Signal From Noise

October 26, 2023

Private-Sector Intelligence After Israel-Gaza

"If you know your enemy and you know yourself, your victory will not be in doubt." ~ Sun Tzu

There seems to be widespread agreement that the horrific attacks on Israel on October 7, 2023 could only have taken place after a catastrophic intelligence failure. The attacks were so numerous and varied that they required months of planning, the involvement of many people, and the procurement of significant quantities of weapons and equipment – the coordination of which would have required extensive communication and funding. The consensus is that much of this should have been noticed by Israeli intelligence, enough to provide sufficient warning to the country's military and policymakers.

The fact that Israel appears to have been taken unaware surprised many who had long seen Israel's intelligence capabilities as among the best in the world. This assessment of failure comes from many experts in the field, perhaps none more qualified to comment than Major General Aharon Haliva, head of the Israeli Defense Force's Military Intelligence Directorate, also known as Aman. "The beginning of the war was an intelligence failure," Maj. Gen. Haliva said in a communication with subordinates. "The Military Intelligence Directorate, under my command, failed to warn of the terror attack carried out by Hamas. We failed in our most important mission, and as the head of the Military Intelligence Directorate, I bear full responsibility for the failure."

Ronen Bar, director of Israel's Shin Bet domestic intelligence agency, expressed a similar opinion. "Despite a series of actions we undertook, regrettably, on Saturday, we failed to provide a sufficient warning that would have allowed us to thwart the attack. As the head of the organization, the responsibility for this falls on me," Bar said.

That is not to claim that intelligence alone was to blame for the country's failure to stop the attacks. Some pundits have argued, for instance, that the root of the country's vulnerability was the belief that Hamas had evolved, at least partly, beyond its terrorist roots and into an organization that is more interested in governance and the well-being of the people it governs.

Nevertheless, in the months and years to come, experts and analysts will surely be conducting in-depth, multi-faceted investigations into the nature of this intelligence failure. They will try to discern what went wrong, what could have been done to prevent it, and what should be done to improve Israel's intelligence capabilities.

Intelligence agencies in other countries, including the United States, will also likely consider what lessons can be learned from Israel's failure to provide adequate actionable warning of Hamas's plans. Was not enough intelligence gathered? Was the intelligence gathered not given the attention it deserved, or somehow interpreted incorrectly? As Amy Zegart, a noted intelligence expert, put it, "Answering these questions will also be essential for the United States. In today's complex and uncertain threat landscape, American intelligence has never been more important. Washington must study Israel's failures so that it does not repeat them."

Intelligence is gathered through four primary methods, and most intelligence contains information compiled from more than one source. It is unusual for an intelligence agency or government to rely on any single source exclusively. Thus, investigators will undoubtedly want to examine each facet of Israel's intelligence-gathering operations.

To be clear: this piece does not aim to do the work of experts in dissecting Israeli intelligence in the aftermath of one of the most tragic events in the country's history. It merely posits that private-sector companies with expertise in one or more aspects of intelligence gathering and analysis might be called upon to help do so.

Human intelligence (HUMINT)

As the term suggests, this refers to information obtained from human sources. This includes information cultivated from cooperative informants, observations provided by trained agents, interrogations of prisoners/detainees, or conversations with witnesses.

There does not seem to be a consensus as to whether Israel had enough human intelligence sources in Gaza. Certainly, experts agree that cultivating such sources would have been extremely difficult: anyone involved with such an effort would be placing themselves – and likely their families – at extreme risk. The possibility therefore exists that Israel had few sources of human intelligence within Hamas or any of the other entities Hamas is believed to work with. Still, others insist that despite the difficulty, Israeli intelligence had managed to cultivate an extensive network of HUMINT sources within Gaza, but had chosen to rely too heavily on technology-based sources of information gathering.

In either case, a close examination of Israel's HUMINT efforts is sure to be conducted, and recommendations for improvement will be made. Allied intelligence services will be following along closely, seeking to apply any lessons learned to their own organizations.

Human-intelligence gathering is a highly specialized skill, and training for such activities is almost exclusively the purview of government entities. Nevertheless, a small number of private-sector companies have positioned themselves to provide useful outside opinions and advice, and several are publicly traded. They include Booz Allen Hamilton ($BAH) and CACI International ($CACI).

