As I recently argued here at War on the Rocks, many of the current Defense Department approaches to risk and risk management could stand an overhaul. In discussions on national security, risk is frequently not well defined, and is often used for purposes (sufficiency and threat analyses) better served by other components of strategy. Too often, risk frameworks generate ambiguous, color-coded assessments grounded in subjective analyses.

In order to build a better model, we need to define the type of choices we’re dealing with. The purpose of such a model is not to address narrow, largely deterministic issues that have something close to a right answer — like how to organize guards at an airport for maximum efficiency and coverage, an issue, which could be solved with an actual equation. An effective model should instead focus on what can be called “complex strategic judgments”: Should we
invade Syria? Should we close the nuclear deal with Iran? Can we move from a nuclear triad to a dyad? These are questions on which information is imperfect, dozens of variables interact in nonlinear ways, and human choice and agency generate unpredictable patterns.

In such contexts, the future will unfold under the influence of dozens of variables interacting in unpredictable ways — meaning that it is not resident in accessible, present information. (You can gather all the data on Pakistan you want — no algorithm will accurately forecast the country’s condition in ten years’ time.) These are contexts, as well, in which values preempt data. Choices are decisively influenced by values rather than facts, and these values will be contested. (Whether we deploy units to Iraq to fight the Islamic State is as much about the obligation to fulfill a commitment and honor past sacrifice as it is about any quantifiable national security benefit.)

Critically, too, each case of complex strategic judgments is fundamentally unique, which makes it mostly impossible to create meaningful data sets or find truly reliable patterns. Just because a U.S. threat deterred someone three times in a row doesn’t provide a reliable basis for believing it will do so again.

These factors add up to a critical distinction when thinking about risk. Risk management in more constrained and predictable contexts is one thing: Insurance companies can estimate the risks of various actuarial choices with some precision, because they are dealing with large, comparable data sets that obey certain rules of probabilistic issues (such as normal distribution). Some programmatic and personnel issues in defense are like that, but not the big challenges of national security strategy, defense policy and statecraft. These are value-based judgment calls on one-off issues where data and patterns will offer very limited guidance. The key question for senior leaders in defense, then, is what can be done to improve the assessment of risk in such uncertain and ambiguous contexts.

Managing Risk for Complex Judgments

In the wake of the financial crisis of 2007-2008, there has been a lot of soul-searching in the investment community about the failure of risk management. But most proposals for reform amount to refinements of the same approaches that failed in 2007: better quantitative models, more explicit treatment of assumptions, and deeper consideration of “fat tail” events (that is, big shocks). All of that makes sense. But arguably the most important lesson of the crisis was that large institutions need to shift their whole mindset for dealing with risk in complex and uncertain environments.

They need to focus on dealing with the human factors — from wishful thinking to personality to groupthink — that undermined even the most elaborate risk procedures in the financial industry, and think of themselves not as mastering identifiable risks, as much as armoring themselves for a trip through a highly uncertain and competitive environment.

Such a revised approach to risk could have four basic elements.

1. **Risk must be tightly integrated into a broader strategy process.**

   Too often, risk processes become highly technical activities detached from the main process of developing strategy. They limit themselves to identifying dangers rather than laying the groundwork for a careful evaluation of the complicated interplay of risk and reward at the core of any complex strategic judgment. The first step toward an effective risk process is to define its role clearly and nest it in a comprehensive strategy process.

   As argued in my previous article, the most important role risk assessments can play in such a strategic process is to impose a disciplined focus on outcomes — things that could go wrong with proposed strategies. The biggest national security disasters and risk calamities often stem from a willful disregard of consequences. Good risk management should force decision-makers captivated by overconfident wishful thinking to pause, take seriously what could go wrong, and spend time putting in place mitigating actions.

2. **Risk processes should generate the right dialogues.**

   Effective risk management is not about forecasting specific dangers. It should not aim to deliver a precise risk
estimate: “Risk is moderate in this scenario,” or “There is a 5 percent chance of losing 25 percent of invested capital.” Instead it should serve as an invitation to discuss key themes and issues around risk. What are the real perils of our proposed strategy? What is the chance our assumptions are wrong? Are several risks interconnected in ways we haven’t anticipated? What are the most likely developments over the next five or ten years that could challenge our plans?

In order to have well-informed dialogues with candor, transparency turns out to be an especially important trait of successful risk management. A major barrier to controlling risk before the 2007-2008 financial crisis was the obscurity involved in many of the financial instruments being built, often in intentionally shadowy operations buried deep within companies. When risk is hidden, it can be more easily dismissed, and massively risky positions can germinate in the shadows without anyone noticing until it’s too late.

3. **Risk processes must be grounded in the right organizational culture.**

Organizations that manage risk well do so in large measure by creating a risk-aware culture — one that values dissent and warning, promotes transparency and demands candor.

A strong risk culture has a number of typical characteristics. It takes the risk part of the risk-reward calculus seriously, and while not abandoning boldness or aggression, makes clear that everyone’s job is being risk-aware. It connects risk management to senior leadership: CEOs and other top officials must set a clear tone of risk appreciation from the top and reinforce the seriousness of the issue with their own actions. It values dissents and warnings and treats those who provide them as prized institutional assets. It imposes accountability for risk management, punishing those who fail to achieve it — no matter how favored they may have been. And it is built around open and shared risk assessments, ensuring a constant dialogue throughout the firm, and making sure that risks don’t become submerged under layers of assumption or wishful thinking.

4. **Being secure in complex environments is ultimately more about managing uncertainty than managing risk.**

In traditional risk management, an organization works to identify potential dangers, measure them and create frameworks or processes to track them. It is most appropriate in deterministic environments. In situations of complex uncertainty, on the other hand, the real demand is to manage uncertainty — to understand and define a wide array of possible futures and build the capabilities and attributes necessary to hedge against them. Its essence is positioning an organization (or a nation) to be robust and resilient within a complex, dynamic and competitive ecosystem.

**What Should a National Security Risk Model Look Like?**

A national security strategy focused on managing uncertainty would cherish diversity, building a balanced joint force with a wide range of capabilities to hedge against many potential missions, threats and futures. It would pursue modularity, ensuring that the loss of any one capability (or type of capability) would not cascade to systemic failure. It would build damping mechanisms into the system: A good example is regulations on leverage and capital reserve requirements in the financial sector to create inherent robustness. It would aim, over time, to create institutions and norms that promote stabilizing feedback loops, such as habitual reactions to terrorism that reduce the impact of each successive attack and solidify the global campaign against the tactic. And in support of many of these principles, it would maximize innovation and experimentation to adapt to changing circumstances and constantly test a range of new concepts and systems.

Managing uncertainty is all about building systems that are inherently robust, stable, and self-healing in their reaction to volatility. Identifying and evaluating potential risks is a critical entry point to managing uncertainty, but the approach recognizes that such efforts will inevitably fail — in part because of the unavoidable human factors that wreak havoc on procedural risk efforts.

A set of principles like these, from improved approaches to risk management to the elements of managing uncertainty, could be integrated throughout the national security planning and policy process — from the formal stages of national
security decisions to planning factors in Defense Department strategy documents. Taken together, they offer a comprehensive mindset for managing uncertainty and mitigating risk, one that takes seriously the uncertain, emerging context that so challenges the architects of U.S. national security strategy.

*Michael Mazarr is a senior political scientist at the RAND Corporation. He completed this research before joining RAND, as a nonresident fellow at the New America Foundation. The views expressed here are his own.*

Photo credit: Secretary of Defense