the IDF expected to face primarily anti-tank guided missile, ballistic missile, and short-range rocket threats, each routine features of the pre-October 7, 2023, threat landscape. Since Israeli strategists foresaw the primary aerial threats to the Israeli homeland as being individual or small quantities of missiles and rockets, Israel relied on its traditional air defenses, particularly the highly effective Iron Dome system—which has an estimated interception rate of roughly 90 percent—to intercept these largely unguided and isolated projectiles.[17] With this belief and capability, Israeli doctrine favored operations that were reactive to enemy threats by defending against projectile attacks or

targeting imminent launches but disfavored preemptive action to destroy the buildup of Hamas or Hezbollah capabilities.

iii. Reinforce

Under the pre-October 7 doctrine, if terrorist assailants circumvented physical fortifications and overwhelmed Israeli border troops, commanders would buttress Israel's border force posture with additional IDF troops, including a rotational battalion ready to deploy to and reinforce any theater. In addition to the rotational battalion, the relevant regional and divisional commands would mobilize battalions and assign them certain sectors to which they were to rapidly deploy. Based on the scope of an attack, commanders could also request IAF mobilization to aid ground forces.

a. Troop Surge and Air Support

Despite reinforcement being a central pillar of Israel's pre-October 7 border doctrine, Israeli planners did not institute any wide-scale, predetermined plan about where units would deploy in the event of a ground incursion. Instead, the plan was for ground troops to rely on divisional commanders' ad hoc orders assigning battalions to deploy to predetermined geographic sectors, with the designated rotational battalion deployed as necessary.[18] Media reports indicate that the IAF had only formulated an action plan for a large-scale invasion in recent years and rarely drilled on it.[19]

b. Civil Defense Units

Israeli civil defense units, comprised of volunteer residents from border communities, formed the last line of defense against a limited terrorist breach into border-adjacent villages until IDF reinforcements could arrive. Civil defense units generally consisted of between 10 to 20 members and lacked uniform organizational structures, with each unit's standard operating procedures determined on a village-by-village basis with Israel Police guidance.[20] In the event of a major attack, Israel expected civil defense forces to serve only as a last line of defense to neutralize or delay a small number of attackers until police or military backup reached the impacted community.

III. Border Security Lessons Learned

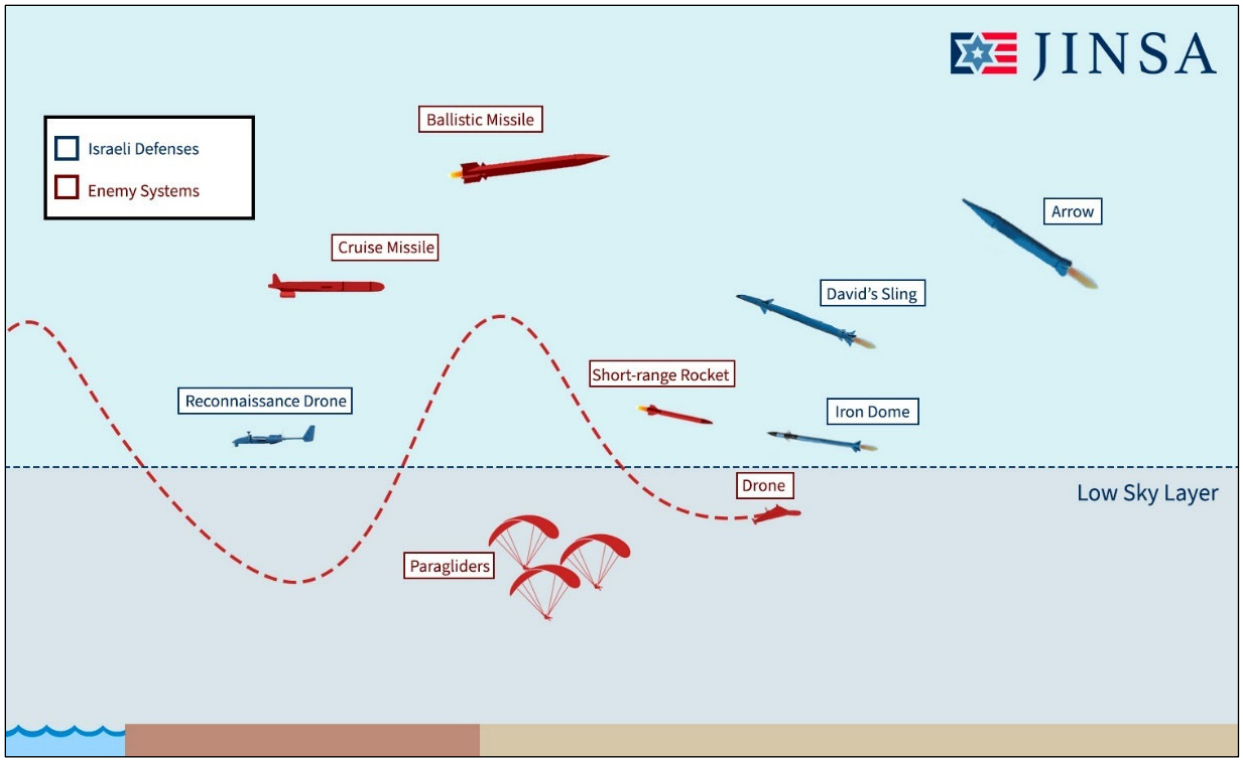
The October 7, 2023, attack and Israel's subsequent wars with Hamas and Hezbollah painfully exposed wide-ranging shortcomings in the existing Israeli border security posture—including primarily, but not exclusively, on the Gaza and Lebanon fronts. Hamas's onslaught represented a central pillar of Iran-led efforts to open an unprecedented multi-theater war and threaten Israel's survival. Iran had been preparing Hezbollah to launch a simultaneous assault into northern Israel that would likely have been far deadlier than the October 7 attack and had similar designs to open other fronts, such as Jordan and the West Bank.

Israel calibrated its border security threat assumptions, strategic and operational concepts, and doctrinal implementation to an insufficiently imaginative and far outdated threat scenario. Israel's overreliance on cyber intelligence and SIGINT; its insufficient synthesis of stove-piped, highly siloed intelligence; and inadequate preparation for the prospect of terrorists employing unconventional infiltration methods were all serial flaws in Israel's border security doctrine.

A. Threat Scenario Assumptions Proved False

The October 7 attack fundamentally upended Israel's assumptions about border infiltration threats. Israel's precepts included that it held a clear understanding of its enemies' intentions; that those intentions did not include launching a massive infiltration; and that, regardless, Israel's enemies were unable to adapt their tactics and techniques to circumvent Israel's border posture. Unlike planners in other regional commands who prepared for a variety of contingencies, prior to October 7, 2023, IDF planners in the Southern Command only prepared to counter a single threat scenario: limited incursions across or under the Israel-Gaza border.[21]

Israel's planners did not anticipate border infiltration taking place in numerous locations roughly simultaneously, nor that such breaches would remain unaddressed for several hours, permitting subsequent waves of incursions. Israel's operating assumptions were that troops would quickly seal physical border breaches, and that command-and-control would function normally, enabling commanders to deploy troops to predetermined geographic sectors and order reinforcements and air support as needed. However, on October 7, the Israel-Gaza border was physically breached in many places, with gaps in the border in some cases remaining open for hours—all while Israel's local command-and-control systems, and communications networks, were besieged and hamstrung by attacks on key nodes like the Re'im base. This further prevented local IDF commanders from notifying higher-ups about their need for troop reinforcements and air support.



