NATIONAL INSTITUTE FOR PUBLIC POLICY

INFORMATION SERIES

Intelligence and the "Unknown Unknown": How to Prepare for and Recover from Fundamental Surprise

Dr. Shmuel Bar
Dr. Shmuel Bar heads Shmuel Bar Research and Analysis, an independent boutique analytic group that specializes in the Middle East and Russia and is CEO of IntuView Ltd. He is a former senior officer in the Israeli Intelligence.

Introduction

In "Alice through the Looking Glass," Alice complains to the White Queen: "One can't believe impossible things." The Queen retorts: "I daresay you haven't had much practice … when I was your age, I always did it for half-an-hour a day… sometimes I've believed as many as six impossible things before breakfast."[1]

The daily routine of "believing (or at least thinking of) six (or more) impossible things before breakfast" is one of the most difficult but also neglected tasks of strategic intelligence. Much has been written on the cause of strategic surprise and ways to minimize—if not to prevent—it. But the "post-surprise surprise" can be no less challenging. Since strategic surprise cannot be fully avoided, intelligence communities must develop methodologies and techniques for "*contingency intelligence*" to cope with the aftermath of such unexpected "Black Swan,"events, to recover from them and to generate intelligence to deal with their consequences. This is the subject of this essay.

"Situational" vs. "Fundamental" Surprises

Many famous strategic surprises seem to have been a bolt out of the skies. Such were Pearl Harbor and the terrorist attacks of September 11, 2001 and October 7, 2023. In many cases, warning signals were available but were not given sufficient attention. But many others were real "Black Swans" - threats that were not in the scope of the intelligence communities' threat perception. The "streetlight effect"[2] tends to be self-reinforcing; an intelligence service issues requirements based on what it is aware of (under the "streetlight"); therefore, the information it gets is from that context and strengthens the perception.

Surprises from a known threat—or "situational surprises"—are those that were not "impossible" but were considered improbable in the prevailing circumstances or timeframe. In the more severe cases of surprise, the "Black Swan" is linked to an entity or theatre that was not previously in the intelligence requirements. These are "fundamental surprises"—scenarios that were never considered at all as possible.[3] The effects of a "fundamental surprise" tend to be more long-term; both recovery of an intelligence service from such a surprise and the need for "customization" and adaptation of collection and analytic capabilities extend far past the initial response.

Strategic Surprises—A Balance Sheet

One may argue that true "fundamental surprises" should be rare. The United States *should have* taken into account a threat from Japan, given the relations between the countries, U.S. sanctions on Japan and Japan's aggression in East Asia; Pearl Harbor was, therefore, clearly a result of misreading of signals. The same is true for the 1973 Yom Kippur War—Israeli intelligence had ample intelligence that indicated that Egypt and Syria intended to attack and subjugated the intelligence to a preconception (the "Conceptsia") that ruled out such an attack. The attack of October 7, 2023—fifty years later—is another case in point.

On the other hand, the use of the atomic bomb against Japan was justifiably a "fundamental surprise" for the Japanese leadership. Japan was aware of the technology behind the atomic bomb but deemed it infeasible and certainly did not expect the Americans to achieve it and to use it. September 11 may also be seen as a "fundamental surprise." The scenario of using hijacked civilian planes as weapons was not included in U.S. intelligence requirements.[4]

There are mitigating explanations for fundamental surprises; no intelligence community—even of a world superpower—can effectively cover all possible scenarios in all possible theatres, lest a threat emerge from those areas. In many of these cases, however, the "fundamental surprise" does not end with its first blow; it continues to "surprise" as the attacked country finds itself without the intelligence infrastructure for unfamiliar theatres and geographic and human terrains.

The strategic surprise of Pearl Harbor has been well documented over the years. However, the "bounce-back" of U.S. intelligence to a focus on the Japanese adversary is also of interest. U.S. intelligence coverage of Japan was almost exclusively reliant on signals intelligence

(SIGINT), but before the war, U.S. SIGINT relied on a handful (until 1937 only one) of Japanese linguists.[5] By the Fall of 1941, the communications intelligence (COMINT) services in the U.S. military had small programs for exploitation of Japanese communications.[6] After Pearl Harbor, U.S. intelligence focused on Japan, but no amount of intercept could be useful, however, without Japanese linguists with an ability to translate and comprehend the contents. However, the recruitment of Japanese linguists was hampered by the suspicion towards American citizens of Japanese origin. Consequently, the surprise of Pearl Harbor was compounded by a lack of intelligence infrastructure to meet the threat, once it had been painfully recognized.