Geospatial/imagery intelligence (GEOINT/IMINT)

Geospatial information includes knowledge about geographic and manmade features of the Earth, generally gathered from satellite imagery, aerial photography, maps, and similar sources. This includes real-time information.

The Hamas attack involved assaults by air, land, and sea. The planning involved smuggling or manufacturing large quantities of weapons, and one source cited by Reuters as being close to Hamas claimed that some of the preparations involved constructing a mock kibbutz within Gaza and having fighters practice storming it. (A similar claim was made by the Associated Press.)

The land assault was carried out after first disabling enough of Israel's extensive network of remote surveillance capabilities (including but not limited to cameras and the cellular communications towers they use to send imagery to analysts) to avoid immediate detection. Afterwards, large numbers of individuals destroyed the fence that separates Gaza from Israeli territory and surged over the border.

That all of this was possible despite what is widely seen as Israel's sophisticated, advanced, and expensive IMINT/GEOINT platform suggests the possibility that Hamas was able to defeat Israel's systems before and during its offensive. There are other possibilities as well, but this one will also be carefully examined in the months and years to come. Companies that might be able to help include Elbit Systems ($ESLT) and Northrop Grumman ($NOC).

Signals intelligence (SIGINT)

One way to obtain intelligence is through surreptitious interception or observation of electronic signals. This can include electronic communications, such as intercepted radio transmissions, electronic messages, or satellite communications. It also includes non-communicative electronic information, such as signals generated through the activation of radar systems and telemetry from missile tests.

Israel's SIGINT capabilities are renowned, considered at least as good as what the U.S. National Security Agency can provide. It is no coincidence that NSO Group, the company that created the well-known Pegasus spyware, employs numerous veterans of the Israeli Defense Force's famed Unit 8200.

Nevertheless, a thorough review of Israeli intelligence would necessarily include an attempt to identify potential improvements in the country's SIGINT capabilities. Companies potentially capable of providing relevant expertise include Northrop Grumman ($NOC) and BAE ($BAESY).

Analytics

Days before the attack, Israel's national security adviser, Tzachi Hanegbi, downplayed the threat presented by Hamas. "Hamas is very, very restrained and understands the implications of further defiance," he said during a radio interview. Admitting to a "mistake" on his part and "all those making intelligence assessments," Hanegbi later said that "we really believed that Hamas learned its lesson from [losses it incurred in 2021.]"

Hindsight is easy, but another possibility for intelligence experts to examine is whether Israel had the information needed to figure out that Hamas was planning a major attack, but simply failed to put the pieces of the puzzle together. Dr. Michael Milshtein, a retired colonel who once oversaw the Department for Palestinian Affairs for IDF Military Intelligence, told the AP afterwards, "We knew about the drones, we knew about booby traps, we knew about cyberattacks and the marine forces. The surprise was the coordination between all those systems."

For example, any dissection of how Hamas was able to prepare for this attack will look at the group's financing. Jessica Davis, a terrorism, intelligence, and financing expert for the Transnational Threats Project, estimates that "[costs for the] October 7 attacks will undoubtedly cross the million-dollar mark, probably by a wide margin," arguing that "the fact that Israeli intelligence, as well as the international intelligence community (specifically the Five Eyes intelligence-sharing network), missed millions of dollars' worth of procurement, planning, and preparation activities by a known terrorist entity is extremely troubling."

Experts might also wish to look at whether there was a better way to analyze individual threats from ground-level surveillance footage. Some analysts noted that it was difficult to differentiate between Hamas members gathering near the Gaza border because they happen to live nearby – the territory is quite small and less than four miles wide at some points – or for some nefarious purpose.

As noted above, a Reuters source reported that Hamas had created a mock settlement which its fighters practiced storming. Far from positing any IMINT inadequacies, the source claimed: "Israel surely saw them but they were convinced that Hamas wasn't keen on getting into a confrontation." And yet there is another possibility still.