Moreover, Israeli military planners did not anticipate Hamas fighters infiltrating into Israeli territory directly from the sky—a method thought to be anachronistic, and which Hamas terrorists had not successfully employed against Israel since 1987 nor attempted for nearly a decade prior to October 7.[22] Yet, on that day, armed fighters swiftly crossed into Israel using hang gliders and motorized paragliders and met no resistance.[23] This "low sky layer" between surface-level threats and higher-altitude rocket and missile threats became a crucial theater on October 7, and—due to persistent drone incursion threats, primarily from Hezbollah but also Iranian proxies in Iraq and Yemen—would remain a primary

feature of the war. However, it also became a sort of Achilles heel for Israel's world-class military and air defenses. At high altitudes, Israel possesses unquestioned superiority against high-flying rockets and missiles because of its multi-tiered air defense capabilities, including the short-range Iron Dome, medium-range David's Sling, and long-range Arrow systems. Israel similarly enjoys numerous military advantages on the ground and at sea. However, former Commander of Israel's Air and Missile Defense Forces BG (ret.) Ran Kochav plainly stated in 2024 that "the enemy has found a loophole" in Israel's defenses by exploiting the low sky layer.[24]

Hezbollah's near-daily drone attacks throughout the war—often launched at or around the same time as short-range rockets—posed an omnipresent threat to Israeli military and civilian targets. Hezbollah calibrated its drones' flight trajectories to severely diminish the effectiveness of Israel's existing air defenses, which Israel constructed to intercept small numbers of rockets and missiles, rather than regularly neutralize difficult-to-detect and low-flying drones—let alone drone clusters or near-simultaneous drone and rocket launches.

Israel discovered other border vulnerabilities during its invasion of southern Lebanon, with troops finding tunnels with exit shafts that were sometimes mere yards from the Israeli border.[25] IDF troops located over 180 tunnel shafts in total on the Lebanese side of the border, most within walking distance of Israeli border towns.[26] While the IDF knew some Hezbollah tunnels existed near its northern border, the scale of the tunnel network, which could have facilitated a large-scale invasion of Israel with Hezbollah elite operatives emerging from shafts directly across the border, was far more extensive than it anticipated. The sheer volume of weapons, including advanced Iranian and Russian-made munitions, that Hezbollah had stockpiled in homes and tunnels also caught Israel's northern border troops by surprise.[27]

In Gaza, too, Israel underestimated the degree to which Hamas utilized its terror tunnels in conflict. As JINSA's Gaza Assessment Task Force noted in its May 2024 report, *The October 7 War: Observations, October 2023 – May 2024*, Hamas constructed "tactical tunnels, smaller and closer to the surface, used by fighters to stage attacks, move between fighting positions, and travel undetected within their area of operations," which the IDF largely anticipated.[28] However, the report also observed that, having learned from prior wars with Israel and the IDF's past successful strikes against its near-surface tactical tunnels, Hamas had also, in recent years, built "more deeply buried and fortified strategic tunnels housing command-and-control centers [and] weapons production and storage facilities."[29] Hamas's strategic tunnels, in particular, were greater in scope and more of a battlefield challenge than Israel had anticipated despite all of Gaza being in close proximity to Israel's borders.

B. Operational Concept Flaws

These failures of Israeli imagination translated directly into a flawed and inadequate operational concept. Israel's highly siloed intelligence gathering, overreliance on border technologies, lack of sufficient border troops, and belief that troops could be rapidly deployed to contain any attack all significantly undercut the effectiveness of Israel's defensive posture.

i. Lack of Intelligence Fusion

For over a year beforehand and up until the day of the October 7 attack, Israel had gathered circumstantial evidence that the Iran-backed terrorist group was preparing a large-scale attack, including the Hamas battle plan itself.[30] This evidence of an imminent attack included Hamas's and other terror groups' "Strong Pillar" military exercises that brought all terror groups operating in Gaza under the command of a joint operations room; Israel's possession of Hamas's "Jericho Wall" battle plan outlining a

October 7-like invasion plan involving the air, land, and maritime domains; and Hamas's activation of hundreds of Israeli SIM cards in Gaza the night before the attack.[31]

However, the process of transmitting this intelligence up the chain of command broke down and key information did not reach senior military officers and decision-makers.[32] Senior IDF Navy commanders did not receive a briefing on the naval invasion plan from the Jericho Wall dossier, which Israel had possessed for over a year prior to the attack.[33] The Gaza Division commander alerted the Ashdod base commander around 4:00 AM local time on October 7 of unusual activity, without providing specific details.[34] When the Ashdod base commander checked with the IDF Navy headquarters, he was told there was no unusual activity, as Navy leaders were unaware of the intelligence that the IDF's Military Intelligence had acquired about Hamas's invasion plan. Regardless, as a precautionary measure, the base commander raised the base's alert level—helping the IDF respond quickly to Hamas's naval invasion.[35]

ii. Overreliance on Cyber Intelligence and SIGINT

Israel's overreliance on cyber and SIGINT methods for its intelligence collection on Gaza meant it had an inadequate number of HUMINT sources gathering intel on Hamas strategy and decision-making. Israel's insufficient allocation of resources—including time and funding—to build a HUMINT network in Gaza meant it could, via SIGINT and cyber detection tools, detect Hamas activities in the lead-up to the October 7 massacre, but not discern why the terrorist group took those actions and the deadly significance those preparations would have during the attack.

Though SIGINT provided the IDF with important information about Hamas, Israel's lack of a robust HUMINT network to help Israeli intelligence monitor Hamas terror plots meant that Israel misinterpreted key pieces of information. Leaked Israeli military intelligence files from October 1, 2023, indicated that while Israel detected Hamas's weekly preparatory drills, intelligence analysts attributed these drills to economic factors and assumed that quiet would return after the drills concluded.[36] Israeli officials also dismissed other key indicators of an imminent attack, including the widespread SIM card activation, and attempts shortly before the October 7 attack to create openings in the Israel-Gaza border wall, as either Hamas bluffs, provocations, or training drills.[37]

Israel had developed a system of indicators and warnings to help alert security forces of an impending cross-border raid, but lacking adequate HUMINT on Hamas strategy, rather than tactics, faulty assumptions informed the evidence used to make determinations.[38] For instance, analysts believed that phone signals would disappear prior to an attack as Hamas fighters moved in tunnels towards Israel's border. The night before the October 7, 2023, attack, Hamas operatives' phone signals never vanished, and, therefore, did not raise the appropriate level of concern for Unit 8200 and the Shin Bet. As a result, when Hamas terrorists activated Israeli SIM cards the night of October 6, intelligence officers chalked this up to a Hamas training exercise, as a similar activation had occurred in the past during a Hamas drill.[39] Hamas's previous exercises lulled Israel into a false sense of security that an attack was not going to happen, instead of providing clear signals that a Hamas operation was likely imminent, which HUMINT insight could have corroborated.

iii. Insufficient Border Force Posture

The IDF's pre-October 7 border doctrine involved an insufficient deployment of forces to prevent ground infiltration. Factors such as the redeployment of forces to the West Bank and other flashpoint areas, and Israel's policy of permitting troops to return home on holidays and weekends, significantly limited the size and capabilities of the Gaza border force on October 7, 2023—particularly given that day was the Jewish holiday of Simchat Torah. However, even had the attack not occurred on a holiday, and border

forces were at full capacity, Israel's force posture would likely not have sufficed to successfully defend against the Hamas attack.[40]

