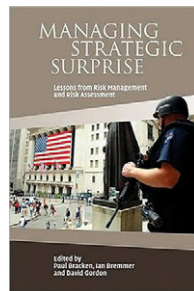


Managing and Assessing Risk by Edward A. Turzanski

Edward A. Turzanski served with the U.S. Intelligence Community in a number of capacities during the Reagan Administration and is an FPRI Senior Fellow with the Center for Terrorism, Counter-Terrorism and Homeland Security.

Managing Strategic Surprise—Lessons From Risk Management and Risk Assessment, edited by Paul Bracken, Ian Bremmer and David Gordon (Cambridge University Press, 2008) 336 pp., \$29.99.



Managing Strategic Surprise – Lessons From Risk Management and Risk Assessment is the result of a nearly two-year process, funded by the National Intelligence Council, in which the editors introduced the concepts of risk management and how it is employed in various activities (finance, business, engineering, environmental protection, epidemiology) to domain experts within various international security fields. For the authors, principles of risk management, specifically tailored and consistently applied to the structures and policies of national security, could help overcome the “sloppy” risk management which they maintain has characterized U.S. foreign policy since the reason for more prudential treatment of risk – the existence of a Soviet threat – was removed from the foreign policy equation. Simply stated: get risk management right and you won’t get Iraq—or WMD proliferation, or terrorism and counter-terror measures, or Iran, or any number of security and foreign policy challenges—wrong. The clear implication (if not stated belief) is that the principles of risk management are missing in sufficient quantity or detail in U.S. security structures and policies, and thus U.S. national security is needlessly compromised. This core presumption serves as both the most valuable “take away” of the collected essays, and the most likely point of contention from critics. Put another way: is the perceived lack of risk management principles accurate and would national interests be better served by a systemic overhaul of the U.S. national security apparatus according to the principals of risk management?

The essays presented cover a wide range of national security concerns: “How to Build a Warning System”; “Intelligence Management and Risk Management: the Case of Surprise Attack”; “Nuclear Proliferation Epidemiol-

ogy: Uncertainty, Surprise and Risk Management”; “Precaution Against Terrorism”; “Defense Planning and Risk Management in the Presence of Deep Uncertainty”; “Managing Energy Security Risks in a Changing World”; “What Markets Miss: Political Stability Frameworks and Country Risk”; “The Risk of Failed State Contagion”; and “Managing Strategic Surprise”. As innovative as this approach demonstrated to national security is one wonders whether the threat matrix represented here would have anticipated the global financial crisis of September 2008, which has prompted a change in the substance of the President’s Daily Brief, which as of February 2009 includes a section on the impact of the global economic crisis on U.S. national security. Far from a criticism of the work, the question speaks to the interconnected and interdependent nature of the world—in political, military and economic terms—to what James Woolsey, former Director of Central Intelligence under President Clinton, liked about the approach here advocated—“Conclusions (that) don’t try to predict the future—It’s about insight, not numbers . . .”¹ Respectful of the broad breadth of the work and the sophisticated nature of the analyses, this review will, for the most part, confine itself to matters specifically dealing with the process and structures of intelligence production, dissemination, and use. That is also the area of national security analysis which is most regularly criticized for “predicting” rather than explaining or managing the unknown.

The first challenge confronting the authors was to provide a workable definition for risk management. As a concept, risk management has developed in different ways across specialized fields in which there is relatively little cross-fertilization of concepts and operations (e.g., engineers who study nuclear power plant safety or financial planners who employ risk management in very sophisticated, specialized ways, but use different terminologies and frameworks for implementation not easily translated from one discipline to another). To meet the challenge, the authors point to the discipline’s origins as the application of statistical methods to the mass production growth of the 1920s and 1930s, further developed during World War II by applying mathematical concepts to military operations, and finally articulated in the 1950s as a distinct discipline of decision sciences under the banner of risk management. For purposes of their analysis, the authors define risk as “the product of two things: likelihood and consequences . . . separating the likelihood that some event will take place from the consequences of if it does.” These two elements lead to three conversations—one about likelihood, one about consequences, and one about the management of the two; which, in turn, led to the conclusion that in national security matters, “Risk management is about insight, not numbers. It isn’t the predictions that matter most but the understanding and discovery of the dynamics of the problems.”