Some outside intelligence experts have suggested that the problem might not have been inadequate intelligence, but rather too much of it. Jake Williams, a former National Security Agency hacker and instructor at the Institute for Applied Network Security, described it thusly: "Intelligence in an environment like Israel isn't finding a needle in a haystack – it's finding the needle that will hurt you in a pile of needles." He elaborated: "I feel confident that there are always Hamas operatives talking about credible plans to attack the IDF. So Israel can't respond with force to every threat, even every credible one. They'd be at a heightened state of alert or actively engaged all the time, and that's probably actually worse for security."

This is where analytics can help. Similar to how businesses maximize their use of large datasets, intelligence agencies can use analytics to help sort through large quantities of disparate forms of data to identify useful trends, patterns, and anomalies. Companies with expertise in intelligence analytics include Palantir Technologies ($PLTR) and IBM ($IBM).

Companies of Interest: Diversified Intelligence

Booz Allen Hamilton ($BAH)

Once dubbed "the world's most profitable spy organization" by Bloomberg, Booz Allen is a management consulting firm with a diverse and deep array of intelligence-related offerings, including a broad range of expertise in human intelligence, electronic intelligence, geospatial/imagery intelligence, and intelligence analytics. Its client base includes agencies throughout the U.S. intelligence community, as well as intelligence and military entities in the Middle East, including in Israel and Saudi Arabia.

BAE Systems ($BAESY)

BAE is one of the largest defense companies in Europe, and a major contractor to the U.S. Department of Defense. In addition to being a major manufacturer of ammunition, artillery systems, missile launchers, and armored combat vehicles, BAE boasts expertise in electronic warfare and cybersecurity. Its intelligence capabilities span multiple disciplines – HUMINT, SIGINT, GEONIT, and the relatively new field of Open Source Intelligence. The company's intelligence analytics offerings feature AI and machine-learning capabilities that enable real-time integration of data from disparate sources and in varying formats.

CACI International ($CACI)

Founded by two alumni of Rand Corporation, the company provides expertise on aviation systems, health enterprises, and data analysis. In the past, its executives and directors have included high-ranking former CIA and NSA personnel, as well as former Cabinet members. The firm's client list is widely reported to include numerous agencies in the U.S. intelligence community and U.S. military. CACI provides operational support, analytics, and technical advice on an array of HUMINT, SIGINT, and GEOINT operations and initiatives.

Leidos ($LDOS)

Leidos provides analytical tools that help to integrate GEOINT, SIGINT, and HUMINT. The company has been working with clients in the intelligence community for more than four decades, assisting in tactical planning, threat assessment and simulations, and SIGINT systems deployment.

Companies of Interest: Intelligence Analytics

Palantir Technologies ($PLTR)

Palantir was founded as a way to help intelligence agencies make the best use of their data, particularly as part of counterterrorism efforts. Although its data-analytics offerings and client base have since expanded significantly, its government contracts continue to generate the lion's share of its revenue. Palantir's offerings help intelligence organizations integrate large volumes of disparate data types, including streaming data, in real time. The company is regarded as a leader in the field of AI and machine learning.

IBM ($IBM)

IBM counts a number of U.S. intelligence and security agencies as clients, including the NSA and CIA. The company's Watson AI and data-analytics capabilities are reportedly used to help prevent cyberattacks and to analyze large datasets.

Companies With Specialized Intelligence Expertise

Northrop Grumman ($NOC)

Northrop Grumman is a major aerospace, defense, and intelligence contractor, though it also has private-sector customers and clients. Within the intelligence segment, its offerings include IMINT systems – both through satellites and through manned and unmanned aircraft. It is also active in the cyberwarfare segment.

Elbit Systems ($ESLT)

Elbit is a diversified Israeli defense contractor with expertise in intelligence, surveillance, and cyberwarfare solutions.

Maxar Technologies ($MAXR)

Maxar is a global leader in satellite imagery and geospatial data and analytics. The company provides a wide range of GEOINT services to government and commercial customers, including satellite imagery, aerial photography, and radar data.

BlackSky ($BKSY)

BlackSky is a geospatial intelligence company that provides real-time satellite imagery and analytics to government and commercial customers. The company's platform provides access to a wide range of GEOINT data, including satellite imagery, video, and analytics.