Israel's inadequate deployment of border troops was not a problem exclusive to the Gaza border. The IDF force posture on the Lebanon border, some two brigades plus four battalions, was insufficient to defend against the large invasion of Hezbollah's elite Radwan forces, consisting of over 2,000 well-trained terrorists on Israel's border at the time, that Hezbollah planned but ultimately elected not to execute.[41] Israeli officials privately have noted that such an incursion could have resulted in mass casualties far greater than those in the Gaza envelope and may have reached as far south as Haifa. Additionally, the IDF's sporadic deployment along its eastern front would likely have produced a similarly inadequate response to an October 7-style terrorist invasion from Jordan.[42]

iv. Reactive Force Mobilization Created Vulnerabilities

Since Israel faced much larger incursions on October 7 than the limited cross-border threats it anticipated, it was unable to mobilize its forces quickly to repel Hamas's widescale, multi-domain assault. While Israel had assumed it could effectively and quickly mobilize a small number of troops to a limited breached border sector in the event of a small invasion, Hamas's near-complete defeat of Israel's local command-and-control (C2) systems and internal communications during the attack precluded the possibility of a rapid force mobilization.[43] This breakdown was specifically engineered by Hamas terrorists, who deliberately targeted antennas, communications towers, and other key nodes—including the regional C2 center in Re'im—of the IDF's internal communications and C2 systems during the attack.[44] Hamas's highly calculated effort utilized considerable intelligence the terror group had gathered on the IDF's internal operations and procedures, resulting in, as one Israeli colonel put it, the "complete destruction" of vital Israeli communication systems.[45]

As a result, Israel was forced into an ad hoc and disjointed response to Hamas's assault, with soldiers responding to attacks based on texts from friends; commanders grabbing weapons and serving as front-line infantry instead of manning command posts; and pilots, reservists, and entire units using television news coverage to locate targets and commercial apps like WhatsApp and Telegram to communicate with one another.[46]

C. Operational Implementation Flaws

Beyond its conceptual problems, Israel's pre-October 7 border doctrine suffered from implementation failures, creating further vulnerabilities which Hamas and other terror adversaries keenly exploited. These included a lack of adequate early-warning alerts for the IDF; insufficient low sky layer threat detection and defenses, including anti-drone capabilities; counter-tunnel measures that faced limitations; and insufficient civilian alert systems.

i. No Early-Warning Alerts

Since information did not adequately travel across channels within Israel's military and intelligence apparatuses, ground forces generally did not know the scale of the unfolding attack on October 7 nor were adequately prepared to fight thousands of terrorists simultaneously storming the border. In addition, Israel's doctrinal reliance on technology, like camera arrays and advanced sensors, to detect infiltration proved a fatal flaw once Hamas kinetically disabled many of these systems and a large portion of the IDF's communications networks. Israel's lack of redundant C2 and communications systems created single points of failure, which magnified the problem. Once Israel's Re'im base, a key C2 node previously thought impenetrable, was overrun by Hamas terrorists, Hamas summarily deactivated entire

sensor banks along the border from the base itself.[47] Similarly, in the first week of the war, Hezbollah shot down roughly 80 percent of Israel's cameras on the border, according to an Israeli official with knowledge of operations in the north. In addition, Israel had not calibrated its radar systems to detect unconventional forms of low sky layer aerial infiltration, including the hang gliders and motorized paragliders Hamas used.

Moreover, due to the close proximity between Hezbollah operatives and Israel's northern border on October 7, Israel's early-warning system would not have been able to alert the IDF in time to repel a large-scale invasion from Lebanon. If Hezbollah terrorists had launched a massive infiltration into Israel along some or all of the dozens of cross-border incursion routes Israeli forces later uncovered, Israeli forces would not have had sufficient warning to prevent catastrophic massacres across Israel's northern villages, like those that Hamas caused in southern Israel.[48]

ii. Insufficient Low Sky Layer Defenses

While Israeli air defenses have repeatedly demonstrated a high rate of success, Israel failed to extend this air superiority to the low sky layer, in which Israel's terror enemies operated drones as well as unconventional threats like motorized paragliders. Drones, even rudimentary ones, have evaded Israeli detection and remain expensive to eliminate. Hezbollah drone incursions posed a consistent threat to northern Israel throughout the conflict, as did sporadic drone attacks from Iranian proxies in Iraq, Jordan, Syria, and Yemen. Israel frequently intercepted drones, but Hezbollah's operational decision to launch them in small groups with other drones or rockets enabled them to confuse or evade Israeli efforts to neutralize them. Israel's inability to consistently intercept all of the projectiles Hezbollah fired in a given attack allowed the terrorist group to strike strategic sites like military bases, population centers such as Haifa, and even Prime Minister Netanyahu's house, exposing serious vulnerabilities in Israel's defense posture.[49]

Israel has made important strides in enhancing its low sky layer defenses by developing non-kinetic air defense means, such as directed energy techniques, but these capabilities are not yet readily deployable in sufficient quantity or quality to replace kinetic systems. For this reason, Israeli air defense operations have heavily relied upon defeating drones through kinetic interception, including ground-based air defenses, like the Iron Dome system, or air-to-air missiles launched from fixed-wing fighter aircraft and helicopters. However, Israel's fighter aircraft and Apache attack helicopter fleet are necessary for other battlefield operations and, in the case of the helicopters, sometimes ineffective against drones. Low-flying drones are also capable of evading ground-based air defenses designed to strike projectiles at higher altitudes.

More glaringly, Israel's use of kinetic interceptors to neutralize roughly a year's worth of near-daily drone attacks has been costly. Israel has a limited number of interceptors and batteries, so each interceptor used against a drone, or a false positive interceptor that Israel launches against a bird, is one that Israel cannot fire against a missile or rocket. According to JINSA figures, Hezbollah launched at least 750 drones at Israel between October 7, 2023, and the December 2024 ceasefire.[50] Israel's method of intercepting drones with kinetic interception, while roughly 80 percent effective throughout the war, is resource-intensive and cost-inefficient.[51] Launching Iron Dome's Tamir interceptors, which cost between $50,000 and $100,000 per unit, at drones that cost between several hundred to a few thousand dollars, attrits Israeli interceptors and incentivizes further asymmetric warfare by Israel's enemies.[52]

iii. Limited Counter-Tunnel Technologies

Israel's current cross-border tunnel detection methods, including an underground wall and sensors on its Gaza border, have proven largely successful. Hamas is not known to have used tunnels to infiltrate into Israel on October 7, 2023, or thereafter. As noted in JINSA's December 2024 report, *Holding the Line: A Strategy for Securing the Philadelphi Corridor*, Israel's world-leading detection techniques employed along its Gaza border included subterranean sensors capable of tracking soundwaves and changes in soil composition produced by tunnel digging.[53]

However, while the IDF is fairly adept at detecting and counteracting cross-border tunnel construction, locating and neutralizing adversary tunnel systems on the other side of Israel's borders has proven far more difficult. The IDF was unaware of the vastness of the tunnel infrastructure in both Gaza and Lebanon, including directly along, but not crossing, Israel's borders. Throughout the war in Gaza, Hamas used its tunnels to move forces and materiel; stage ambush attacks against IDF soldiers; and shield vital assets like headquarters, server rooms, arms caches, and weapons manufacturing sites.[54] Hamas's sprawling tunnel network, estimated to be between 350 and 450 miles long, proved to be more extensive, sophisticated, and difficult to neutralize than the IDF had predicted.[55] Even after months of IDF operations to exhaustively destroy Hamas's tunnel network, many tunnels remained intact, with Israeli officials estimating that it would take years to neutralize them all.[56] Similarly, once IDF soldiers entered southern Lebanon in October 2024 to eliminate Hezbollah's presence there, they found tunnels containing weapons near the border that would have allowed fighters to stage a deadly invasion of Israel like Hamas's October 7 massacre, as Hezbollah originally planned.[57]

iv. Sirens Did Not Reflect Specific Threat Types

Crucial, life-saving Israeli civilian warning sirens to notify civilians of imminent or ongoing projectile attacks are no longer suited for the current threat matrix. Israel has yet to update its warning systems and emergency procedures to address the rising drone threat, and its sirens issue the same sound for rocket and missile attacks, on the one hand, and drone attacks on the other.