Another example of the difficulty in shifting intelligence resources to new threats was the pivot of U.S. intelligence from the Nazi enemy to the new Cold War adversary—the USSR. Only five years after the end of World War II and after the "Iron Curtain" fell over Europe, did the United States formally define the Soviet Union as the prime threat and main focus for U.S. intelligence. On April 14, 1950, the National Security Council issued NSC-68: United States Objectives and Programs for National Security, which became the basis for the U.S. government's Cold War strategy.[7] From this point onwards, the Soviet Union became the U.S. intelligence community's most important target, which it remained for the next forty one years.[8] The centrality of the Soviet Union as the prime strategic threat was expressed in the creation of an intelligence infrastructure-government subsidizing of American academia for Russian studies and the study of the Russian language. This all-encompassing focus, however, kept attention from other emerging threats.

The 1973 Yom Kippur War was a "situational surprise" for the Israeli intelligence community, insofar as the two attacking armies were the key focus of Israeli intelligence. The common wisdom of the Israeli intelligence community, which misinterpreted the enemy movements as an "exercise," was accepted by U.S. intelligence, which fed it back to Israel, thus reinforcing it. This phenomenon of reliance on an intelligence partner that ostensibly has a clearer vision of its key object of intelligence creates a closed cycle of mutual affirmation of assessments. However, in this case, since the enemy was known, once the war broke out, Israeli intelligence could exploit a wide range of capabilities that it had refrained from activating before the war.

The fall of the Shah's regime and its succession by the "Islamic Regime" of Khomeini was a "fundamental surprise." This was due to the fact that American, British, French and Israeli intelligence services were unaware of the extent of influence of the opposition to the Shah among the public and the personality of Khomeini because they did not "cover" the underlying socio-political situation that precipitated the Iranian Revolution. Their assessments were based on the assumption that the intelligence and instincts of local regime services may be relied on, since they extensively "cover" domestic sentiment in their countries. However, reliance on the self-assessment of the regime's own security and intelligence organs (i.e., SAVAK) regarding their own success in maintaining stability is ill-advised; they will never reveal to foreign services (or even to their own leaders) that they have failed in their primary task. Even after the new Iranian regime was set up, it remained an enigma for years. It evolved out of a religious hierarchy and worldview that western intelligence knew nothing about. The process of

adapting intelligence gathering on such a regime was fraught with obstacles—first and foremost, the difficulty in understanding an adversary whose "rationality" and "cultural wiring" was different.

The case of the emergence of radical Islam as an adversary is instructive. Unlike state adversaries such as Nazi Germany, Japan, the Soviet Union and China, the nebulous network-centric nature of the new adversary rendered regular intelligence methodologies and collection methods useless. In a way, the approach to radical Islam was influenced by the experience gained in the conflicts with Iran since the 1977 Iranian Revolution. However, the differences were significant: Persian Iran vs. Arabs, Shiite Iran vs. Arab Sunni Islamists, and the very fact that Iran was a country whereby collection and analysis could follow similar paths as other country targets, whereas the Sunni radical Islamists were groups. Unlike the preparations for the Japanese and Soviet threats in their time, Western intelligence as a whole was unprepared for the Islamist threat. By the time of the attack of 9/11, most Western intelligence agencies suffered from a lack of infrastructure—linguists and cultural-religious experts—to face the threat. The surprise was exacerbated by a lack of intelligence infrastructure on Afghanistan, which had been neglected since the end of the Soviet invasion. One may postulate that if U.S. intelligence had a better picture of the forces in Afghanistan, the learning curve after the relatively swift military operation would have been steeper.

The end of the Cold War (Francis Fukuyama's "The End of History") put an end to the focus on the USSR. Eminent "Kremlinologists" were out of work and were not replaced by experts on the rapidly evolving oligarchic kleptocracy and Putinist authoritarianism that took over Russian politics. Instead of expertise on the ideology and inner workings of the Soviet Politburo, intelligence on the new Russia called for detailed knowledge on the personal interests, social and regional backgrounds of the new oligarchy, but also Russian history and nationalist self-images. A deep knowledge of Russian culture and history became necessary in order to understand the motivation of the new Russian "verticals of power."