¹ Endorsement of the text taken from the back dust jacket.

In discussing the application of risk management principles to national security matters with the various domain experts included in the study, the authors allowed them to “make their own judgment about which (risk management) concepts to use. Because one of the lessons of good risk management is that it is as much an art as a science.” This common-sense decision reflects the fact that difference components of the national security structure have discreet, differentiated functions. Bracken (a professor of management and political science at Yale University with extensive international business and management experience), in his essay on “How to Build a Warning System,” turns the preceding quote on its head and makes the point that the traditional intelligence functions need to become more science than art. For Bracken, the intelligence function of strategic warning is in desperate need of a standardized vocabulary that can be understood by policymakers, an understanding that the traditional “warning” function needs to be part of a more comprehensive risk management system, and a realization that analytical management tools must be employed to bring strategic and organizational coherence to risk management. To illustrate the point, Bracken refers to the failure of the U.S. warning system leading up to the Pearl Harbor surprise attack in December of 1941 and the “magnificent” performance of the system seven months later at the Battle of Midway.

Bracken maintains that U.S. Army Chief of Staff General George C. Marshall’s horizontal management reorganization, in which intelligence collections and analysis and military operations assets were better tasked and organized, was the defining difference between the failure at Pearl Harbor and the success at Midway. After all, “the underlying technologies of radar, direction finding, and code breaking did not change in seven months. No new reconnaissance planes were added to the air fleet. Nor did a flood of better-trained people suddenly, appear, for training took longer than this.” With respect to both Bracken and General Marshall, the former’s formulation fails to mention a significant intelligence breakthrough without which no amount of managerial efficiency would have made victory possible at Midway. The Pearl Harbor SIGINT (signals intelligence) unit, code-named “Hypo” (later known as FRUPac), had made dramatic progress in decrypting the latest version of JN25 (the Japanese Naval Code) after the surprise attack on Hawaii. This made possible what Christopher Andrew, one of the most accomplished historians of intelligence studies, has referred to as “one of the great cryptanalytical coups of the war”: Admiral Yamamoto’s plan to capture Midway Island for the purpose of luring the U.S. Pacific Fleet to be destroyed by his superior force, as a prelude to another attack on Hawaii.² Admiral Chester W. Nimitz, commander in chief of the U.S. Pacific Fleet said of Midway, that it “was essentially a victory of intelligence. In

² Christopher Andrew, *For the President’s Eyes Only – Secret Intelligence and the American Presidency from Washington to Bush* (New York: Harper Collins Publishers, 1995), pp. 124-125.

attempting surprise, the Japanese were themselves surprised.”³ Certainly, to the consequential benefit of the United States, the structures of intelligence processing and integration had been made more efficient and active as a result of the bracing failure at Pearl Harbor. Without the cryptological breakthrough making it possible to read the latest version of the Japanese JN-25 code, however, the victory at Midway might have been another devastating defeat.⁴

The Pearl Harbor intelligence failure adds yet another practical illustration for one of the guiding principles of risk management advanced by Bracken: isolating critical assets from uncertainty. Aircraft carriers had been sent to sea to reduce their vulnerability to attack while congregated in port. In fact, operating on the same theory, planes were stacked wing to wing at Pearl Harbor to allow greater protection against sabotage. Unfortunately, this sabotage counter-measure had disastrous consequences when the threat changed (from ground-based sabotage to surprise attack from the air). In intelligence and warfare, tunnel vision (focus on a primary means of attack at the expense of picking up peripheral threats) has costly consequences. The United States did build a more robust, integrated and forward looking military warning intelligence system during World War II to support the war-fighters. This also meant that intelligence spending—and the tasking it supports—was and remains largely (though not exclusively) focused on and controlled by the Pentagon. Paul K. Davis’ essay on “Defense Planning and Risk Management in the Presence of Deep Uncertainty” makes clear that the Pentagon has been much more advanced in incorporating a more risk management-based planning process in its planning. In large part, the global nature of U.S. military interests as dictated by Cold War and post-Cold War threats served as the lash of necessity that forced planners to employ best practices in managing the vast enterprise that is the U.S. military.