Recognizing this feature of the Israeli response to drone attacks, Hezbollah routinely launched missiles and drones simultaneously to interfere with Israel's civilian alert systems and procedures. Currently, in the event of a missile or rocket attack, standard Israeli procedure is for individuals to duck beneath cover if they are outdoors, or indoors and cannot reach adequate shelter quickly. While an effective approach to protect oneself from missile and rocket shrapnel, drones can loiter in the air and then strike targets with high precision, creating greater urgency for civilians to reach a fortified bunker. Despite this, Israel has not disaggregated the warning sirens for each type of attack, nor developed a third type of siren in the event of a combined attack.

IV. The "Typhoon Doctrine" for Border Defense

Israel cannot afford to ever again encounter a strategic surprise on its borders, requiring its leaders to fundamentally develop and implement a new border defense doctrine to reflect the nature of new threats; protect against the multitude of possible means of incursions across domains; ensure Israel has the capacity to respond flexibly and efficiently to a variety of operational scenarios; and leverage the strong U.S.-Israel security relationship to efficiently and effectively secure the borders. Named for its dynamic and forceful nature, a new "Typhoon Doctrine" reflects the multidirectional responses required to confront modern asymmetric border threats.

Like a typhoon quickly gathering momentum and crashing against the coastline, this doctrine would involve Israeli forces, operating within a modular force structure and at a high degree of readiness, being capable of surging into a conflict zone from all directions. The visual metaphor of a typhoon signifies the doctrine's bedrock premise: enabling troops to negate border threats rapidly and with decisive force. Under the Typhoon Doctrine, border units would be able to rapidly reposition or expand in size, allowing the IDF to scale up its force posture quickly and launch overwhelming counterattacks. Israel should adopt this more flexible, interconnected border security doctrine in light of the rigid pre-October 7 border security concept's linear and compartmentalized nature. By transforming border defense into an active, highly redundant, and malleable system, adopting the proposed doctrine would reshape IDF border security tactics and enhance Israel's readiness against current and future adversaries along its borders.

A. Planning for New Threat Scenarios

Israeli planning for new threat scenarios must factor in the lessons of October 7, Israel's subsequent wars with Hamas and Hezbollah, and repeated projectile attacks from Iran's other regional proxies and Iran itself. Unlike Israel's pre-October 7 doctrine, the Typhoon Doctrine would account for the possibility of simultaneous attacks on multiple borders via land, air, sea, and underground domains. It would prepare soldiers to counteract broad border assaults aiming to cause mass casualties and damage over a broad geographic area and over a timeframe ranging from hours to a few days. But while future border security doctrines must prepare Israel for another attack like October 7, 2023, they must also be flexible so that any future threat, not just another October 7, can be handled swiftly.

B. Detecting Threats

Immediate, preemptive threat detection lies at the very core of the Typhoon Doctrine, forming the backbone of a border defense system that would remain one step ahead of enemy planning. Employing a diverse mix of intelligence collection channels, intelligence fusion centers, and cutting-edge tunnel detection methods, the IDF can equip itself to spot and defuse threats before they spiral out of control. By blending these innovative approaches, Israel can restore and strengthen its border security.

i. Spreading Intelligence Resources More Equitably

To detect the full range of border threats and adversary plans, Israel must more equitably allocate its resources across domains of intelligence collection, with a particular focus on HUMINT to mitigate its overdependence on cyber intelligence and SIGINT capabilities. Diversifying its resources to strengthen HUMINT collection would provide Israel complementary insights into its other intelligence collection means and reduce the risks of miscalculating enemy intentions inherent to a technology-dominant system. The lead-up to the October 7 massacre revealed the innate limitations of SIGINT and other non-HUMINT intelligence collection, as Israeli intelligence officials amassed extensive material on the attack plot but failed to connect the dots and understand that Hamas had both the capability and will to pull off such a daring assault on the Israeli homeland. Additionally, HUMINT sources can help break the mold of status-quo thinking, such as the Israeli security establishment's entrenched pre-October 7 belief that Hamas was generally pacified and more concerned with internal governance than waging war against Israel.[58] Expanding the range of intelligence sources could help prevent Israeli leaders from making wrong assumptions about adversaries and rejecting intelligence that contradicts widely-held assumptions, as had been the case before October 7, 2023.

ii. Developing Intelligence Fusion Centers

Beyond expanding the types of intelligence collected, Israel must develop a centralized intelligence-sharing platform to enable real-time analysis and distribution of intelligence to forces at every level of the IDF and Israel's three intelligence agencies: AMAN, Mossad, and the Shin Bet. The fusion centers that the United States developed after the September 11, 2001, terrorist attacks to synthesize intelligence, reverse years of bureaucratic siloing of vital information, and promote intelligence sharing between different agencies at all governmental levels provide a model for improved Israeli intelligence pooling.[59] These fusion centers pull together data from federal, state, local, and private sources to create a constantly updated picture of potential threats, breaking down communication barriers between agencies. They rely on state-of-the-art analytics and a collaborative approach to quickly sift through information, spot emerging risks, and pass along vital intelligence.

iii. Developing Innovative Tunnel Detection Technologies

Israel will also need to develop new technological means of countering underground tunnels. Israel should prioritize developing new technologies to detect, map, and neutralize terror tunnels, both near its borders and deeper inside enemy territory. Rather than believing terror tunnels no longer threaten its homeland, Israel should expect enemies to continue to exploit the underground domain to counteract Israel's advantages in other domains. Israel should work to become more adept at neutralizing tunnels in adversary-held territory, like those used by Hamas and Hezbollah to stockpile weapons, protect terrorist leaders, and ambush Israeli troops.

The IDF should take advantage of the under-construction buffer zone, a half-mile-wide "no man's land" on the Gaza side of the border, to scan for tunnels in conjunction with increased patrols.[60] It should institute similar practices along the Lebanon border, to the extent events on the ground allow. In addition, while Israel is already a world leader in tunnel defense, further research and development (R&D) and acquisition funding should prioritize emerging technologies to aid detection, such as hyperspectral satellites capable of detecting underground activity from outer space—a technology that has shown promise and attracted U.S. Department of Defense attention.[61]

C. Protection Against Infiltration

With a spotlight on three primary areas—troop presence, low sky layer defenses, and counter-tunnel abilities—the new border defense doctrine emphasizes immediate protection against large-scale attacks. While emphasizing the acute importance of delaying attacking forces, like Israel's previous border doctrine, the Typhoon Doctrine differs in that it is highly robust, with overlapping and reinforcing elements ensuring constant, effective defense and insurance against a single point of failure.

i. Increased Troop Presence on the Border

The threat of large-scale incursions across multiple border sectors requires a static perimeter defense with a significantly increased and constant troop presence along Israel's border as the first layer of protection, with readily available flexible forces capable of providing defense-in-depth support. While previously troops were stationed to match the perceived threat, Israel should presume the constant risk of a surprise border infiltration and, accordingly, deploy a force capable of deterring and responding against a massive infiltration. In particular, to create redundancies in its force posture, Israel should station fire teams, squads, and larger force elements along Israel's borders with limited intervals between them, and in sectors closer to civilian population centers.

ii. Expanded Low Sky Layer Defenses and Counter-Drone Capabilities

A core element of the Typhoon Doctrine is greater Israeli investment in, and attention to, developing ways to defend its low sky layer, particularly against drone threats. Given the vulnerabilities Hamas's use of hang gliders and motorized paragliders in the October 7 attack exposed, Israel must develop and operationalize radar systems capable of painting a more comprehensive threat picture of the low sky layer. Radar systems should have complete aerial coverage, from the atmospheric level to the low sky layer, and be able to differentiate threats even in multifaceted attacks involving a mix of drones, missiles, rockets, and unconventional aerial threats. Israel generally calibrates its radar systems to detect fast-moving, high-trajectory projectiles, highlighting the IDF's need to field new radars with greater domain awareness and train radar operators to detect a broad array of airborne threats.