The Arab Spring of 2010 was also a fundamental surprise for most intelligence agencies, which had not learned the lessons of the fundamental surprise of the Iranian revolution. Many western (and Arab and Israeli) intelligence services were blinded by their dialogues with the security agencies of those regimes just as they had been misled by the Iranian SAVAK in 1979.[9] The "Arab Spring" was the result of developments within the countries themselves, deep economic and social malaise, and the perception of the loss of domestic deterrence by ossified regimes led by aging leaders. The experienced leaders of the regimes that fell in the "Arab Spring" were all elderly, had exercised personal authority for decades and were surrounded by "yes-men." Opposition elements in those countries began to see the decline of the "old lion" and to challenge the regimes. The popular perception that the United States had abandoned its erstwhile allies also contributed to the weakening of those regimes. These were facts that were known before the Fall of 2010 but were not taken into account in most intelligence assessments, which were based on the experience of those regimes' having weathered numerous crises and the experience of their rulers. Intelligence communities dealing in the Middle East ignored the Heraclitan principle that "everything flows—you do not step into the same river twice."

The Syrian Civil War and eventual fall of the Assad regime were also prime examples. The assumption of stability of the Bashar al-Assad regime did not factor in the process of elite transformation. After 30 years of Bashar al-Assad's father's regime in which the same people remained in the top positions for decades, the top figures of the regime were replaced a number of times and a new "imported" elite from Iraq, Lebanon and Iran dislodged the old Ba'ath elite. These internal incremental processes were not on the radar of most intelligence agencies which tried to observe Syria (the United States, Israel, et alia). Therefore, they were surprised when the Syrian Civil War broke out in predominantly "Ba'athist" southern Syria and had no inkling regarding who the rebels were and what they wanted. This lack of "intelligence intimacy" severely hampered the ability of those agencies to exploit the situation to their benefit.

The final collapse of the Assad regime by Hayat Tahrir al-Sham (HTS) within days in December 2024 again surprised the intelligence communities in Israel, the West and, apparently, even Iran and Russia and should be added to the list of strategic surprises to be studied in schools of war and intelligence. Here, too, the assessment of the regime did not take into account its inherent weakness and the fact that it existed on "life-support" provided by Russian air power and Iranian/Hezbollah/other Iranian-proxy militias' ground power. However, these factors had changed. Russia had long withdrawn most of its air force from Syria and was never inclined to endanger Russian troops in a ground war for Bashar al-Assad. Hezbollah, which had been instrumental in support of the Assad regime had been decapitated by Israel and could not rush to Assad's help. Iran, which had been attacked by Israel and did not dare strike back, did not want to risk more defeat. The rebel organizations themselves were a low priority for the intelligence agencies and outside of the "streetlight" which was focused on Gaza, Lebanon and Yemen.

Finally, the 2023 Middle East War was, for Israel, a situational surprise in the guise of a fundamental surprise.[10] Israeli intelligence (IDF Intelligence—AMAN, Shin-Bet and Mossad) had a degree of "intelligence intimacy" with Hamas and Hezbollah almost without precedence. This was demonstrated in the rapid recovery from the surprise and the exploitation of a high level of theatre-specific intelligence on Gaza and Lebanon that enabled it to swiftly move to the offensive against Hamas and Hezbollah after the surprise of October 7th. The pinnacle of these operations was the "Pager Operation" which neutralized thousands of senior Hezbollah operatives at once and eliminated the entire top leadership of Hezbollah in a matter of weeks. Nevertheless, this tactical knowledge did not contribute enough to the strategic analysis and did not provide appropriate early warning.

On the other hand, Israel's intelligence on the Houthis in Yemen was sketchy. In that respect, the Houthis constituted a "fundamental surprise." Here too, the history of Israel's wars[11] should have triggered a scenario of known Iranian proxies who control a strategic maritime bottleneck (Bab al-Mandab on the entrance to the Red Sea). The fact is that in the allocation of efforts of the respective intelligence communities, these theatres did not get the attention they deserved. The result was an extended learning curve before they could be dealt with effectively.

Preparing for and Recovering from Surprise - Possible Approaches

Both God and the Devil are in the details. Strategic intelligence is not a separate body of knowledge; its "building blocks" are the tactical pictures generated by tactical intelligence. Tactical intelligence is meant to provide the military or intelligence agencies with operational capabilities against the threat, such as information on human terrain, whereabouts of leaders, command and control structures and other targets. However, it also generates "capability intelligence" on the enemy, which in turn, should feed strategic intelligence on the enemy's intentions.