Best practices appear to penetrate the national security structure unevenly. Bracken notes that literature on warning generally fails to provide a useful vocabulary or concepts for a productive discussion on how to build a better warning system or as practical guidance for the people who will rely on it. (He does not draw a specific distinction between policymakers and other players in the system, though intelligence professionals would be quick to do so because of the firm belief that intelligence people do not and should not do policy.) He also characterizes the literature on warning as being “gripped by an obsession with failure. It focuses on failure chains, rather than success chains.” Again, focusing on the distinction between those who do the warning and

³ Ibid.

⁴ See: “Intelligence in War: It Can Be Decisive – Winning with Intelligence,” by Gregory Elder, *Studies in Intelligence*, posted April 15, 2007, available on-line at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no2/html_files/Intelligence_War_2.htm.

those who need to be warned, and the practical political consequences of intelligence failures on the relationship between the intelligence community (IC), policymakers and the general public, failure often has immediate, extreme and highly publicized (and often, politicized) effects.⁵ It would follow, therefore, that failure chains are more discussed than success chains, especially in an enterprise where the sources and methods of success are to be protected against countermeasures by not being revealed or discussed. Also, bureaucratic competition for funding and political support within the national security structure makes failure extremely costly. Years ago, intelligence operatives in the field were taught that failure teaches success, but only if you learn the lesson. Though Bracken's point is worth considering, the "focus on failure" is not a zero-sum game that ignores "keys to success."

From a strict intelligence perspective, the most applicable contribution in the book comes from Uzi Arad (*Intelligence Management as Risk Management: the case of surprise attack*). Arad, a veteran of Israel's foreign Intelligence service (the Mossad) makes clear that the potentially fatal combination of attack and surprise makes the task of early warning the cardinal responsibility of intelligence agencies." Where does quote begin? He also acknowledges that intelligence agencies, by virtue of this responsibility, tacitly implement fundamentals of risk assessment and control (probabilistic measurements, evaluation of risk, use of scenarios; and widespread use of risk-control and risk management tools such as backup systems, and risk reduction through diversification and redundancy). In discussing various essays in this book, former colleagues in the IC routinely protested "We already do that. . ." or "We've been doing that for years. . ." when the topic of incorporating risk management strategies in planning and analysis was broached. With this said, Arad correctly observes that failure will push the system even further. Much as crisis forced the insurance and banking industries to do a decade or so ago, recent and feared failures, which have led to the current trend of consolidating and centralizing intelligence structures, will push the IC and the national security system as a whole towards creating and formally institutionalizing a comprehensive risk doctrine.

That doctrine, in Arad's formulation, would address each portion of the intelligence production cycle.⁶ The literature on intelligence warning usually focuses on analysis and production, rather than collection, as the portion of the cycle in which breakdowns occur. As a result, Arad maintains that collection

⁵ For a comprehensive discussion of the pitfalls that ensnare the IC in its dealings with elected officials, see: *Sharing Secrets With Lawmakers: Congress as a User of Intelligence*, section V. Problems and Pitfalls in the Relationship, Centre for the Study of Intelligence, available on-line at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sharing-secrets-with-lawmakers-congress-as-a-user-of-intelligence/5.htm>.

⁶ For a traditional rendering of the intelligence cycle – 1. requirements needs, 2. planning and direction, 3. collection, 4. processing, 5. analysis and production, 6. dissemination – see: Robert M. Clark, *Intelligence Analysis – A Target-Centric Approach*, 2nd ed. (Washington, D.C.: Congressional Quarterly Press, 2007), pp. 10, 11.

rarely receives the attention that it requires in terms of addressing systemic deficiencies. He notes that U.S. government reviews of both the 9/11 and Iraq WMD questions lay the failures at the feet of intelligence collection. Among the most prized, though potentially flawed, collection sources is human intelligence (HUMINT). Intelligence collection relies on signals intelligence (SIGINT), Optical or Electrical Visual Intelligence/Imagery Intelligence (VIS-INT/IMINT), Open-Source Intelligence (OSINT) and Chemical and Optical Measurement Intelligence (MASINT) in order to complement and compensate for the deficiencies and frailties of HUMINT intelligence collection. Arad believes that the problem of poor collection and an accompanying process of validating the collected information require the application of the same intellectual attention, management and processes that are devoted to examining problems in analysis and production. Most of the essays in this work dealing with intelligence decry the absence of a risk management component in the intelligence process, especially, as previously noted, in the area of warning. The one exception is “The indicator-analysis method.”