Central to Israel's success will be its ability to develop and deploy cost-effective, non-kinetic methods of downing drones, rather than relying predominantly on kinetic interceptors. Though not yet operational, potential options include directed energy mechanisms, specifically lasers or high-power microwaves. Israel has already successfully used electronic warfare (EW) methods against hostile drones. Another potential leap forward would involve creating an electromagnetic wall around Israel's borders that could immediately eliminate hostile drones. Israel is presently exploring the use of such systems, while working to mitigate "friendly fire" issues that would disrupt military or civilian use of local airspace and the electromagnetic spectrum.

iii. Improved Civilian Alert Capabilities

To best help civilians once an attack begins, Israel's civilian siren systems must generate distinct siren sounds in the case of a drone attack, a missile or rocket attack, and a combined attack. Additionally, best practices for civilians in the potential line of fire should be clearly differentiated by attack type. When facing rockets and missiles—and their attendant shrapnel even if intercepted—in an attack, civilians would ideally quickly duck beneath a makeshift shelter. However, when facing a drone that can loiter above its target, it is more urgent for civilians to hide in fortified bunkers. Israel should clearly distinguish protocols for different projectile threats and advise citizens on how to optimally defend themselves in various scenarios. Israel must also update its warning systems to better indicate an attack simultaneously involving drones and other projectile threats, as well as its guidance for such incidents regarding finding cover.

Recognizing the severity of its alert system deficiencies, Israel has already made some strides toward a revamped civilian alert model. Israeli leaders are working to create a layered alert system to ensure civilians receive alerts even if they miss phone alerts or audible sirens, including utilizing Internet of Thing devices, like many household televisions, to project specific digital alerts and provide guidance.[62] Israeli planners are also working to enhance alerts' geographic accuracy using cellular broadband networks.[63] Israel should complement these efforts with more methodical alert notification and guidance, particularly to differentiate between drone, rocket, or simultaneous attacks.

D. Rapid Mobilization Capacity

An essential feature of the Typhoon Doctrine is IDF soldiers' envisioned capacity to quell cross-border attacks with rapidity, precision, and coordination at all command levels. Increasing decision-making speed and rapid deployment capabilities, and pre-positioning forward operating bases, will better allow the IDF to adapt quickly to an evolving battlefield, including large-scale incursions. This operational concept draws from the IDF's Asufa Doctrine, adopted in the 1990s to counter Syria's armored warfare doctrine but since shelved.[64] Under the Asufa Doctrine, to prepare for the prospect of a large-scale

Syrian land invasion, the IDF positioned units with specialized firepower capable of destroying high volumes of enemy armor in areas adjacent to the border.

i. Increased Decision-Making Speed

Israel's ability to defend its homeland depends on the speed of its response to threats. The IDF was slow to reach and neutralize terrorist attackers within its territory on October 7 and in the immediate days afterward, largely due to a vast C2 breakdown. The IDF must have an adequate and highly functional C2 structure to make decisions fast and deploy forces in a matter of minutes to counter any future incursion. Israel's new border doctrine must properly dictate the chain of command for ordering force deployment—as well as accounting for potential disintegrations in the chain of command and a variety of contingency scenarios—and include multiple redundancies for decision-making in rapid, unclear, and complicated situations.

ii. Rapid Deployment Capability for Offensive Forces

To respond to threats quickly, Israeli forces must have a high degree of readiness, capability to mobilize rapidly, and ability to travel quickly to any location or series of locations within Israeli borders. To this end, Israel should designate a task force charged with designing a comprehensive plan for establishing traffic routes, assembly areas, and pre-designated staging areas to ensure rapid movement of IDF personnel, vehicles, and equipment throughout Israel—and in particular border-adjacent areas—during crisis situations. The IDF and the Israeli Police should codify and consistently drill emergency response measures, both separately and in tandem. Israel must also strengthen its internal munitions supply chains to ensure troops have the necessary weapons to repel protracted attacks. This new, more adaptable force structure should enable the quick and extensive deployment of active troops to a certain sector, the rapid call-up of reservists in the immediate area, or both.

iii. Pre-Positioned Modular Operating Bases

Israel should establish a number of well-fortified prepositioned C2 centers to build out redundancies and create an insurance policy against a partial or widespread breakdown of Israel's C2, communications, and computer (C4) networks in the event of a major border incursion. The IDF should place these ready-to-go military nodes in numerous locations near its borders for its forces to activate if needed. These bases would host C2 systems that are adaptive and readily deployable—essentially a "warm," rather than "hot," C2 system—and, while generally inert, can be utilized at a moment's notice. Equipped with C4 networks capable of collating and sharing intelligence, as well as potentially military equipment, these pre-positioned operating bases would further bolster Israel's defenses.

E. Force Deployment Flexibility

The dynamic threats facing Israel require not only robust defenses but also unparalleled flexibility in force deployment to counter sudden, complex and large-scale incursions. Lessons from October 7, 2023, and Israel's subsequent multifront war demonstrate that Israel must adapt its doctrine for adversaries employing fast-paced, large-scale attacks.

i. Designing a Modular Force Structure

The key to Israel's force flexibility lies in the IDF adopting a far more modular force structure conducive to scaling and adapting to any threat at a moment's notice. The IDF must be able to deploy rapid reaction units, supported by drones, infantry fighting vehicles, and mobile artillery, to areas under threat within minutes, not hours, requiring a broader array of IDF units to be capable of responding to a serious

border incursion. To this end, designated IDF units stationed at strategic junctures across Israel should double as rapid reaction forces and be equipped with, and trained to use, advanced technology and firepower to defeat threats with overwhelming force that commanders can quickly operationalize in emergency scenarios. Multiple platforms can help advance this effort. The newly integrated Eitan armored fighting vehicle can quickly transport troops into conflict zones while under fire, as proven both in Gaza and during the Battle of Zikim, in which it drove at speeds of up to 75 miles per hour.[65] Combined with the Joint Light Tactical Vehicle (JLTV) Israel recently acquired from the United States, under the Typhoon Doctrine, IDF soldiers would be able to more rapidly respond to any ground threat on Israel's borders and defeat it with overwhelming speed and firepower.[66]

ii. Synthesizing Intelligence More Effectively

To address the multitude of possible border threats, Israel's future C2 networks under the Typhoon Doctrine would enable rapid reaction support units to quickly link battlefield intelligence with shared tracking information. Intelligence systems would autonomously pool and process large volumes of information, detect patterns, and provide actionable insights that enhance situational awareness. Leveraging this data-sharing mechanism, Israeli military leaders and intelligence officers should use artificial intelligence to aid with pattern anomaly detection, helping perceive mounting threats well ahead of time and bolstering the situational awareness—and thus combat readiness—of soldiers in the field.

iii. Deploying Flexible Firepower

The Typhoon Doctrine would also emphasize Israel's need to reliably deploy lethal fire against border threats. While Israel currently operates remote-controlled weapon stations scattered across the Gaza border, these are remotely operated by soldiers and cannot act autonomously.[67] Autonomizing these weapon stations and incorporating unmanned ground vehicles (UGVs) would provide a constant, active presence along the border to support permanently stationed troops. Israel should integrate these systems with the larger C2 framework envisioned under the Typhoon Doctrine, enabling it to engage threats either fully autonomously or with human guidance. Israel acquiring or developing new long-range artillery systems, including those with greater range, mobility, and autonomy than traditional systems, such as the platforms the U.S. Army Futures Command has urged the Department of Defense to prioritize deploying in the field, can also proactively neutralize border threats before they breach critical areas.[68]

iv. Installing More Advanced Communications Systems

Under the Typhoon Doctrine, IDF leaders away from the battle and soldiers fighting in combat would increase communication systems across commands, divisions, and domains (Air Force, Ground Forces, Navy) to best address a wide variety of threats. This enhanced communication would enable IDF troops to bring the fastest, most effective, and most efficient firepower against threats while minimizing risk to other friendly forces.

