BESA
The Begin-Sadat Center
for Strategic Studies
Bar-Ilan University
PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

The "Seven Sins" of Intelligence: A Basis for Discussion

by Col. (res.) Shay Shabtai

BESA Center Perspectives Paper No. 2,279, May 12, 2024

EXECUTIVE SUMMARY: In the wake of the massive intelligence failure of October 7, fundamental changes will have to be made to Israeli national security doctrine. The intelligence community is obliged to improve its early warning capabilities – not merely in an attempt to prevent another great failure of the kind that might occur once in 50 years, but to improve its ability to contribute to the ongoing security effort. Israeli intelligence committed seven "sins" in the lead-up to October 7 that will have to be examined closely if the required changes are to be put in place. Those "sins" are politicization, certainty, preoccupation with cyber, targeting, professionalism, understanding, and risk management.

Israel's intelligence community is among the most powerful in the world, certainly relative to the size of the country. Early warning is the historical cornerstone and a key element of Israel's security doctrine. It failed catastrophically on October 7.

The early warning pillar was developed to bridge the inherent tension between Israel's relatively small size, which has resulted in limited access to resources it can allocate to security needs, and the magnitude and intensity of the security threats with which it has always to deal. These threats have grown over the years from knife attacks to the threat of a nuclear attack; from the threat of terrorism in the streets to the threat of precision weapons launched from a distance; and from the threat of lone wolves to threats from regional powers and even superpowers.

The main problem with early warning is that it requires not only an understanding of the present but a capacity to predict the future. The assessment of future events, when they concern human behavior, is always marked by great uncertainty and contains a built-in margin of error.

A quick analysis of the professional literature dealing with business strategies reveals that "outstanding organizations" only manage to achieve two-thirds of their long-term goals. If we translate this to intelligence work, this means that even those intelligence organizations that are the most outstanding in terms of information-gathering, analysis and understanding - even those that conduct the kind of in-depth soul-searching I advise in the second part of this article - will be wrong in their estimates of the future a third of the time.

The statement, "Once every 50 years, intelligence will be wrong in a way that leads to a severe blow to national security" exposes the need for a fundamental change in Israel's security doctrine. Unlike the first decades of the State of Israel's existence, when early warning was adopted as a central component, Israel is now in a situation where it is possible to increase the security margin. Israel is an economically and technologically strong country, both in absolute terms relative to its size and relative to its environment.

If the resources allocated to date provide a quality response to the country's security challenges, then a wise increase in resources would create a level of security that reduces the problematic reliance on early warning. This resource increase should be based on careful risk management and should contain internal and external controls.

The security margin can be based on a clear technological and operational advantage over both known enemies and possible adversaries; broad and effective integrated land maneuvering capabilities, which are the insurance policy of national existence; accurate targeting and countering capabilities of both near and distant threats; aggregate power that creates deterrence and is a basis for effective international and regional alliances; use of security strengths as a lever to promote the solid economic base and national infrastructure; and a base of agreed values that strengthens vital national cohesion.

One of the more effective uses of additional resources would be the further development of a strong intelligence community. This would form the basis for the detection of threats, accurate intelligence for targeting and operations, and a base cooperation with international and regional alliances. It would also provide an improved early warning capability that would allow at least two-thirds of the threats to be predicted in advance and thwarted ahead of time.

To develop such an intelligence community, we must draw relevant lessons from the failure of early warning on October 7. I suggest that there were seven failures, or "sins," of intelligence that led to the catastrophe. The following is intended to open the conversation, not end it, and support analysis of the reasons for what happened and the lessons learned.

It is possible that some of the ideas raised here will turn out to be incorrect, but in this writer's opinion, they should all be discussed. These failures are aimed at different levels of the intelligence work: from the decision-making at the top of the pyramid to the junior levels of collection and research, which are sometimes the most important, as can be learned from those who did think differently and tried to warn of what was to come.

"Sin" #1: Politicization. The year before the failure was not good for the intelligence community in this regard. The heads of that community found themselves in the midst of a political storm but seemed unable to steer the ship. They sent letters and early warnings up to the political level, but the necessary conclusions were not subsequently drawn by that level. Early warning of a change in the enemy's intentions should have led to an obsessive preoccupation with operational early warning, but this did not happen. There were too many briefings by senior intelligence community members to the media on political matters, whether or not they were identified as such, which interfered with proper professional functioning.

Another significant issue was the failed handling of the refusal/non-volunteering initiatives. The failure to eliminate them decisively harmed the functioning of the intelligence echelons, shook them, and diverted attention away from the preoccupation with early warning.

Another relevant matter was the political statements made by former senior officials in the name of alleged intelligence analysis, which did not help.