Used primarily for early warning purposes, the indicator-analysis method has as its core presumption the belief that no attack, either engineered as a surprise or enhanced by deception, occurs without emitting some type of signal—even if only a perceptible deviation from routine. In colloquial terms, indicator-analysis is an “All hands on deck!” call to action in which common indicators and descriptive terms allow cross-community participation in the activity. For indicator-analysis to work, appropriate analysis and collection requirements must be in place (i.e., a systemic ordering of lists of indicators and of appropriate collection tools for locating and monitoring them). This is where the science of risk management meets the art of intelligence warning (Arad calls indicator-analysis “the fullest manifestation of risk management in the intelligence world.”) Indicator-analysis is a demanding task that includes an element of probability assessment in determining the correlation between various indicators and the significance of the correlation. The strongest characteristic of indicator-analysis is that it provides a measurable guide as to where additional resources need too be applied as the intelligence system monitors a particular situation. Its main drawback, however, is that in many situations indicators that constitute a necessary condition for developing an attack may also be present in routine situations. How then, does one clearly identify an imminent attack, and only an imminent attack?

Arad’s densely technical, but compelling, discussion of the indicator-analysis method would have benefitted the reader much more had he included a practical illustration of the method functioning correctly, as well as one in which the system failed. Part of the problem in illustrating success and failure in indicator-analysis is that surprise attacks rarely occur; and in the event of preemption of such an attack, it is entirely probable that preservation of sources and methods would preclude any open-source or declassified discussion of the event. Most frequently, indicator-analysis is largely conducted through national

technical means – because the technological means that allow constant, voluminous and easily calibrated means of information collection. Arad points out that indicator-analysis is also used with HUMINT, though the sources in question are often lower-level human assets people⁷ to whom access is relatively easy and who can provide real time information about an imminent attack. The United States and Israel, two states that have been subject to surprise attacks, can attest to the fact that the combination of a classic early-warning system and an indicator-analysis system is difficult to manage in-tandem over time. One would hope that Arad, or someone, of similar competence, will one day be able to review the performance of the US IC in the Summer of 2001, when Richard Clarke was “running around with his hair on fire” over the threat of a potential al Qaeda attack against U.S. interests to determine whether the indicator-analysis method had been used, and if so to what effect. Arad states that maintaining an indicator-analysis system requires flexibility and adjustment to changing circumstances, which affects necessary collection tasking. Again, mindful of the “intelligence chatter” during the summer of 2001, what happens to the effectiveness of the indicator-analysis method the longer it is used at an intense pace? Mere mortals in the military, intelligence, counter-terror and law enforcement fields cannot sustain the same pace of intense readiness or tasking over long periods of time without some deterioration of capacity. And even national technical means (machines) have their limits—usually because of the demands of competing crises or needs (consider complaints made about the re-taking of Predator drones to Iraq and away from Afghanistan . . . only so many drones to go around).

Even the best designed warning system can yield the wrong result. In his discussion of how intelligence services try to prevent early warning failure at the analysis phase (employ advanced research methods involving the types of problems with which intelligence must cope, and use specific tools and instruments, designed to overcome the risk of missing an early warning) Arad maintains that “there has never been an early-warning failure in the history of intelligence that was caused by a theoretical disciplinary lag in the assessment units.” In almost every case of early warning failure, analysts had information which should have yielded the right warning. Why, then, does the system suffer failure? The answer is: people. Misperceptions of reality and information in the systems, pre-conceived mindsets, social pressures that reinforce group-think, and bureaucratic dispositions can skew perceptions of information and distort its significance.⁷ Among the pathologies of failed analysis, Arad mentions suppression of minority opinions challenging majority views within