With a more robust level of communication, the IDF can more easily send the optimal number of forces to address a threat without sending too many troops to a specific area that could have been deployed to help another under-protected target. Existing systems used by countries can advance this effort. For example, the U.S. military's Android Team Awareness Kit (ATAK) enables soldiers to track, share data and communicate with, and navigate alongside, one another.[69] Encrypted communication systems such as the MPU5 radio enable live GPS feeds and data streaming, and can integrate either with individual troops or with drones and vehicles.[70]

F. Building Protection Through Greater U.S.-Israel Cooperation

In support of each of these efforts, Israel's strategic partnership with the United States remains essential to its capacity to adjust and adapt in the face of constantly changing threats. Cooperation between the two countries is more than simply a diplomatic partnership; it is a vital link defending U.S. strategic interests in the Middle East. By supporting Israel's security and national defense, the United States has helped deter and degrade their shared adversaries, most notably Iran and its proxies. By creating an environment of "no daylight" between the two countries through highly visible expedited weapon deliveries, expanded joint R&D programs, and more frequent and well-publicized bilateral exercises, U.S.-Israel cooperation can serve as the backbone of Israel's border defense strategy.

i. Expanded Joint R&D for Drone, Tunnel, and Other Emerging Threats

Israel is not only a recipient of U.S. military assistance but also a technological foundry developing cutting-edge military and dual-use innovations.[71] The United States and Israel would both benefit from increasing their technological cooperation—ensuring that each country can access and use innovative products developed by the other—as well as their investment in joint R&D to combat the drone and tunnel threats which increasingly confront the United States on its own borders.[72] For example, a joint fund to advance commercial technology that has dual military use would also further enable the U.S. and Israeli militaries to acquire capabilities without adding production burdens to the defense industrial base.[73]

ii. Expanded Joint Programs for Intelligence Fusion, Counter-Drone and Counter-Tunnel Initiatives

Greater integration of intelligence and operational capabilities between the United States and Israel is essential to address the 21st-century threat landscape. Joint military exercises like Juniper Oak and Juniper Falcon have allowed the United States and Israel to jointly enhance capabilities and, in the case of Juniper Falcon, simulate missile defense.[74] There are also collaborative programs between Israel and the U.S. Department of Homeland Security (DHS) to develop new technologies, such as the Binational Industrial Research and Development (BIRD) Foundation. The BIRD program supports, through grants, U.S.-Israeli private sector collaboration for homeland security needs.[75]

Similarly, U.S.-Israel collaboration to develop intelligence fusion centers in Israel would enable greater intelligence pooling, analysis, and dissemination at all levels of Israel's security apparatus. The United States should consider sending one or multiple DHS and intelligence community officials, as well as potentially flag officers, to Israel in order to oversee a potential Israeli fusion center pilot program and share best practices with Israeli counterparts.

Congressional funding will aid in developing American and Israeli subterranean warfare capabilities, border security measures, counter-drone methods, and emerging defense technologies, each of which would strengthen Israel's border posture to complement the Typhoon Doctrine. Congress's fiscal year 2025 National Defense Authorization Act included provisions to support these capabilities. Among these key legislative measures include funding for the United States–Israel Anti-Tunnel Cooperation program to jointly develop funding to detect, map, maneuver in, and neutralize terror tunnels; annual subterranean warfare exercises between American and Israeli military forces; a mandated Secretary of Defense briefing on U.S.-Israel counter-drone cooperation; and over $150 million in funding for joint R&D and testing of emerging defense technologies.[76]

iii. No Daylight Between the U.S. and Israeli Governments

Fostering a more visibly ironclad environment of no daylight between the United States and Israel will show that Israel has emerged from the October 7 attack and the onslaught of subsequent attacks from seven fronts stronger than ever with the United States firmly by its side. The United States must show unwavering support for Israel's right to self-defense, and the two governments must do their best to remain outwardly aligned on crucial issues such as the Iran problem set, the Abraham Accords, and border security, among others. Such cohesion supports Israeli confidence in facing existential dangers and strengthens deterrence against its enemies. The United States can enable Israel to successfully eliminate threats while reducing the length and severity of conflict by expediting weapon shipments, strengthening air defense systems, and coordinating diplomatic efforts. Publicly, and tangibly, the United States must make abundantly clear that Israel's security is synonymous with its own to project a unified front against shared enemies.[77]

iv. Expedited Weaponry and Equipment Deliveries to Israel

As became repeatedly and potently clear throughout the war, speed and efficiency in the delivery of weapons and critical defense equipment is essential in times of crisis. When Israel faced its last major invasion during the 1973 Yom Kippur War, the U.S. airlift of weapons and equipment under Operation Nickel Grass proved to be crucial in achieving Israeli victory.[78] Previous delays in U.S. weapons shipments to Israel during the Gaza conflict, such as the Biden administration's pause on sending Israel precision-guided munitions due to concerns over civilian casualties, underscore the critical importance of timely military support.[79] President Trump's decision to unfreeze critical arms packages to Israel strengthens Israeli deterrence against its adversaries and ability to further degrade them, but the United States should further expedite the delivery of weaponry that Israel needs.[80]

v. Upgraded and Replenished U.S. Arms Stockpile in Israel

U.S. mechanisms such as pre-positioning weapon platforms and lifting bureaucratic hurdles on urgent military aid can significantly enhance Israel's operational capabilities. The War Reserve Stockpile for Allies-Israel (WRSA-I) serves as a vital resource for Israel during wartime by providing it immediate access to prepositioned stocks of U.S. military supplies. As JINSA has recommended since 2020, WRSA-I replenishment must include Joint Direct Attack Munition (JDAM) tail kits, counter-drone technology, and other supplies necessary for 21st-century combat challenges.[81]

