Incorporating Risk into National Security Planning

By Malia K. Du Mont, Non-Resident Fellow @ the Atlantic Council

Risk is a critical concept for helping decision-makers identify and make policy choices that support strategic priorities, but it is often mis-applied. The failure to integrate risk appropriately into strategic planning leads to strategies that 1) do not allow for adequate flexibility for addressing future uncertainties and opportunities, 2) are largely reactive instead of forward-looking; and 3) have not taken into account the full range of potential implications of the strategic choices enshrined therein.

To ensure that risk is appropriately informing strategic decision-making, it is essential to avoid some common pitfalls by taking the approach described below.

- **Risk assessment, not threat assessment.**

  Much of the apparatus of national security policymaking is structured to consider and incorporate threat assessment more easily than risk assessment. This is true for several reasons:

  - There is no common risk language across the interagency. Even within the Department of Defense, there is no formally recognized lexicon for discussing risk. As a result, key terms are not utilized consistently across or within agencies, making it difficult for the interagency to arrive at a shared understanding of the contents and implications of strategic risk.

  - There is no broadly accepted methodology for assessing risks to national security strategy. The SWOT (strengths, weaknesses, opportunities, threats) method is well known, but its application varies greatly, and other methods are also sometimes in use. In contrast, the intelligence community has a well-established, consistent set of threat assessment frameworks that have long been in wide usage, with analysts receiving regularized training in the details of threat assessment and associated terminology. National security decision-makers are accustomed to seeing the products of these threat assessment processes and generally understand how to consume and take action based on their analysis: threats are generally tangible and must be mitigated.

  - Foresight, which is central to understanding the full range of future risks and risk triggers, is not consistently utilized and incorporated into strategy-making. There is no centralized government body for engaging in foresight, and agencies are not required to coordinate with or draw on the products of the foresight organizations that do exist.

  In other words, threat assessment is embedded in the culture of organizations charged with national security to a degree that risk assessment is not; as a result it takes sustained leadership attention to shift institutional focus away from threats to incorporate risks in the development of strategy.

Although the two concepts are often (wrongly) conflated in national security circles, threats are not the same thing as risks. Threats to national security are tangible problems that must be resolved in order to achieve national security objectives, whereas risks are exposures to the chance of challenge or loss. In the context of national security, a threat once identified requires mitigation, but a risk could be managed in a variety of ways and does not automatically demand mitigation. Mitigating threats thus involves fewer policy choices than managing risk and is in many ways a reactive process – even if the assessment is focused on future threats. National security strategy that is built around addressing future threats is reactive over the long term and does not really help policy-makers proactively shape world events for the benefit of American interests. Threat assessment also largely ignores the possibility of strategic opportunities, further limiting its usefulness as a strategy tool.

Risk assessment identifies a broader array of issues than mere threat assessment, including the risk of missed opportunities. As a tool to inform policy-makers of the range of choices they confront, it thus facilitates a more comprehensive approach to national security strategy development. In order for U.S. national security strategy to effectively incorporate risk assessment, the national security community needs to agree to use a common methodology. National Security Staff has in recent years undertaken some efforts to move towards a common risk language and methodology to use across the interagency, but these efforts have not yet resulted in an agreed-upon approach.

- **Risk management, not risk mitigation.**

Not all risks must be mitigated; the concept of risk management incorporates a range of choices including mitigation but also acceptance, avoidance, and transfer of risk. Yet many national security practitioners automatically and incorrectly take a mitigation approach to risk when developing policy. Congress too makes this mistake: the NDAA requires the Chairman of the Joint Chiefs of Staff to produce a classified Risk Assessment on an annual basis, to be accompanied by a classified Risk Mitigation Plan which must address every risk identified in the Risk Assessment. This legislation forces the Defense Department to take a reactive approach wherein the mere identification of a risk requires its mitigation.

Requiring all risks to be mitigated de facto substitutes policy choices with a rules-based control model that greatly reduces leadership flexibility and leaders' ability to minimize the implications of risk events should they occur. Good risk management does not eliminate risks but rather enables leaders to thoughtfully consider which risks are worth accepting and where limited resources should be targeted, and organizations to develop the resilience necessary for absorbing a certain unavoidable degree of risk. Good risk management also distinguishes between serious risks for which a strategy is required, and high impact/low probability events. Effective national security strategy, when appropriately incorporating risk management principles, prioritizes risk based on its potential effects on national security objectives. Strategy risks are not necessarily inherently undesirable; a bold national security strategy that is expected to significantly advance American interests in the world generally requires the national security establishment to accept significant risk. The process of managing those risks in itself can be a key driver in advancing U.S. interests.

It is important for a risk management plan, as articulated via national security strategy, to take into account the fact that there are long-standing challenges with implementing risk management in a national security context. Key among them are 1) the difficulties associated with enterprise risk management, and 2) the chilling effect of politics. With regard to the former, there is no consistently accepted method for managing risk across enterprises as large and siloed as the Defense Department. Effective risk management must be integrated across organizations; this can happen to a certain extent through the strategic planning process. However, maintaining that integration beyond the development of a strategic plan into its implementation phase is extremely challenging. With regard to the latter, political optics can constrain risk management choices. Leaders may feel driven to mitigate risks even when accepting them does not represent real danger to American national security interests and mitigating them requires significant resources. Ironically, few political leaders are comfortable taking the risk of accepting risk.

- **Strategic trade-offs, not quantitative calculations.**

  In the private sector, risk is often quantifiable to a great degree of detail in terms of the probability of various kinds of failure and the subsequent impact to a company's bottom line. National security risk does not lend itself to the same quantifiable definitions. Progress towards meeting national security goals can be partially tied to some quantitative metrics, but defining strategic risk in purely quantitative terms prematurely determines those metrics, and suggests that the implications of strategic choices are binary rather than complex. Rather, it is more useful to think of strategic risk choices as a series of strategic trade-offs, with a sliding risk calculus between them. The most recent QDR, for example, incorporated a risk triangle that helped leaders prioritize and understand trade-offs between capabilities, capacity, and readiness.

  Strategic trade-offs can also be made between current and future risk, internal and external risk, and operational and strategic risk. This kind of approach creates a risk framework that enables policy-makers to make nuanced choices based on strategic priorities, and doesn't automatically drive them in one particular direction.