⁷ For a detailed discussion of the kind of problems that can beset early warning, see: *The Perils of Analysis: Revisiting Sherman Kent’s Defense of SNIE 85-3-62 – The Cuban Missile Crisis.*, by Michael Douglas Smith, *Studies in Intelligence*, posted January 9, 2009, available on-line at : <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no3/revisiting-sherman-kent2019s-defense-of-snie-85-3-62.html>.

intelligence structures as another potential problem. His presentation on the topic would have benefitted from a discussion of the complementary problem of the National Intelligence Estimate (NIE), an intelligence product representing the consensus view of the intelligence community which, over time, has come to embody most of the criticisms of the IC mentioned in this and other intelligence reviews.⁸ Socio-psychological pathologies among analysts are dealt with primarily through what Richard Heuer calls Alternative Analysis⁹ and structural reform of the organizations producing analysis by means of diversification and redundancy. Alternative Analysis is accomplished by means of the following:

- Competing Group A and Group B analysis in which two groups are given the same information and asked to provide their own analysis, or where Team “B” is given the task of critiquing Team “A’s” analysis.
- Red Cell analysis in which role playing is intended to impart an understanding of the adversary’s point of view (typically used to encourage development of a consensus view).
- “What if” analysis focusing on causes and consequences of an unlikely event.
- Analysis of Competing Hypothesis (ACH) intended to produce the maximum number of alternative assessments of a given problem, and
- Key Assumptions Checks which requires that the analyst monitors in practice those events that would occur in the event his hypothesis is valid.

The methodological and structural tinkering to minimize wrong calls by analysts is summarized in Arad’s differentiation between the Israeli and the British approaches to early warning best practices. As a response to the surprise attack of the 1973 Yom Kippur War, the Israelis created, what Arad calls, the only “pluralistic” warning system in the world, in which competing analysis force best practices (though he does warn that competitive analysis, if not prudently metered, risks being over-used to the point of giving bizarre counterpoints equal standing with competent analysis). Conversely, the British insist on the achievement of a consensus opinion. That two respected intelligence services would craft such distinctive approaches to the common problem of insuring the accuracy of early warning points to the role that

⁸ For a discussion concerning the problematic aspects of NIEs within the specific context of the IC’s views on Iranian nuclear weapons development, see: Edward A. Turzanski, Policy Disruption by NIE, FPRI E-Notes, January 2008, available on-line at: <http://www.fpri.org/enotes/200801.turzanski.policydisruptionnie.html>.

⁹ Richard J. Heuer, “The limits of intelligence analysis,” *Orbis*, Winter 2005, as cited by Azard, pp. 61-63.

historic, geographic and cultural context plays in the structure and process of intelligence. Simply stated, best practices go only so far, because nations do differ, in significant ways, from one another.

The two concluding elements of Arad's presentation – the elected official as consumer of intelligence, and structural reform of the IC as a result of the 9/11 warning failure – speak to what some might infer to be the real sources of, recent intelligence failure. What happens if the chief consumer of intelligence, the constitutionally-empowered policymaker, chooses not to accept the consensus view, or shops about in the national security apparatus until he finds an analysis with which he agrees? As Christopher Andrew's survey of Intelligence and the American Presidency makes clear, the ways in which American Presidents treat the process and product that is intelligence is very much a reflection of the individual tastes, character and context of events of that President. There is little that the IC can do, within the law, if a President chooses to disregard its assessment of a specific security question.

On the matter of organizing the IC, Arad correctly points out that the post-9/11 reform spoke to multidimensional integration and centralization of the system. The Director of Central Intelligence (DCI) was seen as being institutionally incapable of leading the IC by virtue of his relationship to one of the components (as head of the CIA). Post-9/11, the problem was addressed by creating the office of Director of National Intelligence (DNI), who, unlike the DCI, would, theoretically, be seen as being truly independent of the entire IC structure because of his lack of entanglement with any one element of the same. What is left out, however, is the fact that as was the case with the DCI, the DNI controls less of the overall intelligence budget than does the Secretary of Defense.¹⁰ Because the Secretary controls most of the budget, he controls most of the IC assets and most of the tasking of them. In intelligence, politics and life, the maxim "You pay, you say!" is not without truth or practical effect. Another concern raised by the creation of the DNI position is the effect of adding yet another layer of bureaucracy to the IC. Structures rarely become more focused and precise through the addition of new layers of management. Also, the ability of an intelligence manager to appreciate the "feel" of the product – how it was made, its strengths and weaknesses, its relationship to tangential issues – is diminished by degrees of separation from the collection point (the further one is from the building of the product, the less one knows about it).