We close by reiterating in the strongest terms possible that the above is not meant to speculate on the specifics of what went wrong with Israeli intelligence preceding Hamas's brutal attack. Instead, we seek to identify some of the companies in the private sector that might help the United States and its allies answer this question and help to prevent similar catastrophes from happening again. As always, *Signal From Noise* is meant to serve as a starting point for further investigation, rather than as an investment recommendation.

We encourage you to also explore our full *Signal From Noise* library, which includes deep dives on the path to automation, the world of Big Data, and the ever-increasing global water crisis.

Disclosures

This research is for the clients of FS Insight only. FSI Subscription entitles the subscriber to 1 user, research cannot be shared or redistributed. For additional information, please contact your sales representative or FS Insight at fsinsight.com.

Conflicts of Interest

This research contains the views, opinions and recommendations of FS Insight. At the time of publication of this report, FS Insight does not know of, or have reason to know of any material conflicts of interest.

General Disclosures

FS Insight is an independent research company and is not a registered investment advisor and is not acting as a broker dealer under any federal or state securities laws.

FS Insight is a member of IRC Securities' Research Prime Services Platform. IRC Securities is a FINRA registered broker-dealer that is focused on supporting the independent research industry. Certain personnel of FS Insight (i.e. Research Analysts) are registered representatives of IRC Securities, a FINRA member firm registered as a broker-dealer with the Securities and Exchange Commission and certain state securities regulators. As registered representatives and independent contractors of IRC Securities, such personnel may receive commissions paid to or shared with IRC Securities for transactions placed by FS Insight clients directly with IRC Securities or with securities firms that may share commissions with IRC Securities in accordance with applicable SEC and FINRA requirements. IRC Securities does not distribute the research of FS Insight, which is available to select institutional clients that have engaged FS Insight.

As registered representatives of IRC Securities our analysts must follow IRC Securities' Written Supervisory Procedures. Notable compliance policies include (1) prohibition of insider trading or the facilitation thereof, (2) maintaining client confidentiality, (3) archival of electronic communications, and (4) appropriate use of electronic communications, amongst other compliance related policies.

FS Insight does not have the same conflicts that traditional sell-side research organizations have because FS Insight (1) does not conduct any investment banking activities, and (2) does not manage any investment funds.

This communication is issued by FS Insight and/or affiliates of FS Insight. This is not a personal recommendation, nor an offer to buy or sell nor a solicitation to buy or sell any securities, investment products or other financial instruments or services. This material is distributed for general informational and educational purposes only and is not intended to constitute legal, tax, accounting or investment advice. The statements in this document shall not be considered as an objective or independent explanation of the matters. Please note that this document (a) has not been prepared in accordance with legal requirements designed to promote the independence of investment research, and (b) is not subject

to any prohibition on dealing ahead of the dissemination or publication of investment research. Intended for recipient only and not for further distribution without the consent of FS Insight.

This research is for the clients of FS Insight only. Additional information is available upon request. Information has been obtained from sources believed to be reliable, but FS Insight does not warrant its completeness or accuracy except with respect to any disclosures relative to FS Insight and the analyst's involvement (if any) with any of the subject companies of the research. All pricing is as of the market close for the securities discussed, unless otherwise stated. Opinions and estimates constitute our judgment as of the date of this material and are subject to change without notice. Past performance is not indicative of future results. This material is not intended as an offer or solicitation for the purchase or sale of any financial instrument. The opinions and recommendations herein do not take into account individual client circumstances, risk tolerance, objectives, or needs and are not intended as recommendations of particular securities, financial instruments or strategies. The recipient of this report must make its own independent decision regarding any securities or financial instruments mentioned herein. Except in circumstances where FS Insight expressly agrees otherwise in writing, FS Insight is not acting as a municipal advisor and the opinions or views contained herein are not intended to be, and do not constitute, advice, including within the meaning of Section 15B of the Securities Exchange Act of 1934. All research reports are disseminated and available to all clients simultaneously through electronic publication to our internal client website, fsinsight.com. Not all research content is redistributed to our clients or made available to third-party aggregators or the media. Please contact your sales representative if you would like to receive any of our research publications.