Endnotes

1. Ishaan Tharoor, "Biden's Rift With Netanyahu Grows Wider," *Washington Post*, March 5, 2024, https://www.washingtonpost.com/world/2024/03/05/biden-netanyahu-gantz/; "Hamas Hails Biden's 'Clear Changes' on Israel Policy," *Newsweek,* March 27, 2024, https://www.newsweek.com/hamas-hails-bidens-clear-changes-israel-policy-1883665.
2. Ronen Bergman et al., "Where Was the Israeli Military When Hamas Attacked?" *New York Times*, January 3, 2024, https://www.nytimes.com/2023/12/30/world/middleeast/israeli-military-hamas-failures.html.
3. Aaron Boxerman, "Israel set to raise work permit quotas for Gazans to 20,000," *Times of Israel*, March 26, 2022, https://www.timesofisrael.com/israel-set-to-raise-work-permit-quotas-for-gazans-to-20000/; Nima Elbagir et al., "Qatar sent millions to Gaza for years – with Israel's backing," *CNN,* December 12, 2023, https://www.cnn.com/2023/12/11/middleeast/qatar-hamas-funds-israel-backing-intl/index.html.
4. Briefings with the authors.
5. Itay Ilnai, "'The errors didn't begin on Oct. 7': Anatomy of an intelligence failure," *Israel Hayom*, October 6, 2024, https://www.israelhayom.com/2024/10/02/the-errors-made-by-the-idf-didnt-begin-on-october-7-an-anatomy-of-intelligence-failure/.
6. Ibid.
7. Briefings with the authors.
8. Ilnai, "The errors didn't begin on Oct. 7," *Israel Hayom*.
9. "Israel announces completion of security barrier around Gaza," *Defense News*, December 8, 2021, https://www.defensenews.com/global/mideast-africa/2021/12/08/israel-announces-completion-of-security-barrier-around-gaza/; Liam Adiv, "The Barrier and the Breach: This is How the Security Promise Worth NIS 3.5 Billion Collapsed," *Maariv*, October 7, 2024, https://www.maariv.co.il/journalists/article-1138246.
10. *Failure at the Fence*, Frontline PBS, December 19, 2023, https://www.youtube.com/watch?v=c5gKaqOrCpk, 10:30-10:35.
11. Ilnai, "The errors didn't begin on Oct. 7," *Israel Hayom*.
12. Briefings with the authors.
13. "Years of subterfuge, high-tech barrier paralyzed: How Hamas busted Israel's defenses," *Times of Israel*, October 11, 2023, https://www.timesofisrael.com/years-of-subterfuge-high-tech-barrier-paralyzed-how-hamas-busted-israels-defenses/.
14. Briefings with the authors.
15. "Israel announces completion of security barrier around Gaza," *Defense News*; Adiv, "The Barrier and the Breach," *Maariv.*
16. Roy Sharon, "A huge wall with sensors: This is what the Israel-Gaza border will look like," *Kan*, April 26, 2023, https://www.kan.org.il/content/kan-news/defense/224412/; Barbara Opall-Rome, "Israel touts 'steel dome' as answer to terror tunnels," *Defense News*, January 15, 2018, https://www.defensenews.com/global/mideast-africa/2018/01/15/israel-touts-steel-dome-as-answer-to-terror-tunnels/.
17. Lauren Irwin, "How does Israel's Iron Dome work?" *The Hill*, October 1, 2024, https://thehill.com/policy/defense/4909838-israel-iron-dome-iran-strikes/.
18. Briefings with the authors.
19. "2 jets, few plans and no clue: Probe finds air force unready and in the dark on Oct. 7," *Times of Israel*, September 12, 2024, https://www.timesofisrael.com/2-jets-few-plans-and-no-clue-probe-finds-air-force-unready-and-in-the-dark-on-oct-7/.
20. Mirit Lavi and Yael Litmanovitz, "Explainer: Civilian Defense Squads in Urban Settings," Israel Democracy Institute, December 5, 2023, https://en.idi.org.il/articles/51759.
21. Briefings with the authors.
22. Jonathan Edwards, "Paragliding Fighters Flew Into Israel. A Similar Attack Happened 35 Years Ago," *Washington Post*, October 9, 2023, https://www.washingtonpost.com/history/2023/10/09/israel-night-of-the-gliders-2023/; Adiv Sterman, "Captured Hamas operative reveals paragliding attack plan," *Times of Israel*, July 30, 2024, https://www.timesofisrael.com/captured-hamas-operative-reveals-paragliding-attack-plan/.

23. Benjamin Weinthal, "Exclusive: Hamas document reveals devious paraglider terrorism attack plan," *Fox News Digital*, August 12, 2024, https://www.foxnews.com/world/exclusive-hamas-document-reveals-devious-paraglider-terrorism-attack-plan.
24. Brig. Gen. Ran Kochav and Brig. Gen. Eran Ortal, *To Defend Israel, Rearrange the Sky*, Begin-Sadat Center for Strategic Studies, August 11, 2024, https://besacenter.org/to-defend-israel-rearrange-the-sky/, p. 3.
25. Diana Bletter, "Hezbollah's Radwan force planned to invade from this village; now the IDF controls it," *Times of Israel*, October 29, 2024, https://www.timesofisrael.com/hezbollahs-radwan-force-planned-to-invade-israel-from-this-village-now-the-idf-controls-it/.
26. Briefings with the authors.
27. Yoav Zitun, "'Tunnels like in Vietnam': Hezbollah's secret war machine thrived underneath IDF and UN watch," *Ynetnews*, October 14, 2024, https://www.ynetnews.com/article/byanc49y1l.
28. JINSA Gaza Assessment Task Force, *The October 7 War: Observations, October 2023-May 2024*, May 30, 2024, https://jinsa.org/jinsa_report/gaza-war-observations-2023-2024/, pp. 34-35.
29. Ibid.
30. Michel Wyss, "The October 7 Attack: An Assessment of the Intelligence Failings," *CTC Sentinel*, Vol. 17, Issue 9, October 2024, https://ctc.westpoint.edu/the-october-7-attack-an-assessment-of-the-intelligence-failings/.
31. Ibid.
32. Yonah Jeremy Bob, "Probing the night before: IDF investigations to shed light on October 7 massacre," *Jerusalem Post*, February 24, 2025, https://www.jpost.com/israel-news/defense-news/article-843551.
33. Amir Bohbot, "IDF failed to pass intel on Hamas's October 7 coastal raid, Navy charges," *Jerusalem Post*, January 12, 2025, https://www.jpost.com/israel-news/article-837155#google_vignette; Ronen Bergman and Adam Goldman, "Israel Knew Hamas's Attack Plan More Than a Year Ago," *New York Times*, December 2, 2023, https://www.nytimes.com/2023/11/30/world/middleeast/israel-hamas-attack-intelligence.html.
34. Bohbot, "IDF failed to pass intel on Hamas's October 7 coastal raid, Navy charges," *Jerusalem Post.*
35. Ibid.
36. "More details unveiled of IDF intel on Oct. 7 plans, consults hours before Hamas attack," *Times of Israel*, December 5, 2023, https://www.timesofisrael.com/more-details-unveiled-of-idf-intel-on-oct-7-plans-consults-hours-before-hamas-attack/.
37. "IDF detected Hamas terrorists switching to Israeli SIMs ahead of Oct. 7," *JNS*, February 26, 2024, https://www.jns.org/idf-detected-gaza-terrorists-switching-to-israeli-sims-ahead-of-oct-7/.
38. Ilnai, "The errors didn't begin on Oct. 7," *Israel Hayom*.
39. Ibid.
40. Briefings with the authors.
41. Briefings with the authors; Emanuel Fabian and Michael Bachner, "IDF: Hezbollah was ready to invade en masse after Oct. 7; we covertly raided 1,000 sites," *Times of Israel*, October 1, 2024, https://www.timesofisrael.com/idf-hezbollah-was-ready-to-invade-en-masse-after-oct-7-we-covertly-raided-1000-sites/.
42. Briefings with the authors.
43. Yonah Jeremy Bob, "October 7 probes: IDF's slow response on day of Hamas attack due to chaos, commanders' denial," *Jerusalem Post*, February 28, 2025, https://www.jpost.com/israel-news/defense-news/article-844012.
44. Shira Rubin and Loveday Morris, "How Hamas Broke Through Israel's Border Defenses During Oct. 7 Attack," *Washington Post*, October 27, 2023, https://www.washingtonpost.com/world/2023/10/27/hamas-attack-israel-october-7-hostages/.
45. Ibid.
46. Briefings with the authors; "Amid Oct. 7 bedlam, Israeli pilots instructed to use Telegram to select targets," *Ynetnews*, December 30, 2023, https://www.ynetnews.com/article/r18ekttvp.
47. Rubin and Morris, "How Hamas Broke Through Israel's Border Defenses," *Washington Post*.
48. Briefings with the authors.
49. Steven Scheer, "Hezbollah rockets hit Israel's Haifa in first direct hit to city," Reuters, October 7, 2024, https://www.reuters.com/world/middle-east/hezbollah-rockets-hit-israels-haifa-10-injured-2024-10-06/; Irene Nasser and Isaac Yee,

"Video shows damage to Netanyahu's beach house as Hezbollah claims drone attack," *CNN*, October 23, 2024, https://www.cnn.com/2024/10/23/middleeast/video-netanyahu-beach-hezbollah-drone-attack-intl-hnk/index.html.

50. "Iran Projectile Tracker," Jewish Institute for National Security of America, https://jinsa.org/iran-projectile-tracker/, accessed April 26, 2025.

51. Yoav Zitun, "This is how the Hezbollah UAV evaded detection, with fatal results," *Ynetnews*, October 15, 2024, https://www.ynetnews.com/article/sy8ttzoj1e.