Arad states that mechanization may provide the key to solving many of the problems presented by limitations on human objectivity and rationality. Those who have spent a career on the operations end of the intelligence spectrum would greet that news with considerable reserve. Certainly mechanized capacities can – and do – enhance intelligence collection and processing, but their limitations come in judgment; there they are a poor substitute for

¹⁰ Mark Lowenthal, *Intelligence – From Secrets to Policy*, 3rd ed. (Washington, D.C.: CQ Press, 2006), p. 42.

human intuition – as fallible as that capacity often is. To his credit, Arad admits that the full application of risk management principles in surprise attack warning goes well beyond the IC and requires the use of the entire national security apparatus. As previously stated, the IC's role is not to make policy, but rather to inform and support those who do. Also, poor outcomes related to intelligence are not necessarily the product of poor structures and procedures – though both factors may be problematic in some sense. Regarding 9/11, Deputy Attorney General Jamie Gorelick's "Wall Memo" maintaining a strict separation between the investigative and counter-terror functions of the FBI (to preserve the integrity of criminal prosecutions) reflected a problematic mindset, immune to risk management principles in the sense that they were driven by philosophic belief or political ideology.¹¹ Treating counter-terrorism as primarily an issue of law enforcement rather than one of war fighting compromised national security. The decision to do so rested with the constitutionally responsible elected policymakers – not with the IC.

In the conclusion to their book, Bracken, Bremmer and Gordon state that conditional probability – the chances of an event occurring if another thing happens-is one of the basic ideas that made statistics applicable to fields as diverse as operations research and finance. Throughout their study, the authors were struck by how infrequently and informally this concept had been incorporated into the practice and theory of international relations. With all due respect, and in appreciation for the rich, cross-disciplinary analysis of various components of national security, considerable evidence exists that risk management theory is – and has been – much more present in national security formation than here suggested. Part of the difficulty in identifying the presence of these concepts rests in proprietary language that is not easily translated from one discipline or security aspect to another.

Kudos to the authors for making the clear recommendation that a more commonly accepted terminology for risk assessment be adopted for purposes of national security analysis and formation. The more challenging obstacle to embracing risk assessment may lie in the nature of human beings, the laws which govern our foreign affairs, and in the intuitive preferences of those who seek to explain – or, as the authors would prefer, manage – the unknown. National security policymakers are not philosopher kings but people with ideological predispositions who depend upon political considerations to win and maintain their constitutionally-held offices. This means that they will, occasionally, reject the advice given by their risk managers, no matter how technically sound it may be (intelligence professionals are accustomed to, though often vexed by, the peculiarities of those who care not to be

¹¹ For a review of the Wall Memo and its impact on Counter-terror functions, see: Andrew C. McCarthy, "The Wall Truth," National Review On-Line, April 19, 2004. Available on-line at: <http://www.nationalreview.com/mccarthy/mccarthy200404190849.asp>.

“informed”). There are also instances when the most sophisticated of risk management formulas fail to anticipate or adequately assess the unpredictability of human beings. Herein lies both the challenge and the opportunity for the formalization of risk management practices in the field of national security policy.

Former Secretary of Defense Donald Rumsfeld once famously answered a reporter’s question about an event that had not occurred with the following words: “Reports that say that something hasn’t happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don’t know we don’t know. And if one looks throughout the history of our country and other free countries, it is the latter category that tends to be the difficult ones.”¹² Bracken, Bremmer and Gordon have rendered admirable service in advancing the conversation of how to manage the “difficult unknowns.”



¹²February 12, 2002 DOD Briefing with Secretary Rumsfeld and General Myers, available on-line at <http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=2636>.