The importance of integrating tactical intelligence as a component of strategic intelligence has grown over the last few decades. One of the causes of intelligence failures has been the dearth of intelligence on "micro" factors that ultimately come together to create a strategic reality. This was manifested in the lack of understanding of the ideology, leadership and motivation of the Jihadi network in Afghanistan, which the West supported during the Soviet invasion. The absence of sufficient intelligence on the religious leadership and ideology that was to become the Iranian regime is another case in point. This has been exacerbated by the disintegration of the Middle East since the "Arab Spring." "Non-governed areas" in Syria, Iraq, Africa and potentially in other areas have cropped up and pose a challenge. The renaissance of tribal identity also poses a new challenge. This "re-tribalization" of the Middle East will have a significant effect on intelligence collection and analysis. Whereas in the 20th century regional studies relied heavily on country studies that described the workings of government in primarily military modernist regimes, understanding of the region in the first decades of the 21st century will call for "micro-understanding" of the working of tribal affiliations and coalitions.

A "situational surprise" usually has a short timeframe. Most of the intelligence collection and analytic capabilities for a known threat are in place and can be brought to bear once the initial surprise has been overcome. This is different with a "fundamental surprise." The "ship of intelligence" has a heavy "helm" and the time it takes to turn its course is out of synch with the tempo of war. Consequently, the time lapse from the initial "fundamental surprise" to achievement of the degree of "intelligence intimacy" with the adversary that enables interpretation of incoming intelligence (SIGINT and HUMINT), and intelligence-intensive operations is usually quite long. Furthermore, it is the absence of this "intelligence intimacy" that allowed the "fundamental surprise" in the first place.

Turning the "helm" of intelligence on the object of a "fundamental surprise" requires the creation of a wide range of tactical capabilities that cannot be achieved overnight. Investing additional resources can only marginally shorten this timeframe. The acquisition of knowledge on the physical and human terrain of the hitherto unfamiliar adversary—language, culture, social structure and decision-making—and subsequent generation of collection and analytic capabilities is an arduous task.

This difficulty raises a number of questions: how can technology and methodology expedite the process of achieving "intelligence intimacy" and restoring "intelligence dominance" towards the object of a fundamental surprise? Are there ways to create, in advance, an "intelligence contingency infrastructure" for scenarios that conventional wisdom may view as improbable?

Construction of such an infrastructure should not wait for a strategic trauma. The identification of potential "low probability-high risk" scenarios and actors should take place as a regular methodology in the intelligence tool box in order to generate "watchlists" of signs that the improbable may be becoming a reality—and thus to reduce the risk of fundamental surprise and, if such surprise occurs, to reduce the time frame for acquisition of the intelligence dominance necessary to defeat the new threat. A methodology is needed for early warning on "unknowns" that lurk in the dark and for rapid response to fundamental surprises. Such a methodology should enable us to postulate developments that may have strategic implications, deriving from theatres, means and intentions that we have not yet encountered, and be flexible enough to deal with challenges that stem out of a wide variety of geographic, demographic and cultural environments and enable quick adaptation of assets, and identification and prioritization of targets.

One approach may be technological. AI is already used to facilitate regular intelligence operations. AI systems can be used to identify growing trends not only in areas of interest (i.e. of intelligence requirements) but in a wide spectrum of areas. Such an approach may be useful in "flagging" such trends as potentially worthy of of direct attention and inclusion in the intelligence requirement. Such a methodology should include a wide range of factors—economic, social indicators, changes in prominence of political figures and entities, et alia. Models or "maps" based on integration of all of these can help broaden the "circle of the streetlight" and identify potential vectors emerging from them.

The "Devil's Advocate" or "Other Opinion" system that was developed in Israeli intelligence along with enforcement of intelligence pluralism may be part of such a methodology. After the Yom Kippur War (1973), Israeli intelligence agencies "competed" in challenging each other's assumptions. While much of this competition may have been motivated by a desire to get the attention of political leaders, it enhanced the dynamics of intelligence assessment. An important tool in the "quiver" of such a discipline should be deductive reasoning.[12] Since the identification of a threat on which there is no extant information cannot rely on traditional inductive reasoning, the process was based on presentation of hypotheses—even ostensibly far-fetched ones—and identifying the signals that could indicate that they are emerging.

One important component of such a methodology should be the development of tools for dealing with the constantly shifting sands of human terrain. Collecting intelligence from governmental and military sources is not enough; it will have to have to be augmented with information on social, religious, cultural factors on local levels. Such information should target societies which are under constant flux, "non-governed" and "reduced-governance" areas, groups switching loyalties and creating new coalitions, religious trends, and other factors that

could create new strategic realities. Such a methodology should strive to identify telltale signs of emerging conditions that can develop into breeding grounds for strategic challenges and accord "risk ranks" to theatres and trans-national trends. Flagging such theatres or objects should generate intelligence requirements that result in allocation of collection and analytic resources. While some—or even many—of these objects may not evolve into actual threats, the rule of thumb of "low probability-high risk" should drive this methodology.