"Sin" #2: Certainty. Predicting the future is inherently uncertain. It requires extreme caution. Alternatives must be presented, but they can never cover the entire spectrum of possibilities. A leading alternative must be determined and other alternatives evaluated according to their decreasing probability. Possible turning points need to be considered, together with the risks arising from their realization. There must be transparency with regard to the uncertainty levels of those alternatives and risks.

All of this has been eroded in recent years, at least as far as the assessment of Hamas in Gaza is concerned. This is the result of three main problems: excessive confidence in the assessment, which resulted in a failure to recognize how the adversary had changed; an effort to satisfy the demands of decision-makers and security system officials for higher certainty through an improbably precise description of a future reality; and the desire to give greater validity to the policy and operational recommendations of the intelligence.

"Sin" #3: Cyber. In recent years, cyber has occupied the attention of the intelligence community to a greater and greater extent. This is reflected in three characteristics: the focus of attention on cyber operations; shifting the balance sharply towards cyber at the expense of classic sigint, humint and visint; and an increased preoccupation with cyber threats to the State of Israel and defense that drew resources from other threats. Adapting the intelligence system to new capabilities is a welcome process, and the various efforts in the cyber domain have resulted in significant intelligence and operational achievements. The claim, to be clear, is that there was an imbalance in terms of the distribution of resources and quality personnel and their transfer from other intelligence tasks to cyber tasks.

"Sin" #4: Targeting. In recent years, the attention of intelligence personnel dealing with analysis and assessment has been directed toward dealing with operations. The greatest attention has been given to research that creates targets. There is no doubt that the contribution of accurate intelligence to operational activity - with an emphasis on accurate fire - that effectively damages the adversary and reduces collateral damage fulfills a vital need. The problem is that the focus on targeting

resulted in the breaking down of the enemy into tiny elements, which resulted in a decreased ability to analyze that enemy as a strategic and operational entity. In addition, the preoccupation with promoting recommendations for policy and operational action and participating in their implementation seriously damaged the ability to perform an assessment detached from the perspective of the "blue side" regarding the adversary's intentions and capabilities. Despite the resource challenge, there is a need to maintain a dedicated group of intelligence personnel to deal exclusively with analysis and evaluation of the "red side."

"Sin" #5: Professionalism. In recent years, the professionalism of analysis and assessment has been eroded in two areas that are critical to early warning, both of which failed on October 7: a political-strategic analysis of the perceptions, strategies and intentions of the other side; and a professional analysis of its military organizations and operations. This erosion caused Israel to view its adversaries, Hezbollah and Hamas, as armies rather than state-level entities. An analysis of the leaked NCO V from 8200 might indicate that looking at Hamas as a military system, rather than as a terrorist organization capable of only local and limited operations, could have led to a more substantial reference to the raid plan known as the "Wall of Jericho." A reference of this kind was required in the fields of both collection and analysis for early warning and should have led to other conclusions and a different preparation by the Southern Command and the Gaza division against the potential threat.

"Sin" #6: Understanding. In recent years, intelligence organizations has given less respect to expertise from the fields of humanities and social sciences, which are in fact the basis of intelligence analysis and assessment. This eroded Israel's understanding of the language and culture of the other side. In-depth knowledge of the history of the Middle East is required, as is the use of theoretical tools from fields in the social sciences, such as international relations, comparative politics, sociology, anthropology, economics, and more. The "best for technology" approach has replaced the "best for analysis and assessment" approach. Technological tools for language translation and the monitoring of human behavior were seen as substitutes for the knowledge and deep understanding once required of intelligence analysts. But rather than strengthen human ability, these tools actually weakened it and eroded the required ability for analysis and assessment.

"Sin" #7: Risk management. The senior intelligence officials committed to providing early warning with high certainty did not present its limitations and inherent risks, especially after the strategic early warnings that they allegedly passed on to the political level. Based on leaks from internal forums, it seems that they even saw it as a substitute for deploying forces and maintaining alertness. However, the problem of assessing and preparing for risk is consigned not only to intelligence officials but also to political and military decision-makers. An orderly risk analysis could have shown that the deployment of the IDF on the Gaza border was insufficient in the face of scenarios that were broader than a few raids at once, especially in the face of the dangerous course of action (DPA) of implementing the "Wall of Jericho" plan. The IDF and the decision-makers above it need to substantially improve the process of risk management.

The "seven sins" presented above represent a proposal for the analysis of the debriefings that will occur on the intelligence failure that led to October 7. They are critical to a re-strengthening of the analysis and assessment capacities that are the basis of early warning and that remain important components of the Israeli security doctrine.

Col. (res.) Shay Shabtai is a senior researcher at the BESA Center and an expert in national security, strategic planning, and strategic communication. He is a cyber security strategist and a consultant to leading companies in Israel.