52. Eti Abramov, "'We thought we were the only ones developing drones, we weren't prepared for attacks,'" *Ynetnews*, October 25, 2024, https://www.ynetnews.com/magazine/article/s1jnuotlkx.

53. Brig. Gen. Effie Defrin and Yoni Tobin, *Holding the Line: A Strategy for Securing the Philadelphi Corridor*," Jewish Institute for National Security of America, December 23, 2024, https://jinsa.org/jinsa_report/holding-the-line-strategy-for-securing-the-philadelphi-corridor/, pp. 10-11.

54. *The October 7 War: Observations, October 2023 – May 2024*, Jewish Institute for National Security of America, May 30, 2024, https://jinsa.org/jinsa_report/gaza-war-observations-2023-2024/, p. 35.

55. "IDF assesses much of Hamas tunnel network still in 'good functional state' – report," *Times of Israel*, July 8, 2024, https://www.timesofisrael.com/idf-assesses-much-of-hamas-tunnel-network-still-in-good-functional-state-report/.

56. Ibid.

57. "IDF unearths Hezbollah tunnels, weapons in southern Lebanon mosque," *Jerusalem Post*, January 24, 2025, https://www.jpost.com/israel-news/article-839076; Bletter, "Hezbollah's Radwan force planned to invade Israel," *Times of Israel*.

58. Amnon Sofrin, "The Intelligence Failure of October 7 – Roots and Lessons," *Jerusalem Strategic Tribune*, November 26, 2023, https://jstribune.com/sofrim-the-intelligence-failure-of-october-7-roots-and-lessons/.

59. "FBI Partnering with Fusion Centers to Tackle Threats," United States Federal Bureau of Investigation, April 14, 2022, https://www.fbi.gov/news/speeches/fbi-partnering-with-fusion-centers-to-tackle-threats-041422.

60. Camilla Bressange et al., "How Israel's Proposed Buffer Zone Reshapes the Gaza Strip," *Wall Street Journal*, March 16, 2024, https://www.wsj.com/world/middle-east/israel-gaza-hamas-war-buffer-zone-explained-2a7347af.

61. Courtney Albon, "National Reconnaissance Office seeks commercial hyperspectral imaging," *Defense News*, November 17, 2022, https://www.defensenews.com/space/2022/11/17/national-reconnaissance-office-seeks-commercial-hyperspectral-imaging/.

62. Seth J. Frantzman, "Smaller polygons and cell alerts: How Israel's Home Front Command honed its civilian alert system," *Breaking Defense*, February 26, 2025, https://breakingdefense.com/2025/02/smaller-polygons-and-cell-alerts-how-israels-home-front-command-honed-its-civilian-alert-system/.

63. Ibid.

64. Briefings with the authors.

65. Gil Zohar, "The Battle of Zikim Beach: The IDF Oct. 7 victory that paved the way for Gaza offensive," *Jerusalem Post*, April 29, 2024, https://www.jpost.com/israel-hamas-war/article-798929.

66. Seth J. Frantzman, "Israel to buy new corvettes, 'hundreds' of JLTVs," *Breaking Defense*, November 25, 2024, https://breakingdefense.com/2024/11/israel-to-buy-new-corvettes-hundreds-of-jltvs/.

67. "Israel Defends Gaza Border With Remote-Control Guns," *Aviation Week*, January 1, 2009, https://aviationweek.com/israel-defends-gaza-border-remote-control-guns.

68. Jen Judson, "Army artillery needs more range, mobility and autonomy, study finds," *Defense News*, March 27, 2024, https://www.defensenews.com/digital-show-dailies/global-force-symposium/2024/03/27/army-artillery-needs-more-range-mobility-and-autonomy-study-finds/.

69. Sgt. Sergio Gamboa, "Defenders ATAK system ready," United States Air Forces Central Command, December 21, 2023, https://www.afcent.af.mil/News/Article/3628231/defenders-atak-system-ready/.

70. Capt. Matthew Harrison, "MPU5 Radio: Rakkasan Tested," United States Army, May 17, 2019, https://www.army.mil/article/222056/mpu5_radio_rakkasan_tested.

71. Seth J. Frantzman, "How Israel's military is prioritizing dual-use start-ups to accelerate defense tech," *Breaking Defense*, July 28, 2023, https://breakingdefense.com/2023/07/how-israels-military-is-prioritizing-dual-use-start-ups-to-accelerate-defense-tech/.
72. Billal Rahman, "U.S. Border Agents Now Face Drone Bombs Threat: Report," *Newsweek*, February 4, 2025, https://www.newsweek.com/cartels-explosives-us-border-agents-2025721; Adam Shaw, "'Our agents are relentless': Feds shut down cross-border tunnel used by Mexican cartels for smuggling into U.S.," *Fox News Digital*, January 16, 2025, https://www.foxnews.com/politics/feds-shut-down-cross-border-cartel-tunnel-used-smuggling-us.
73. *Israel's Strategic Challenges and Security Cooperation: JINSA Generals & Admirals 2024 Program Report*, Jewish Institute for National Security of America, August 28, 2024, https://jinsa.org/jinsa_report/jinsa-generals-admirals-2024-program-report/, p. 11.
74. Yoni Tobin, "U.S. and Israel Display Combat Capabilities, But Deterrence Against Iran Still Deficient," Jewish Institute for National Security of America, July 28, 2023, https://jinsa.org/jinsa_report/us-israel-display-combat-capability-deterrence-against-iran/; Emanuel Fabian, "IDF launches joint air defense, cyber drill with US Central Command," *Times of Israel*, February 12, 2023, https://www.timesofisrael.com/idf-launches-joint-air-defense-cyber-drill-with-us-central-command/; Stavros Atlamazoglou, "Juniper Falcon '21: Where Missile Defense Meets Remote Warfighting," *National Interest*, March 1, 2021, https://nationalinterest.org/blog/reboot/juniper-falcon-21-where-missile-defense-meets-remote-warfighting-178828.
75. Shoshanna Solomon, "U.S.-Israel fund to invest in 3 joint homeland security R&D projects," *Times of Israel*, January 13, 2020, https://www.timesofisrael.com/us-israel-fund-to-invest-in-3-joint-homeland-security-rd-projects/.
76. Matthew Kenney, "Key Middle East Provisions in the Fiscal Year 2025 National Defense Authorization Act," Jewish Institute for National Security of America, December 17, 2024, https://jinsa.org/jinsa_report/key-provisions-2025-ndaa/.
77. *No Daylight: U.S. Strategy if Israel Attacks Iran*, Jewish Institute for National Security of America, July 24, 2023, https://jinsa.org/jinsa_report/no-daylight-us-strategy-if-israel-attacks-iran/.
78. Jason Maoz, "Thirty-Six Years Ago Today, Richard Nixon Saved Israel—But Got No Credit," *Commentary*, October 6, 2009, https://www.commentary.org/articles/jason-maoz-2/thirty-six-years-ago-today-richard-nixon-saved-israel-but-got-no-credit/.
79. Anne Flaherty and Chris Boccia, "U.S. withheld bomb shipment to Israel out of fears it could be used in Rafah," *ABC News*, May 8, 2024, https://abcnews.go.com/Politics/biden-administration-pauses-ammunition-shipments-israel-us-officials/story?id=109993270.
80. Blaise Misztal and Ari Cicurel, "President Trump must use every tool to speed up arms for Israel," *Breaking Defense*, February 25, 2025, https://breakingdefense.com/2025/02/president-trump-must-use-every-tool-to-speed-up-arms-for-israel/.
81. *Anchoring the U.S.-Israel Alliance: Rebuilding America's Arms Stockpile in Israel,* Jewish Institute for National Security of America, June 10, 2020, https://jinsa.org/jinsa_report/anchoring-the-u-s-israel-alliance-rebuilding-americas-arms-stockpile-in-israel/.


JINSA
The Jewish Institute for
National Security of America