Finally, the art of intelligence assessment calls for non-linear relational thinking. This is particularly relevant when trying to understand the actions of a movement. The "Gestalt" of a popular movement or even of an organization with an established leadership is far more prone to influences of the proverbial butterfly.[13] The tendency to individualize the collective adversary or collective processes and to apply individual cost-benefit rationality to it is natural, but usually incorrect. A mass movement does not behave like an individual. An intelligence methodology should factor this in as well. Modern Western intelligence communities may learn from the modus operandi described in the memoirs and histories of Laurence of Arabia and Gertrude Bell, who worked in the region in the pre-state era. Therefore, the study of "tribal landscapes" should be among the key intelligence requirements.

---

[1] Lewis Carrol, *Alice's Adventures in Wonderland and through the Looking Glass*, Bantam, New York, 1981, pp. 166-167.

[2] A cognitive and observational bias that causes people to only consider the information that is easiest to find, sometimes described as the tendency of people to look for their lost keys under the streetlight because there is light there.

[3] For this distinction see Zvi Lanir, *Fundamental Surprise: The National Intelligence Crisis, 1983*. Published in Hebrew: ההפתעה הבסיסית, מודיעין במשבר

[4] Ironically exactly such a scenario was envisaged in Israel (code-named צבא שמים—"Host of Heaven") and was the basis of exercises and standing operation procedures that were directed to prevent any hijacked plane from coming near populated areas in the country—even at the cost of shooting them down.

[5] National Security Agency/Central Security Service, *Historical Events; Linguists*, August 20, 2021, available at https://www.nsa.gov/History/Cryptologic-History/Historical-Events/Article-View/Article/2740656/linguists/.

[6] National Security Agency/Central Security Service, *Historical Events; Pearl Harbor*, August 20, 2021, available at https://www.nsa.gov/History/Cryptologic-History/Historical-Events/Article-View/Article/2740705/pearl-harbor/.

[7] It stated that "The Soviet Union, *unlike previous aspirants to hegemon*y, is animated by a new fanatic faith, antithetical to our own, and seeks to impose its own authority over the rest of the world"Ironically this characterization of the Soviet Union was made only five years after the Nazi regime which was clearly "animated by a fanatic faith antithetical to that of the US" was defeated in its quest for world domination. See *A Report to the National Securiity Council by the Executive Secretary on United States Objectives and Programs for National Security*, April 14, 1950, available at https://info.publicintelligence.net/US-NSC-68.pdf.

[8] A Top Secret December 1951 report by the CIA to the NSC (since declassified) stated that "The USSR is now the center of opposition to American policy, and the one power menace to American security; thus the need for knowledge of the USSR, the orbit of its domination, and its worldwide communist organization transcends all other intelligence requirements." See Central Intelligence Agency, *Intellgence and the Structure of National Foreign Policy*, December 26, 1951, available at https://www.cia.gov/readingroom/print/58557.

[9] The author of this article presented in June 2010 a scenario of the possible fall of the Mubarak regime in Egypt due to the president's illness, the failure of the succession scenario of his son, Gamal Mubarak, the lack of alternative leadership in the regime and the growing strength of the Muslim Brotherhood. A senior U.S. intelligence official reacted by saying that the scenario was highly unlikely because the Head of Egyptian Intelligence, Omar Suleiman had assured them that "succession was under control."

[10] See Shmuel Bar, "The Unlearning of the Lessons of 1973," *Information Series* No. 589 (Fairfax, VA: National Institute Press, June 11, 2024), available at https://nipp.org/information_series/shmuel-bar-7-october-the-unlearning-of-the-lessons-of-1973-no-589-june-11-2024/.

[11] The main casus belli for the 1956 Sinai War and the 1967 "Six Day War" was the blocking of Israel's shipping routes.

[12] One of the drawbacks of this method was that the officers in the "Devil's Advocate" unit were seconded for a period of service and then went on to other positions in their relevant agency. Hence, they were subject to pressures and constraints stemming from their career decisions. An alternative that has been considered is to form a unit of "elder statesmen" of various ranks and proficiencies who would not be subject to those personal considerations. These would rotate annually (like in the UK Joint Intelligence Organisation) but unlike that body would not return to regular service. Their output would be sent to the political level without any intermediaries.

[13] In Chaos Theory, the "Butterfly Effect" suggests that the flight of a butterfly in India can contribute to the formation of a storm in the Pacific Ocean.